IV. AĞ VE BİLGİ GÜVENLİĞİ SEMPOZYUMU

BİLDİRİLER KİTABI

25-26 KASIM 2011
ANKARA
Atılım Üniversitesi-Orhan Zaim Konferans Salonu

Düzenleyen Kuruluşlar:

ELEKTRİK MÜHENDİSLERİ ODASI • TMMOB • 1954 • ANKARA ŞUBESİ

1 9 9 6 ATILIM ÜNİVERSİTESİ

ODTÜ

Destekleyen Kuruluş

TÜBİTAK

TMMOB
Elektrik Mühendisleri Odası
Ankara Şubesi Yayınıdır

IV. AĞ VE BİLGİ GÜVENLİĞİ SEMPOZYUMU

1. Baskı: Ankara
Aralık 2011

EMO Yayın No: sk/2011/11
ISBN: 978-605-01-0221-5

TMMOB ELEKTRİK MÜHENDİSLERİ ODASI ANKARA ŞUBESİ
Necatibey Cd. No: 102/3 06570 Maltepe/Ankara
Tel: (0.312) 231 44 74 Faks: (0.312) 232 10 88
http://ankara.emo.org.tr&ankara@emo.org.tr

Baskı
Hermes Ofset Ltd. Şti.
K. Karabekir Cad. No:39/16 İskitler/ANKARA
Tel: (0312) 384 34 32 - www.hermesofset.com.tr

İÇİNDEKİLER

ORGANİZASYON

IV. ABGS DÜZENLEME KURULU

Prof. Dr. Adnan YAZICI (Eş.Bşk)	*ODTÜ*
Prof. Dr. İbrahim AKMAN (Eş.Bşk.)	*Atılım Üniversitesi*
Prof. Dr. Ali YAZICI	*Atılım Üniversitesi*
Dr. Attila ÖZGİT	*ODTÜ*
Dr. Cevat ŞENER	*ODTÜ*
Dr. Onur Tolga ŞEHİTOĞLU	*ODTÜ*
Mehmet BOZKIRLIOĞLU	*EMO YK Üyesi*
Hüseyin YEŞİLSEVEN	EMO *Bilgisayar MEDAK*
Burak OĞUZ	*EMO Ankara Şubesi*
Gölay ŞAKİROĞULLARI	*EMO Ankara Şubesi*
Ramazan PEKTAŞ	*EMO Ankara Şubesi*
Taylan Özgür YILDIRIM	*EMO Ankara Şubesi*

IV. ABGS YÜRÜTME KURULU

Prof. Dr. Adnan YAZICI (Eş.Bşk)	*ODTÜ*
Prof. Dr. İbrahim AKMAN (Eş.Bşk.)	*Atılım Üniversitesi*
Prof. Dr. Ali YAZICI	*Atılım Üniversitesi*
Prof. Dr. Eşref ADALI	*İTÜ*
Prof. Dr. Hayri SEVER	*Hacettepe Üniversitesi*
Prof. Dr. M. Ufuk ÇAĞLAYAN	*Boğaziçi Üniversitesi*
Prof. Dr. Mehmet R. TOLUN	*Çankaya Üniveristesi*
Prof. Dr. Özgür ULUSOY	*Bilkent Üniversitesi*
Prof. Dr. Ziya AKTAŞ	*Başkent Üniversitesi*
Doç. Dr. Yücel SAYGIN	*Sabancı Üniversitesi*
Yrd. Doç. Dr. Atila BOSTAN	*Atılım Üniversitesi*
Yrd. Doç. Dr. Murat KOYUNCU	*Atılım Üniversitesi*
Dr. Attila ÖZGİT	*ODTÜ*
Dr. Cevat ŞENER	*ODTÜ*
Dr. Onur Tolga ŞEHİTOĞLU	*ODTÜ*
Dr. Ruken ÇAKICI	*ODTÜ*
Dr. Sevil ŞEN	*Hacettepe Üniversitesi*
Ziya KARAKAYA	*Atılım Üniversitesi*
Dr. Mehmet KARA	*TÜBİTAK*
Burak OĞUZ	*EMO Ankara Şubesi*
Gölay ŞAKİROĞULLARI	*EMO Ankara Şubesi*
Hasan BAYCAN	*EMO Ankara Şubesi*
İzlem GÖZÜKELEŞ	*EMO Ankara Şubesi*
Mehmet BOZKIRLIOĞLU	*EMO*
Murat KÜÇÜKARSLAN	*EMO Ankara Şubesi*
Ömürhan SOYSAL	*EMO Ankara Şubesi*
Ramazan PEKTAŞ	*EMO Ankara Şubesi*
Taylan Özgür YILDIRIM	*EMO Ankara Şubesi*
Tülay IŞIK	*EMO Ankara Şubesi*

IV. ABGS BİLİM KURULU

Prof. Dr. M. Bülent ÖRENCİK	*TÜBİTAK MAM*
Prof. Dr. Ercan SOLAK	*Işık Üniversitesi*
Prof. Dr. Ersan AKYILDIZ	*ODTÜ*
Prof. Dr. Ferruh ÖZBUDAK	*ODTÜ*
Prof. Dr. Mehmet E. DALKILIÇ	*Ege Üniversitesi*
Prof. Dr. Mehmet Ufuk ÇAĞLAYAN	*Boğaziçi Üniv.*
Doç. Dr. Bülent TAVLI	*TOBB ETÜ*
Doç. Dr. Nurcan TÖRENLİ	*Ankara Üniversitesi*
Doç. Dr. Nevcihan DURU	*Kocaeli Üniversitesi*
Yrd. Doç. Dr. Atila BOSTAN	*Atılım Üniversitesi*
Yrd. Doç. Dr. Enis KARAARSLAN	*Muğla Üniversitesi*
Yrd. Doç. Dr. Alptekin KÜPCÜ	*Koç Üniversitesi*
Yrd. Doç. Dr. Hüseyin YÜCE	*Marmara Üniv.*
Yrd. Doç. Dr. Tuğkan TUĞLULAR	*İzmir Yük. Tek. Ens.*
Dr. Attila ÖZGİT	*ODTÜ*
Dr. Cevat ŞENER	*ODTÜ*
Dr. Hamdi Murat YILDIRIM	*Bilkent Üniversitesi*
Dr. İlker KORKMAZ	*İzmir Ekonomi Üniv.*
Dr. Onur Tolga ŞEHİTOĞLU	*ODTÜ*
Dr. Sedat AKLEYLEK	*Ondokuzmayıs Üniv.*
Dr. Selçuk KAVUT	*Gebze Yük. Tek. Ens.*
Dr. Ahmet Emir DİRİK	*Uludağ Üniversitesi*
Dr. Hidayet TAKCI	*Gebze Yük. Tek. Ens.*
Dr. Necdet YÜCEL	*Onkesiz Mart Üniv.*
Çağdaş ÇALIK	*ODTÜ*
Zaliha YÜCE TOK	*ODTÜ*
Ziya KARAKAYA	*Atılım Üniversitesi*

IV. ABGS DANIŞMA KURULU

Yrd. Doç. Dr. Hüseyin POLAT	*Anadolu Üniversitesi*
Ali YAZICI	*ASELSAN*
Dr. Emrah TOMUR	*BDDK*
K. Sacid SARIKAYA	*Bilgi Tek. ve İltş. Kur.*
Mustafa ÜNVER	*Bilgi Tek. ve İltş. Kur.*
Yrd. Doç. Dr. Gökay SALDAMLI	*Boğaziçi Üniversitesi*
Deniz VAROL	*Çevre ve Orman Bak.*
Meltem YILDIRIM	*Dokuz Eylül Üniv.*
Muzaffer YILDIRIM	*EGA*
Tahir Emre KALAYCI	*Ege Üniversitesi*
Ramazan BALTA	*EMO Bursa Şube*
Aktan ATLI	*EMO Diyarbakır Şube*
Murat ÇELİK	*EMO Diyarbakır Şube*
Ender KELLECİ	*EMO Eskişehir Şube*
Ahmet YAZİCİ	*EMO Eskişehir Şube*
Süleyman MERT	*EMO İstanbul Şube*
Ceyda CİRİTOĞLU	*EMO İstanbul Şube*
Avni HAZNEDAROĞLU	*EMO Kocaeli Şube*
Nevcihan DURU	*EMO Kocaeli Şube*
Alkan ALKAYA	*EMO Mersin Şube*
Veysel BAYSAL	*EMO Mersin Şube*
Mehmet ÖZDAĞ	*EMO Samsun Şube*
Gökhan KAYHAN	*EMO Samsun Şube*
Dr. Adnan ÖZDEMİR	*Enerji ve Tab.Kay. Bak.*
Yrd. Doç. Dr. Ahmet YAZICI	*Esk. Osmangazi Üniv.*
Yrd. Doç. Dr. Selçuk CANBEK	*Esk. Osmangazi Üniv.*
Necla VARDAL	*Fintek*
Dr. İbrahim SOĞUKPINAR	*Gebze Yük.Tek. Enst.*
Bilgin TAŞYÜREK	*HSBC*
Hilal BOĞA	*İçişleri Bakanlığı*
Zafer KARACA	*İçişleri Bakanlığı*
Doç. Dr. Hasan ERBAY	*Kırıkkale Üniversitesi*
Aytunç AYHAN	*Milli Prodük. Merk.*
Yrd. Doç. Dr. Ercan BULUŞ	*Namık Kemal Üniv.*
Dr. Mehmet KARA	*TÜBİTAK-BİLGEM-UEKAE*
Bülent ARSAL	*Türk Telekom*
Duygu FİDANCIOĞLU	*Türk Telekom*
Melike BURAKGAZİ BİLGEN	*Türk Telekom*
Özgür ŞANLI	*T.C. Merkez Bankası*
Turgut ÖZSOY	*T.C. Merkez Bankası*
Prof. Dr. Coşkun SÖNMEZ	*Yıldız Teknik Üni.*
Prof. Dr. Oya KALIPSIZ	*Yıldız Teknik Üni.*

4. Ağ ve Bilgi Güvenliği Sempzoyumu Programı

25 Kasım 2011

10:00- 12:00	**Açılış Konuşmaları (Salon A)** Prof.Dr. İbrahim AKMAN — Atılım Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanı Ramazan PEKTAŞ — EMO Ankara Şubesi Başkanı Mehmet BOZKIRLIOĞLU — EMO Yönetim Kurulu Üyesi Prof.Dr. Abdürrahim ÖZGENOĞLU — Atılım Üniversitesi Rektörü	
	SALON A	**SALON B**
12:00-13:00	**Çağrılı Bildiri : Türkiye ve Dünyada Ağ ve Bilgi Güvenliği** ***Prof.Dr. Eşref ADALI***	
14:00-15:30	**Bildiri Oturumu-1 : Bilgi ve Veri Güvenliği-I** **Oturum Başkanı : Prof.Dr. Ziya AKTAŞ** • Atlamalı Aralık Yayın Şifreleme Sisteminde Bedava Alıcıların İyi Yerleştirilmesi / *Murat AK-Ali Aydın SELÇUK* • LSB Ekleme Yönteminde Bilgi Gizleme İçin Tek Renk Kanal Kullanımının Güvenliğe Etkileri / *Emir ÖZTÜRK -Andaç ŞAHİN MESUT-Altan MESUT* • Bilişim Güvenliği : Kullanıcı Açısından bir Durum Tespiti / *Atila BOSTAN-İbrahim AKMAN*	**Bildiri Oturumu-2 : Sistem ve Ağ Güvenliği-I** **Oturum Başkanı : Yrd.Doç.Dr. Murat KOYUNCU** • İnternet Bankacılığında Akıllı SMS İçin Üç Yollu El Sıkışma / *Onur GÖK-H. Engin DEMİRAY* • SNMPv3 İle Güvenli Ağ Topoloji Keşfi / *Musa BALTA-İbrahim ÖZÇELİK* • Şifreli İnternet Trafiğinin Gerçek Zamanlı Sınıflandırılması / *Cihangir BEŞİKTAŞ-Hacı Ali MANTAR* • IPv4 / IPv6 Güvenlik Tehditleri ve Karsılastırılması / *Muhammed Ali AYDIN-Ayhan ÇAKIN*
15:45-18:00	**Panel : İnternet Yasakları, Kişisel Haklar ve Özgürlükler, Kişisel Bilginin Mahremiyeti** **Oturum Başkanı : Dr. Onur Tolga ŞEHİTOĞLU** • Doç.Dr. Mustafa AKGÜL-Bilkent Üniv. • Dr. Meltem TARHAN YÖNDEM-Sabancı Üniv. • Yüksel SAMAST-Verion • İzlem GÖZÜKELEŞ-EMO Ankara Şube	

26 Kasım 2011

10:00-11:30	**Bildiri Oturumu-3 : Bilgi ve Veri Güvenliği-II** **Oturum Başkanı : Prof.Dr. İbrahim AKMAN** • Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği / *Mehmet KARA-Soner ÇELİKKOL* • Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği / Volkan EVRİN-Mehmet DEMİRER • Bir Kuruluşun Bilgi Sistemi Güvenliği için Bir Yaklaşım / Hakan TAN-Ziya AKTAŞ • Tekil Değer Ayrışımı Tabanlı Yeni Bir Kırılgan Resim Damgalama / *Veysel ASLANTAŞ-Mevlüt DOĞRU*	**Bildiri Oturumu-4 : Sistem ve Ağ Güvenliği-II / Kablosuz Ağlarda Güvenlik** **Oturum Başkanı : Yrd.Doç.Dr. Atila BOSTAN** • Güvenli Bilgi Paylaşımı ve Sanal Hava Boşluğu / Ali YAZICI-ASELSAN • HTML5 Güvenliği - Yeni Nesil Web Tehditleri / *Emre ÇAKIR* • Mobil Ağlarda Kimlik Doğrulama Hakkında Bir İnceleme / *Fatma AKGÜN-Ercan BULUŞ* • Kablosuz Geçici Ağlarda Yönlendirme Saldırılarının Analizi ve Önlenmesi / *İbrahim ZAĞLI-Güray YILMAZ-Coşkun SÖNMEZ* • MDS Kod Tabanlı Gizlilik Paylaşım Şemasında Hileli Katılımcıları Tespit Etmek ve Kimliklendirmek / *Derya ARDA-Ercan BULUŞ*
11:45-13:00	**Özel Oturum 1 : Adli Bilişim Analizi** / Hüzeyfe ÖNAL-Bilgi Güvenliği Akademisi	**Eğitim 2 : Sosyal Mühendislik Atakları** / Ünal TATAR-TÜBİTAK BİLGEM UEKAE
14:00-15:45	**Bildiri Oturumu-5 : Kriptoloji** **Oturum Başkanı : Prof.Dr. Ali YAZICI** • Bilgi Güvenliğinde Kuantum Teknikler / *Mustafa TOYRAN-Thomas PEDERSEN-Attila HASEKİOĞLU-Ali CAN-Savaş BERBER* • Kaos Tabanlı Yeni Bir Blok Şifreleme Algoritması / *Fatih ÖZKAYNAK-Ahmet Bedri ÖZER-Sırma YAVUZ* • Kısmi Anahtarlı Çok Alıcılı Bir Şifreleme Anahtar Yönetimi Algoritması / *Dindar ÖZ-Ersin GÜLAÇTI-Işıl ÖZ* • Blakley Gizli Paylaşımı Dayanarak DataMatrix ECC200 Kodları / *Katira Soleyman ZADEH-Vasif NABİYEV*	**Çalıştay : Üniversitelerde Bilgi Güvenliği Eğitimi Nasıl Ele Alınmalı?** • Dr. Mehmet KARA-TÜBİTAK BİLGEM UEKAE • Doç.Dr. İbrahim SOĞUKPINAR-Gebze Yüksek Teknoloji Enstitüsü • Yrd.Doç.Dr. Kemal İLTER-Yıldırım Beyazıt Üniversitesi
16:15-17:30	**Özel Oturum 3 : Dijital Beden ve Dijital Gözetim** **Oturum Başkanı : Prof.Dr. Mutlu BİNARK** • Dijital Gözetim Olgusu: Panoptikondan, Süperpanoptikona ve Sinoptikona Dijital Gözetimin Farklı Boyutları / *Selma Arslantaş-Gülden Gürsoy* • İnternet'te Dijital Gözetimin Farklı Boyutları / *Alkım Özaygen* • Türkiye'de Mernis'den E-Kimliğe doğru TC. Kimlik numarası ile yurttaşın dijital bedenlenişi / *Şafak Dikmen* • TC. Kimlik Numarası Özelinde Kişisel Verilerin Güvenliği / *Elif Küzeci* • Yurttaşın Veri Bütünlüğü ve İnsan Hakları Temelinde Sorun Tespiti ve Öneriler / *Prof.Dr. Mutlu Binark*	**Özel Oturum 2 : Özgür Yazılımlarda Güvenlik Çözümleri** *Fatih ÖZAVCI-GamaSEC*

1. KISIM:
BİLGİ VE VERİ GÜVENLİĞİ

MDS Kod Tabanlı Gizlilik Paylaşım Şemasında Hileli Katılımcıları Tespit Etmek ve Kimliklendirmek

Derya Arda[1] Ercan Buluş[2]

[1]Bilgisayar Mühendisliği Bölümü, Trakya Üniversitesi, Edirne
[2]Bilgisayar Mühendisliği Bölümü, Namık Kemal Üniversitesi, Çorlu

[1]e-posta: deryaa@trakya.edu.tr [2] e-posta: ercanbulus@nku.edu.tr

Özetçe

Bir (k,n) Gizlilik Paylaşım Şeması, kriptografik anahtarlar gibi gizli veriyi korumak için geliştirilmiş bir tekniktir. Bu şemada gizlilik n paylaşımcı arasında dağıtılmıştır ve bu paylaşımcılardan sadece herhangi k tanesi bir araya gelerek gizliliği yeniden elde edebilirken, k' dan daha az paylaşımcı bir araya gelerek gizlilik hakkında hiçbir bilgi elde edemezler. Bu şemadaki amaç yapılacak saldırılara karşı anahtarın tek bir kullanıcıda bulunmaktansa pek çok kullanıcıya dağıtılarak güvenliğini arttırmaktır. Gizlilik Paylaşım Şeması ilk olarak 1979 yılında Shamir ve Blakley tarafından birbirlerinden bağımsız olarak ortaya atılmıştır. Daha sonraları literatürde pek çok gizlilik paylaşım şemaları önerilmiştir. Bunlardan bazıları McEliece ve Sarwate tarafından önerilen hata doğrulama kod tabanlı gizlilik paylaşım şemasıdır. Gizlilik paylaşım şemalarında hileli katılımcılar olduğu zaman gizliliği yeniden elde etmek her zaman mümkün değildir. Hatalı veriyi tespit etmek ve kimliklendirmek gizliliği yeniden elde etmede oldukça önemlidir. Bu çalışmada (n+1, k) MDS (maksimum uzaklıkla ayrılabilen) kod kullanarak bir (k, n) eşik gizlilik paylaşım şeması tasarlandı. Aynı zamanda hata doğrulama kod tekniklerinden faydalanılarak, gizlilik paylaşım şemasında hileli katılımcılar tespit edilip onların bozuk paylaşımları düzeltilip gizliliğin yeniden elde edildiği gösterildi.

1. Giriş

Çağdaş kriptografi ve kodlama teorisi 60 yıldan daha fazla başarılı bir tarihe sahiptir. 1948' de Claude Shannon "Haberleşmenin Matematiksel Teorisi" adlı makalesinde bilgi teorisi ve kodlama teorisi gibi iki disiplini başlatıp geliştirmiştir.[3] Daha sonra Nyquist ve Hardley'in teorilerini genişleterek bilginin ölçülmesine olasılık kavramını eklemiştir. Böylelikle bilgi kuramı ile kriptoloji arasındaki bağıntıyı kurmuştur ve kripto sistemlerin matematiksel esaslarını belirlemiştir.

Kriptografi ve kodlama teorisinin bilgi iletişiminde amaçları farklıdır. Kriptografinin amacı iki ya da daha fazla kişinin haberleşmesinde gizlilik, veri bütünlüğü, doğrulama ve inkar edememe esaslarını birleştirerek mesajın güvenli iletişimini sağlamaktır. Kodlama teorisinin amacı ise iletim sırasında oluşan hataları doğrulamak anlamında güvenli iletişim sağlamaktır.

Kriptografide diğer önemli bir mesele şifreleme algoritmalarında kullanılan anahtarın korunması ve saklanması problemidir. Bir (k,n) Gizlilik Paylaşım Şeması, kriptografik anahtarlar gibi gizli veriyi korumak için geliştirilmiş bir tekniktir. Gizlilik paylaşım şeması yapılacak saldırılara karşı anahtarın tek bir kullanıcıda bulunmaktansa pek çok kullanıcıya dağıtılarak güvenliğini arttırmak için tasarlanmış bir yapıdır. Bu şema ilk olarak 1979 yılında Shamir [1] ve Blakley [2] tarafından birbirlerinden bağımsız olarak ortaya atılmıştır. Daha sonraları literatürde pek çok gizlilik paylaşım şemaları önerilmiştir. Bunlardan bazıları hata doğrulama kod tabanlıdır [5,6]. Örneğin bunlardan birisi McEliece ve Sarwate tarafından önerilen hata doğrulama kod tabanlı gizlilik paylaşım şemasıdır [6].

Gizlilik paylaşım şemalarında hileli katılımcılar olduğu zaman gizliliği yeniden elde etmek her zaman mümkün değildir. Hatalı veriyi tespit etmek ve kimliklendirmek gizliliği yeniden elde etmede oldukça önemlidir.

Bu çalışmada (n+1, k) MDS (maksimum uzaklıkla ayrılabilen) kod kullanarak bir (k, n) eşik gizlilik paylaşım şeması tasarlandı. Aynı zamanda hata doğrulama kod tekniklerinden faydalanılarak, gizlilik paylaşım şemasında hileli katılımcılar tespit edilip onların bozuk paylaşımları düzeltilip gizliliğin yeniden elde edildiği gösterildi.

2. Gizlilik Paylaşım Şeması

Gizlilik paylaşımı anahtar yönetimi ve anahtar dağıtımı ile ilişkilidir. Bu anahtar dağıtım ve yönetim problemi bütün kriptosistemlerde oldukça sık rastlanan bir problemdir.
Temel olarak bir (k,n) gizlilik paylaşım şemasında d gizliliği n kişi arasında dağıtılır ve her hangi k kişi veya daha fazlası birleşerek gizliliği yeniden elde edebilir. Ancak $k-1$ veya daha az kişi gizliliği elde edemezler [4,7].

3. Kodlama Teorisinde Kullanılan Temel Kavramlar

Tanım 3.1. (Minimum uzaklık): C kodunun elemanları olan kod kelimeleri arasındaki uzaklıkların en küçüğüne C kodunun minimum uzaklığı denir ve $d(C)$ ile gösterilir [9].

$$d = d(C) = \min_{\substack{u,v \in C \\ u \neq v}} d(u,v)$$

Tanım 3.2. (Doğrusal Kod) : q elemanlı cisme Galois cismi denir. $GF(q)$ veya IF_q ile gösterilir . Burada p bir asal sayı $n \in N$ olmak üzere $q = p^n$ biçimindedir.

$V(n,q) = IF_q^n = \left\{ x = (x_1, x_2, ..., x_n) \,\middle|\, x_i \in IF_q \right\}$

kümesi IF_q üzerinde n boyutlu bir vektör uzayı olmak üzere, IF_q^n'in bir C alt uzayına doğrusal kod denir.

C, IF_q^n vektör uzayının k boyutlu bir alt uzayı ise C doğrusal kodu $[n,k]$ ile d minimum uzaklığı da belirtilmek isteniyorsa $[n,k,d]$ ile gösterilir.

C, $[n,k,d]$ parametreli bir doğrusal kod ise kodun eleman sayısı $M = q^k$, kodun oranı $R = \frac{k}{n}$' dir [10].

Tanım 3.3. (Ağırlık Fonksiyonu) x, IF_q^n vektör uzayının herhangi bir elemanı olmak üzere x 'in sıfırdan farklı bileşenlerin sayısına x elemanının ağırlığı denir ve $w(x)$ ile gösterilir.

Bir C kodunun sıfırdan farklı tüm kod kelimelerinin ağırlıklarının en küçüğüne C kodunun minimum ağırlığı denir ve $w(c)$ ile gösterilir [10].

Tanım 3.4. (Üreteç Matris) $[n,k]$ şeklindeki C bir doğrusal kod olsun. Satırları C kodunun bir baz vektörlerinden oluşan *kxn* boyutlu G matrisine, C kodunun üreteç matrisi denir.

Eğer G matrisi C kodunun üreteç matrisi ise C kodunun kod kelimeleri, G matrisinin satırlarının doğrusal bileşimidir. $G = (I_k | A)$ bu üreteç matrisi standart formdadır [10].

Tanım 3.5. (Kontrol Matris) C kodunun üreteç matrisi $G = (I_k | A)$ olmak üzere; $GH^T = 0$ şartını sağlayan $H = (-A^T | I_{n-k})$ matrisine C kodunun kontrol matrisi denir [10].

4. MDS Kodlar ve Özellikleri

Tanım 4.1. C bir $[n,k,d]$ doğrusal kod ise, $k + d \le n + 1$ 'dir. $d = n - k + 1$ Singleton sınırı ile $[n,k,d]$ kodları (MDS) maksimum uzaklıkla ayrılabilen kodlar olarak adlandırılır. Kodlama teorisindeki önemli kodlardan birisi de maksimum uzaklıkla ayrılabilen kodlardır. Çünkü bu tür kodlar, n ve k verildiğinde d 'si (dolayısıyla, düzeltilebilme kapasitesi) en fazla olan kodlardır [11].

Önerme 4.1. d uzaklığına sahip bir C doğrusal kodunun H kontrol matrisinin her $d-1$ sütunları doğrusal bağımsızdır. Tanımlandığı gibi bir MDS kod $n-k+1$ uzaklığa sahiptir. Böylece, kontrol matrisinin her $n-k$ sütunlarının kümesi doğrusal bağımsızdır.[11]

Önerme 4.2. A'nın her kare alt matrisinin determinantı sıfırdan farklı ($\det \neq 0$) ve tekil olmayan (nonsingular) ise aşağıdaki G üreteç matrisi ile bir [n,k,d] kodu MDS koddur.

$$G = [I_{kxk} A_{kx(n-k)}]$$

MDS kodların en iyi bilinen sınıfı etkin inşa algoritmalarına sahip olan Reed-Solomon kodlardır. [11]

5. GF(2^n) sonlu cisminde Reed-Solomon Kodlar ve MDS Kodlar

Tanım 5.1. Sonlu cisim adından da anlaşılacağı üzere sonlu sayıda elemana sahip bir 'cisim'dir. Sonlu cismin sahip olduğu eleman sayısı sonlu cismin düzenini belirler [12].

Tanım 5.2. GF(2) üzerinde oluşturulan m. Dereceden p(X) polinomu m'den daha küçük dereceli polinomlara bölünemiyorsa p(X) GF(2) üzerinde indirgenemez denir [13].

Örnek1 : $GF(2^3)$ sonlu cisim üzerinde $x^3 + x + 1$ indirgenemez polinomuna göre minimum Hamming uzaklığı 5 olan ve en fazla 2 hata düzeltebilen bir Reed Solomon kod inşa edelim. α, GF(2^3) cisminde bir üreteçtir. Bu cismin elemanları aşağıdaki Tablo1 ile gösterilmiştir.

Kod kelimesinin uzunluğu $n = q - 1 = 8 - 1 = 7$

Hata düzeltme kapasitesi $t = \frac{d-1}{2} = \frac{5-1}{2} = 2$

g(x) üreteç polinomunun derecesi $2t = 4 = n - k \Rightarrow$

$7 - k = 4 \Rightarrow k = 3$

Boyutu k=3'tür.

Dolayısıyla $n - k + 1 = 5$(*singleton* sınırı) (n,k,d;q) = (7, 3, 5; 8) olan bir MDS koddur.

Tablo1: GF(2^3) cisminin elemanları

Sayısal karşılığı	Polinomsal gösterimi	İkili karşılığı
1	α^0	001
2	$\alpha^1 = \alpha$	010
4	α^2	100
3	$\alpha^3 = \alpha + 1$	011
6	$\alpha^4 = \alpha^2 + \alpha$	110
7	$\alpha^5 = \alpha^2 + \alpha + 1$	111
5	$\alpha^6 = \alpha^2 + 1$	101
1	$\alpha^7 = 1$	001

$g(x) = (x + \alpha^0)(x + \alpha^1)(x + \alpha^2)(x + \alpha^3)$ üreteç polinomudur [14].

$g(x) = x^4 + \alpha^2 x^3 + \alpha^5 x^2 + \alpha^5 x + \alpha^6$. Buradan üreteç matrisini oluşturalım.

$$G = \begin{pmatrix} \alpha^6 & \alpha^5 & \alpha^5 & \alpha^2 & 1 & 0 & 0 \\ 0 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^2 & 1 & 0 \\ 0 & 0 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^2 & 1 \end{pmatrix}$$

Sistematik forma dönüştürülmüş G üreteç matrisi aşağıda gösterilmiştir.

$$G=\begin{pmatrix}1&0&0&\alpha^6&\alpha^5&\alpha^5&\alpha^2\\0&1&0&\alpha&\alpha^2&\alpha^4&1\\0&0&1&\alpha^6&\alpha^6&\alpha^3&\alpha\end{pmatrix}\cong\begin{pmatrix}1&0&0&5&7&7&4\\0&1&0&2&4&6&1\\0&0&1&5&5&3&2\end{pmatrix}$$

Kontrol Matrisi H,

$$H=\begin{pmatrix}\alpha^6&\alpha&\alpha^6&1&0&0&0\\\alpha^5&\alpha^2&\alpha^6&0&1&0&0\\\alpha^5&\alpha^4&\alpha^3&0&0&1&0\\\alpha^2&1&\alpha&0&0&0&1\end{pmatrix}$$

6. GF(2^3) sonlu cisminde (7,3,5) MDS kodu ile Gizlilik Paylaşımı ve Hileli Katılımcıları Tespit etmek ve Kimliklendirmek

6.1. (7,3,5) MDS kod ile Gizlilik Paylaşımı

(7,3,5) MDS kodun üreteç matrisi G yukarıda elde edilmişti. Bu kod (3,6) eşik gizlilik paylaşım şemasını belirler. Bu durum en fazla 6 paylaşımcının olduğunu ve en az 3 paylaşımcının birleşerek gizliliği elde edebileceğini söyler. C kodu için 6 paylaşımcı P_1, P_2, P_3, P_4 ,P_5 ,P_6 olsun

Örneğin seçtiğimiz bilgi vektörü $s=[1,\alpha^6,\alpha^5]$ olsun. Bu bilgi vektörünün sorumlu olduğu kod kelimesi,

$$t=(t_0,t_1,t_2,t_3,t_4,t_5,t_6)=sG=\left[1,\alpha^6,\alpha^5,\alpha,\alpha^3,\alpha^4,\alpha^2\right]$$ ve

paylaşımlar Tablo2'de gösterilmiştir.

Tablo 2 Katılımcıların gizli paylaşım değerleri

Paylaşımlar	Gizli Değerler
t_0 (gizli bileşen)	1
P_1= (1. Katılımcı)	α^6
P_2= (2. Katılımcı)	α^5
P_3= (3. Katılımcı)	α
P_4= (4. Katılımcı)	α^3
P_5= (5. Katılımcı)	α^4
P_6= (6. Katılımcı)	α^2

MDS kod tabanlı gizlilik paylaşımı için daha detaylı bir örnek [7] numaralı kaynakta gösterilmiştir.

6.2. MDS kod ile Gizlilik Paylaşımında Hileli Katılımcıları Tespit Etmek ve Kimliklendirmek

MDS kod tabanlı gizlilik paylaşım şemalarında, bu kodların etkin kod çözme algoritmaları olduğu için hileli katılımcılara karşı oldukça ilgi çekici yapılardır.

Teorem1: Gizlilik paylaşımı için bir $[k,n]$ eşik şemasında, $k+j$ katılımcılar gizliliği belirleyebilmek için bir araya geldiklerinde $\left[(n-k)/2\right]+k+j-n$'e kadar hileli katılımcının yanlış verisi düzeltilebilir.[8]

Örnek 2: Örnek 1'de [7,3,5] MDS kod için hileli katılımcıları tespit edip, düzletme aşamalarına bakalım. Bu kod $t=(n-k)/2=2$ hata düzeltme kapasitesine sahiptir. Teorem 1'e göre k+j katılımcı bir araya gelip hileli katılımcıları bulabilir. Bu durumda $4\le j$ şartı altında hileli katılımcıları tespit edebilirler. Diyelim ki P_1, P_2, P_3 katılımcılarından iki tanesi yanlış bilgi gönderdi. Bu aşamaları aşağıdaki gibi gösterelim. Bu örnekte hileli katılımcıları tespit etmek için Reed-Solomon Kodların sendrom kod çözme algoritması kullanılmıştır. Daha detaylı bilgiye [14] numaralı kaynaktan ulaşılabilir.

1. Hileli katılımcı var mı yok mu tespit et.

   Diyelim $P_1=\alpha^6$, $P_2=\alpha$, $P_3=\alpha^2$ paylaşım bilgilerini gönderdi. P_2 ve P_3 yanlış bilgi gönderdi. Ya da bunlar hileli katılımcılar olsun. Diğer katılımcıların bilgileri ise $P_0=1$, $P_4=\alpha^3$, $P_5=\alpha^4$, $P_6=\alpha^2$

Öncelikle hata olup olmadığını tespit etmek için alınan kod kelimesi eşlik sınama matrisinin transpozesi ile çarpılır ve sonuç sıfır değilse hata var yani hileli katılımcı var demektir.

$$w.H^T=0\Rightarrow hatayok$$
$$w.H^T\neq 0\Rightarrow hata\ \text{var}$$

Bu durumda alınan vektör $w=(1,\alpha^6,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^2)$ dur. $w.H^T=(1,\alpha^5,\alpha^2,1)\neq 0$ olduğu için hileli katılımcılar var demektir.

2. Sendromları hesapla.

   Sendrom polinomu

$$w(x)=1+\alpha^6x+\alpha x^2+\alpha^2x^3+\alpha^3x^4+\alpha^4x^5+\alpha^2x^6$$

Sendrom polinomundan $s_0,s_1,...,s_{e-1}$ sendromları hesaplanır.

$$s_0=w(\alpha^0)=w(1)=\alpha^3$$
$$s_1=w(\alpha)=\alpha^3$$
$$s_2=w(\alpha^2)=0$$
$$s_3=w(\alpha^3)=\alpha$$

3. Aşağıdaki denkleme göre hatalı olan bileşenin yerleri tespit edilir.

Örneğimize göre çözelim.

$$\begin{pmatrix}\alpha^3&\alpha^3\\\alpha^3&0\end{pmatrix}\begin{pmatrix}\sigma_0\\\sigma_1\end{pmatrix}=\begin{pmatrix}0\\\alpha\end{pmatrix}\Rightarrow\sigma_0=\alpha^5\ \text{ve}\ \sigma_1=\alpha^5$$

Hata yeri polinomu 6.1 denklem ile gösterilmiştir.

$$\sigma_A(x)=\sigma_0+\sigma_1x+\sigma_2x^2+...+x^e \qquad 6.1$$

$\sigma_A(x)=(x-a_1).....(x-a_e)$ formunda düzenlenip $a_1,...,a_e$ bulunur. Bunlar hileli katılımcıları tespit eder.

Bu durumda hata yeri polinomundan faydalanarak,

$$\sigma_A(x)=\alpha^5+\alpha^5x+x^2=(\alpha^3+x)(\alpha^2+x)$$

$a_1 = \alpha^2$, $a_2 = \alpha^3$ hata yerleri bulunur. Yani P_2 ve P_3 katılımcıları hileli katılımcılardır.

4. Hatalı olan bileşenler 6.2 denklemi ile düzeltilir.

$$\begin{pmatrix} a_1^0 & a_2^0 & \dots & a_e^0 \\ a_1^1 & a_2^1 & \dots & a_e^1 \\ . & & & \\ . & & & \\ a_1^{e-1} & a_2^{e-1} & \dots & a_e^{e-1} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ . \\ . \\ b_e \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \\ \\ \\ s_{e-1} \end{pmatrix} \qquad 6.2$$

$$\begin{pmatrix} a_1^0 & a_2^0 \\ a_1^1 & a_2^1 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ \alpha^2 & \alpha^3 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} \alpha^3 \\ \alpha^3 \end{pmatrix}$$

Denklem sistemi çözümünden

$b_1 = \alpha^6$ ve $b_2 = \alpha^4$ elde edilir.

$a_1 = \alpha^2$ ve $a_2 = \alpha^3$ pozisyonlarında hata oluşmuştu. Yani P_2 ve P_3 katılımcıları hileli katılımcılardı. Bu hileli katılımcıların hatalı verileri doğru verilerle düzeltilir. Yani

$a_1 = \alpha^2$ yerine $b_1 = \alpha^6$ ile düzeltilir.

$a_2 = \alpha^3$ yerine $b_2 = \alpha^4$

Alınan vektör $w = (1, \alpha^6, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^2)$

Hata vektörü yani hileli katılımcıların tespit edildiği vektör $e = (0,0,\alpha^2,\alpha^3,0,0,0)$ düzeltilip "w" ile XOR işlemi $e = (0,0,\alpha^6,\alpha^4,0,0,0)$

yapıldığında doğru kod kelimesine ulaşılır.

$$c = w \oplus e = (1, \alpha^6, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^2) \oplus (0,0,\alpha^6,\alpha^4,0,0,0)$$
$$c = (1, \alpha^6, \alpha^5, \alpha, \alpha^3, \alpha^4, \alpha^2)$$

7. Sonuç

Gizlilik paylaşım şemaları güvenliği arttırmak için geliştirilmiş kriptografik anahtar yönetimi ve anahtar dağıtımı ile ilişkili bir kavramdır. Çeşitli yapılarda gizlilik paylaşım şemaları mevcuttur. Bunlardan bazıları kodlama teorisi tabanlı gizlilik paylaşım şemalarıdır. Bu çalışmada kodlama teorisi ile özellikle MDS kodlar ile ilişkilendirilmiş bir gizlilik paylaşım şemasında hileli katılımcılar olduğu zaman bunların hata doğrulama tekniklerinden faydalanılarak tespit edilip kimliklendirildiği gösterilmiştir.

8. Kaynakça

[1] Shamir, " How to share a secret", Communications of the ACM 22 (11) (1979) 612-613.

[2] Blakely, G. R., "Safeguarding cryptography keys", Proc. AFIPS 1979 National Computer Conference, 48, (1979), 313-317.

[3] C.E. Shannon "A Mathematical Theory of Communication" http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf

[4] Arda D., Buluş E., Akgün F., Yerlikaya T., "Secret Sharing Scheme in Cryptographic Key Management Problem", International Scientific Conference UNITECH'08 Gabrovo,2008

[5] Bhondo C., De Santis A., Gargano L., Vaccaro U., "Secret sharing schemes with veto capabilities", In: Proceedings of the First French-Israeli Workshop on Algebraic Coding, LNCS, vol.781, pp. 82-89. Springer-Verlag,1993.

[6] McEliece R. J., Sarwate D. V., "On sharing secrets and Reed Solomon Codes", Comm. ACM 24, 583-584,1981.

[7] Arda D., Buluş E., Yerlikaya T., "MDS Kod tabanlı Kriptografik Gizlilik Paylaşım Şeması, 4. International Information Security&Cryptology Conference ISCTURKEY , Ankara,2010

[8] C. Ding , T. Laihonen , A. Renvall, " Linear Multisecret-Sharing Schemes and Error-Correcting Codes" volume 3, pages 1023-1036, Journal of Universal Computer Science, 1997

[9] RAYMOND H., "A first course in coding theory", Oxford Press, 1996.

[10] ROMAN S., "Coding and Information Theory", Graduate Text in Mathematics, Springer Verlag, 1992.

[11] J.L.Massey, "Some Applications of Code Duality in Cryptography", www.mat.unb.br/~matcont/21_11.ps

[12] Bilgiç H., "Soyut Matematik Ders Notları", Kahramanmaraş Sütçü İmam Üniversitesi, Eylül 2009.

[13] Zorlu Y., " Reed-Solomon Kodların AWGN ve Rayleigh Kanallarda Başarım Analizi", Yüksek Lisans Tezi, Temmuz 2006.

[14] A.A. Bruen, M. A. Forcinito, " Cryptography, Information Theory, and Error-Correction", John Wiley&sons, Inc.,Hoboken, New Jersey, 2005.

LSB Ekleme Yönteminde Bilgi Gizleme İçin Tek Renk Kanal Kullanımının Güvenliğe Etkileri

Emir ÖZTÜRK[1] Andaç ŞAHİN MESUT[2] Altan MESUT[3]

[1,2,3]Bilgisayar Mühendisliği Bölümü, Trakya Üniversitesi, Edirne

[1]e-posta: emirozturk@trakya.edu.tr [2] e-posta: andacs@trakya.edu.tr
[3] e-posta: altanmesut@trakya.edu.tr

Özetçe

Teknolojinin gelişmesiyle birlikte dijital ortamdaki verilerin güvenliğini sağlamak gerekliliği ortaya çıkmıştır. Bilgi güvenliği sağlamak amacıyla genellikle şifreleme teknikleri ve steganografi teknikleri kullanılmaktadır. Bu iki yöntem tek başlarına kullanılabildikleri gibi güvenliği arttırmak amacıyla birlikte de kullanılabilmektedir. Şifrelemede amaç verinin içeriğinin korunması iken steganografinin amacı verinin varlığının gizlenmesidir. Steganografik yöntemler metin, görüntü ve ses dosyalarına uygulanabilmektedir. Bu çalışmada görüntü dosyalarına bilgi gizlemede yaygın olarak kullanılan bir steganografi yöntemi olan LSB yönteminin, 24 bitlik bmp formatındaki bir görüntü üzerinde tüm renk kanalları kullanılmayıp seçilen herhangi bir renk kanalı üzerinde uygulanması incelenmektedir.

Anahtar Kelimeler: Steganografi, Steganaliz, En Önemsiz Bite Ekleme Yöntemi

1. Giriş

Bilgi gizleme yönteminin önemli bir alt disiplini olan Steganografi, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir [1]. Steganografi kelimesi kökleri "στεγανός" ve "γραφειν"'den gelen Yunan alfabesinden türetilmiştir. Tam olarak anlamı "kaplanmış yazı" (covered writing) demektir [2]. Steganografi'nin amacı gizli mesaj ya da bilginin varlığını saklamaktır. Taşınmak istenen mesaj bir başka masum görünüşlü ortamda saklanarak, üçüncü şahısların iletilen mesajın varlığından haberdar olması engellenir. Bu yaklaşımla ses, sayısal resim, video görüntüleri üzerine veri saklanabilir. Görüntü dosyaları içerisine saklanacak veriler metin dosyası olabileceği gibi, herhangi bir görüntü içerisine gizlenmiş başka bir görüntü dosyası da olabilir [3].

Gizli bilgiyi bir resim içine gizleme işleminde iki dosya söz konusudur. Kapak resim ya da örtü verisi (cover image) olarak adlandırılan ilk dosya, gizli bilgiyi saklayacak olan resim dosyasıdır. İkinci dosya ise stego-text adı verilen gizlenecek olan mesajdır. Gizleme işlemi sonucunda kapak resim ve gizli mesajın oluşturduğu dosyaya "stego resim" adı verilir [4].

Görüntü dosyalarına bilgi gizlemek için geliştirilen çeşitli steganografik yöntemleri 3 başlıkta toplamak mümkündür.

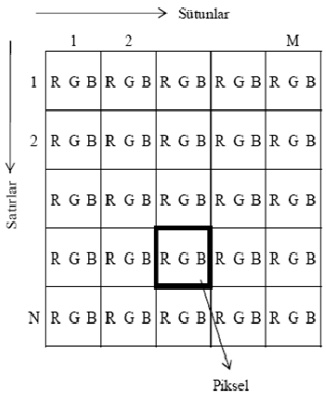
- En önemsiz bite ekleme
- Maskeleme ve filtreleme
- Algoritmalar ve dönüşümler [5].

En önemsiz bite ekleme yönteminde resmi oluşturan her pikselin her byte'nın en önemsiz biti olan son biti değiştirilerek o bitin yerine gizlenmesini istediğimiz verinin bitleri sırasıyla verinin başlangıcından itibaren birer birer yerleştirilmektedir. Bu yöntemde bilgi gizlemek amacıyla sayısal bir resmi oluşturan tüm renk kanalları (Kırmızı, Yeşil, Mavi – Red, Green, Blue) kullanılmaktadır.

Bu çalışmada 24 bitlik bmp formatındaki bir görüntü dosyasında tüm kanallar yerine sadece seçilen bir renk kanalının bilgi gizlenmesi amacıyla kullanılması durumunda bilginin sezilebilirliğinin değişip değişmediği incelenmektedir.

2. Sayısal Resmin Yapısı

Bir sayısal görüntü N satır ve M sütundan oluşan bir dizi şeklindedir. Dizinin her elmanı piksel olarak adlandırılır. En basit görüntülerde piksel değeri 1 veya 0 olabilir. Bu tip görüntülere ikili görüntü adı verilir. Genellikle 24 bitlik görüntüler üzerine veri gizleme işlemi yapılır. 24 bitlik görüntülerde bir piksel başına 3 byte kullanılmaktadır. Her pikselin rengi; Kırmızı (red), Yeşil (green), Mavi (blue) olmak üzere üç ana renkten elde edilmektedir. Buna pikselin RGB değeri denilmektedir [6].



Şekil 1: 24 bitlik renkli sayısal resmin yapısı.

24 bitlik bir görüntüde her renk 0 ile 255 arasında değer alabilen ikili kodlar olarak ifade edilir. Örneğin turkuaz renkli bir pikselin RGB kodu aşağıdaki gibidir.

R = 48 = 00110000
G = 214 = 11010110
B = 200 = 11001000

3. En Önemsiz Bite Ekleme Yöntemi

En önemsiz bite ekleme yöntemi (Least Significant Bit Insertion Methods) yaygın olarak kullanılan ve uygulaması basit bir yöntemdir. Fakat yöntemin dikkatsizce uygulanması durumunda veri kayıpları ortaya çıkmaktadır. Bu yöntemde; resmi oluşturan her pikselin her byte'nın en önemsiz biti olan son biti değiştirilerek o bitin yerine gizlenmesini istediğimiz verinin bitleri sırasıyla verinin başlangıcından itibaren birer birer yerleştirilmektedir. Burada her sekiz bitin en fazla bir biti değişikliğe uğratıldığından ve eğer değişiklik olmuşsa da değişiklik yapılan bitin byte'ın en az anlamlı biti olmasından dolayı, ortaya çıkan stego-resim (= örtü verisi + gömülü veri) değişimler insan tarafından algılanamaz boyutta olmaktadır. Son bite ekleme işlemi resmin başından ya da sonundan olmak üzere sıralı bir şekilde olabileceği gibi, bir rasgele fonksiyon üreteci (random function generator) kullanılarak belirlenen bir piksel üzerinde değişiklik yapılması şeklinde gerçekleştirilebilmektedir.

Bazı steganografik sistemler bazı gizli anahtarlar da kullanabilmektedir. Bu anahtarlar ikiye ayrılırlar:

1. Steganografik anahtarlar; mesajı resmin içine gizleme ve tekrar elde etme işlemini kontrol etme için kullanılırlar.
2. Kriptografik anahtarlar; Mesajın resmin içine gizlenmeden önce şifrelenmesi ve daha sonra deşifrelenmesinde kullanılırlar [7].

4. Steganografik Yöntemin Değerlendirilmesi

Bir steganografik yöntem ya da algoritma değerlendirilirken 3 temel kriter göz önünde bulundurulur. Bunlar

- Kapasite
- Taşıyıcıdaki değişim
- Dayanıklılık'tır.

Taşıyıcıdaki değişimi yada resimdeki bozulma oranının belirlenmesi için çeşitli ölçme yöntemleri vardır. Bunlar arasında en bilinenleri; MSE (Mean Squared Error), RMSE (Root Mean Squared Error) ve PSNR(Peak Signal to Noise Ratio)'dır [8]. MSE hataların kareleri toplamının ortalamasıdır. RMSE ise MSE'nin karekköküdür. Bazen MSE yerine, hatanın büyüklüğünün orijinal piksel değerinin en büyüğü (peak-tepe) ile olan ilişkisi ile ilgilenilir. Bu gibi durumlarda PSNR yöntemi kullanılmaktadır.

Bir steganografik sistemin dayanıklılığını ölçmek için ise steganaliz yöntemleri kullanılmaktadır. Steganaliz, bir örtü verisi (cover data) içerisinde herhangi bir bilgi olup olmadığını bulmayı ve eğer var ise bu bilgiyi elde etmek amacıyla steganografik algoritma kullanılan sisteme karşı yapılan saldırı yöntemleridir [9].

Kapasite kriterinde ise dosya türü önemli rol oynamaktadır.

5. Geliştirilen Uygulama ve Elde Edilen Sonuçlar

Uygulama Visual Studio.Net platformu kullanılarak geliştirilmiştir ve hem tüm kanallara son bite ekleme hem de seçilebilen tek bir renk kanalı üzerinde son bite ekleme yapabilmektedir. Geliştirilen program ayrıca orijinal ve bilgi gizlenmiş resimlerin histogramlarını çıkartabilmekte, resmin bozulma oranlarını ölçebilmekte ve görsel atak uygulayabilmektedir.

Bu yaklaşımın nasıl sonuçlar verdiğini inceleyebilmek amacıyla örnek olarak 4 resim seçilmiştir. Seçilen örnek resimler 24 bitlik bmp formatında görüntülerdir ve şekil 2'de verilmektedir. Daha sonra bu resimlere 3 KByte büyüklüğündeki Türkçe bir metin gizlenmiştir. Gizleme işlemi tüm renk kanallarında ve daha sonra ayrı ayrı renk kanalları üzerinde yapılmıştır. Bilgi gizleme işlemi sonucunda elde edilen bizli gizlenmiş resim dosyalarının sonuna hangi renk kanalının kullanıldığını belirten harfler eklenmiştir.


meyveler.bmp
210x230 piksel


deniz.bmp
210x230 piksel


nehir.bmp
210x230 piksel


çiçek.bmp
210x230 piksel

Şekil 2: Örnek olarak seçinle 24 bitlik bmp resimler

Yöntemi değerlendirebilmek amacıyla bilgi gizlenmiş resimlere sırasıyla bozulma oranlarını hesaplayabilmek için MSE ve PSNR ölçümleri, dayanıklılık kriterini ölçmek amacıyla RS Steganaliz ve Histogram analizi uygulanmış ve elde edilen değerler aşağıda verilmiştir.

PSNR ve MSE ölçümü için her kanal için ayrı hesaplama yapılmıştır. Elde edilen değerler Tablo 1'de verilmektedir. Genel görüş olarak PSNR değerlerinin yüksek MSE değerlerinin düşük olması resimde çok fazla bozulma olmadığını göstermektedir.

Tablo 1'deki değerlerden de görülebileceği gibi bilgi gizleme işlemi için tüm kanalların kullanılması durumunda MSE oranı üç renk kanalına yayılmakta fakat bilgi gizleme için tek renk kanalı kullanılması durumunda bozulma tek renk kanalında olduğu için MSE değeri bozulmanın olduğu renk kanalı için yüksek çıkmaktadır. Aynı durum PSNR değerleri için de geçerlidir. Bu durumda tek kanala gizlemenin kolaylıkla sezilebildiği düşünülebilir. Ancak bozulmayı ölçmek için orijinal resme ihtiyaç duyulduğu ve saldırganın elinde de orijinal resim olmadığı göz önünde bulundurulmalıdır. Genel olarak PSNR değerlerinin yüksek MSE değerlerinin düşük olması dolayısıyla bilgi gizlemek için tüm renk kanallarının kullanılması ya da sadece tek renk kanalının kullanılması durumlarının ikisinde de taşıyıcıdaki değişimin çok olmadığı söylenebilir.

Tablo 1:Bilgi gizlenmiş resimler ve orijinal resim arasındaki bozulma oranları (MSE ve PSNR)

	MSE			PSNR		
	R	G	B	R	G	B
meyveler-rgb.bmp	0.08519669	0.08583851	0.08507247	58.82658	58.79398	58.83291
meyveler-r.bmp	0.2567081	0	0	54.03641	Inf	Inf
meyveler-g.bmp	0	0.2562526	0	Inf	54.04412	Inf
meyveler-b.bmp	0	0	0.2561284	Inf	Inf	54.04623
deniz-rgb.bmp	0.08440994	0.08509317	0.08457557	58.86687	58.83186	58.85835
deniz-r.bmp	0.256853	0	0	54.03396	Inf	Inf
deniz-g.bmp	0	0.2555694	0	Inf	54.05572	Inf
deniz-b.bmp	0	0	0.2558178	Inf	Inf	54.05149
nehir-rgb.bmp	0.08625259	0.08751553	0.08575569	58.77308	58.70995	58.79818
nehir-r.bmp	0.2570393	0	0	54.03081	Inf	Inf
nehir-g.bmp	0	0.2558592	0	Inf	54.05079	Inf
nehir-b.bmp	0	0	0.2559627	Inf	Inf	54.04904
çiçek-rgb.bmp	0.0852795	0.0842443	0.08608696	58.82236	58.8754	58.78143
çiçek-r.bmp	0.2550104	0	0	54.06522	Inf	Inf
çiçek-g.bmp	0	0.2547619	0	Inf	54.06946	Inf
çiçek-b.bmp	0	0	0.253913	Inf	Inf	54.08395

RS Steganalizde her renk kanalı için pikseller gruplara ayrılır. Seçilen maske değerine göre yapılan çeşitli kaydırma işlemleri sonucunda elde edilen değerlerin sıfır ya da sıfıra yakın çıkması o resim dosyasının içinde gizli bilgi olmadığını ya da steganografik algoritmanın çok iyi olduğunu ve bu analize karşı dayanıklı olduğunu göstermektedir. RS Steganalizde kaydırma işlemleri için kullanılan maske değeri daha önce yapılmış olan çalışmalarımız esnasında denenen ve en uygun sonuçları veren maskeler arasından seçilmiştir [10].

Tablo 2,3,4 ve 5'teki değerlere bakıldığında tüm renk kanallarına ya da seçilen bir renk kanalına bilgi gizlenmiş resimlere uygulanan RS steganaliz sonucunda anlamlı kabul edebileceğimiz seviyede farklı değerler elde edilmediği hatta nehir.bmp resminin kırmızı ve yeşil renk kanalı kullanılarak bilgi gizlenmesi sonucunda sıfır değerlerinin elde edilerek en iyi sonuçlara ulaşıldığı görülmüştür.

Bu durumda bilgi gizleme amacıyla tüm kanalların ya da tek bir renk kanalının kullanılmasının RS Steganaliz açısından çok fark etmediği görülmektedir.

Tablo 2: Bilgi gizlenmiş meyveler resmine $M = (0,-1,1,-1)$ kullanılarak elde edilen RS Steganaliz sonuçları

		meyveler-rgb.bmp	meyveler-r.bmp	meyveler-g.bmp	meyveler-b.bmp
R (Kırmızı) renk kanalı için	R	7	12	10	10
	S	7	12	10	10
	U	0	0	0	0
G (Yeşil) renk kanalı için	R	8	5	2	5
	S	8	5	2	5
	U	0	0	0	0
B (Mavi) renk kanalı için	R	20	24	24	8
	S	20	24	24	8
	U	0	0	0	0

Tablo 3: Bilgi gizlenmiş deniz resmine $M = (0,-1,1,-1)$ kullanılarak elde edilen RS Steganaliz sonuçları

		deniz-rgb.bmp	deniz-r.bmp	deniz-g.bmp	deniz-b.bmp
R (Kırmızı) renk kanalı için	R	27	18	27	27
	S	27	18	27	27
	U	0	0	0	0
G (Yeşil) renk kanalı için	R	33	35	20	35
	S	33	35	20	35
	U	0	0	0	0
B (Mavi) renk kanalı için	R	6	16	16	6
	S	6	16	16	6
	U	0	0	0	0

Tablo 4: Bilgi gizlenmiş nehir resmine $M = (0,-1,1,-1)$ kullanılarak elde edilen RS Steganaliz sonuçları

		nehir-rgb.bmp	nehir-r.bmp	nehir-g.bmp	nehir-b.bmp
R (Kırmızı) renk kanalı için	R	2	1	0	0
	S	2	1	0	0
	U	0	0	0	0
G (Yeşil) renk kanalı için	R	2	4	6	4
	S	2	4	6	4
	U	0	0	0	0
B (Mavi) renk kanalı için	R	5	9	9	5
	S	5	9	9	5
	U	0	0	0	0

Tablo 5: Bilgi gizlenmiş çiçek resmine $M = (0,-1,1,-1)$ kullanılarak elde edilen RS Steganaliz sonuçları

		çiçek-rgb.bmp	çiçek-r.bmp	çiçek-g.bmp	çiçek-b.bmp
R (Kırmızı) renk kanalı için	R	0	2	3	3
	S	0	2	3	3
	U	0	0	0	0
G (Yeşil) renk kanalı için	R	7	9	15	9
	S	7	9	15	9
	U	0	0	0	0
B (Mavi) renk kanalı için	R	2	5	5	3
	S	2	5	5	3
	U	0	0	0	0

.

Görsel ataklarda amaç dosyanın içinde veri olup olmadığını belirtmek ve varsa yeri hakkında da bilgi vermektir. Bu saldırı yöntemi Westfeld ve Pfitzmann tarafından geliştirilmiştir [7]. Genellikle LSB üzerinde etkili olan bu saldırı yönteminde amaç resim üzerindeki her pikselin LSB değerini arttırma üzerine kuruludur. Resim ilk pikselden son piksele kadar taranır, sadece son bit değerine göre işlem yapılır. Uygulaması çok basit olmakla beraber karmaşık yüzeylerde anlaşılırlığı zordur.

Meyveler resminin orijinal haline uygulanan görsel atak sonucu şekil 3'te ve bilgi gizlenmiş hallerine uygulanan görsel atak sonucu şekil 4'te gösterilmiştir.

meyveler.bmp

Şekil 3: Orijinal meyveler.bmp resmine uygulanan görsel atak sonucu

meyveler-rgb.bmp

meyveler-r.bmp

meyveler-g.bmp

meyveler-b.bmp

Şekil 4: Bilgi gizlenmiş meyveler resminlerine uygulanan görsel atak sonucu

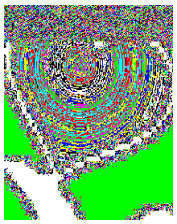
Şekillerden de görüleceği üzere resmin karmaşık yüzeye sahip olmasından dolayı saldırgan kesin bir yargıya varamayacaktır.

Genellikle düz yüzeyli renk geçişleri az olan resimlerde uygulanması daha iyi sonuçlar vermektedir. Bu durumu göstermek amacıyla 210x230 piksel boyutundaki kalp.bmp resmine 3 Kbyte bilgi tüm kanallarına ve seçilen kanalına gizlenmiş ve görsel atak uygulanmıştır. Orijinal resime uygulanan görsel atak sonucu şekil 5'te, bilgi gizlenmiş resimlere uygulanan görsel atak sonuçları ise şekil 6'da gösterilmiştir.

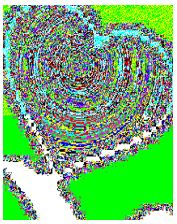
kalp.bmp
210x230 piksel

görsel atak yapılmış hali

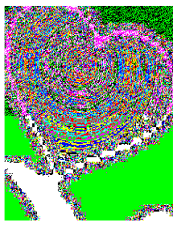
Şekil 5: Orijinal kalp.bmp resmi ve uygulanan görsel atak sonucu



kalp-rgb.bmp



kalp-r.bmp



kalp-g.bmp

kalp-b.bmp

Şekil 6: Bilgi gizlenmiş kalp resimlerine uygulanan görsel atak sonucu

Arka yüzeyin düz ve renk geçişlerinin çok olmadığı bir resim dosyasına yapılan görsel ataklar daha iyi sonuçlar vermektedir. Burada yeşil renk kanalına saklanan bilginin diğer kanallara yada tüm renk kanallarına saklamaya nazaran daha çok sezilebildiği görülebilmektedir.

6. Sonuçlar

Teknolojinin çok hızlı bir şekilde gelişmesi ve internetin hızlanması ve yaygınlaşması neticesinde bilgisayar sistemlerinin güvenliği ve özellikle bilgi güvenliği oldukça önemli bir konu halini almıştır. İnternetin yaygınlaşması sonucunda veri alışverişi ve paylaşımı da artmıştır. Değişik türde verileri içeren farklı tipteki dosyalar dünyanın birçok yerindeki insanlar tarafından paylaşılabilir hale gelmiştir. Bu sayede dijital ortamların içine gönderilmek istenilen bilgilerin gizlenip diğer kişilere aktarılması oldukça kolaylaşmıştır.

Bu çalışmada yaygın olarak kullanılan LSB yönteminde bilgi gizleme amacıyla tüm renk kanallarının değil de seçilen bir renk kanalının kullanılmasının güvenliği nasıl etkilediği incelenmiştir. Bu durum güvenliği negatif yönde etkilememekle birlikte saldırganın işini daha zorlaştırmak amacıyla kolaylıkla uygulanabilir. Saldırganın elinde orijinal resim olmadığı için bilgiyi sezmek ve elde etmek için daha fazla çaba sarf etmesi gerekmektedir. Ayrıca bilgi gizleme işleminin sıralı değil de bir anahtar değere göre rastgele yapılması steganalitik saldırılara karşı daha güçlü olmasını sağlayacaktır.

7. Kaynakça

[1] Petitcolas F.A.P., Anderson R.J., Kuhn M.G., "Information Hiding–A Survey", Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, 87(7):1062-1078, July 1999.

[2] Murray A.H., Burchfiled R.W (eds.), "The Oxford English Dictionary: Being a Corrected Re-issue", Oxford, England: Clarendon Pres, 1933.

[3] Wang H., Wang S., "Cyber Warfare: Steganography vs. Steganalysis", Communications of the ACM, vol. 47, no. 10, October 2004.

[4] Kharrazi M., Sencar H.T., Memon N, "Image Steganography: Concepts and Practice", WSPC/Lecture Notes Series, April 22, 2004.

[5] Sellars D., "An Introduction to Steganography", Student Papers, 1999. http://www.cs.uct.ac.za/courses/CS400W/NIS04/papers99/dsellars/index.html

[6] Morkel T., Eloff J.H.P., Olivier M.S., "An Overview of Image Steganography", Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005/

[7] Westfeld A., Pfitzmann A., "Attacks on Steganographic Systems", Information Hiding. Third International Workshop, IH'99, Dresden, Germany, September/October, 1999, Proceedings, LNCS 1768, Springer-Verlag Berlin Heidelberg 2000. 70.

[8] Sayood K.: "Introduction to Data Compression", Morgan Kauffman Publishers, Inc. 340 Pine Street, Sixth Floor, San Francisco, CA 94104-3205, USA, 1996. 61.

[9] Phan R.C.W., Ling H.C., "Steganalysis of Random LSB Insertion Using Discrete Logarithms Proposed At Cıta03", M2USIC03, PJ, Malaysia, 2-3 October 2003.

[10] Şahin A., Buluş E.,Buluş H.N., Sakallı M.T., "24-bit Renkli Resimler Üzerine Uygulanan RS Steganalizde Maske Seçimlerinin Etkileri" Elektrik Elektronik Bilgisayar Mühendisliği Sempozyumu (ELECO 2006), Bursa-TÜRKİYE, Aralık-2006.

Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği

Mehmet Kara[1] Soner Çelikkol[2]

[1]TÜBİTAK BİLGEM UEKAE, Kocaeli
[2]Kullar Meslek Yüksek Okulu, Kocaeli Üniversitesi, Kocaeli
[1]e-posta: mkara@uekae.tubitak.gov.tr, [2]e-posta: scelikkol@kocaeli.edu.tr

Özetçe

Elektrik üretim ve dağıtım sistemleri ülkedeki önemli kritik altyapılardan biridir. Bu altyapıların daha kolay ve etkin yönetim için büyük ölçüde SCADA sistemleri kullanılmaktadır. Günümüzde SCADA sistemlerinin internet protokollerini yaygın olarak kullanmaya başlaması siber güvenlik tehditlerine varabilecek tehditleri de beraberinde getirmektedir. Çünkü bir ülkenin veya bir bölgenin kısa bir süreliğine bile elektriğinin kesilmesi çok ciddi sonuçlar doğurabilir. Bu makalede SCADA sistemlerinin genel yapısı iletişim protokolleri ele alınmış, enerji iletim ve dağıtım altyapılarında kullanılan SCADA sistemlerinin güvenli çalışması için alınması gereken önlemler vurgulanarak, Türkiye'deki durum irdelenmiştir.

1. Giriş

Kritik altyapılar, bir ülkede ekonomi ve sosyal hayatın sağlıklı bir şekilde işlemesi için ciddi öneme sahip olan fiziksel ve sayısal sistemler olarak tanımlanmıştır. Enerji üretim ve dağıtım sistemleri de önemli kritik altyapıların başında gelmektedir. Geçmiş senelerde, kritik altyapılar fiziksel ve mantıksal olarak değerlendirildiğinde güvenlik denildiğinde daha çok fiziksel güvenliğe önem verilmiştir. Fakat bilgi teknolojilerindeki gelişmeler hem altyapıları hem de altyapılar arasındaki ilişkileri ve bağımlılığı etkilediği için bu sistemlerin fiziksel güvenlik yanında mantıksal güvenliği de ön plana çıkmıştır. Çünkü günümüzde kritik altyapı BT (Bilgi Teknolojileri) sistemleri genellikle bilgisayar sistemleri ile kontrol edilmekte ve izlenmektedir. Bilgisayar sistemleri de TCP/IP protokol ailesini kullandığı için internete bağlı olsa da olmasa da güvenlik riskleriyle karşı karşıyadır.

Kritik altyapı kavramının ortaya çıkmasının en önemli nedeni bilgi teknolojilerinin yaygın bir şekilde kullanılmasıdır [1]. Kritik altyapılar ve bilgi teknolojileri birçok yönden, ciddi şekilde kesişmektedir. Bu kesişimler bilgi teknolojilerinin önemini çok açık bir şekilde göstermektedir. Bu önem, "kritik bilgi altyapıları" teriminin ortaya çıkmasına yol açmıştır. OECD (Organisation for Economic Co-operation and Development) kritik bilgi altyapılarını, fonksiyonelliğini yitirmesi durumunda sağlık hizmetlerine, toplumsal emniyet ve güvenliğe, vatandaşların ekonomik refahına veya hükümetin/ekonominin verimli çalışmasına ciddi yönde tesir eden bilgi ağları ve sistemleri olarak tanımlamaktadır [2].

2. Elektrik Üretim ve Dağıtım Sistemlerinin Otomasyonu

Günümüzde enerji üretim ve dağıtımının kontrolü, su, doğal gaz, kanalizasyon sistemleri gibi kritik altyapıların kontrol edilmesi ve izlenmesini de sağlayan SCADA (Supervisory Control And Data Acquisition) sistemleri tarafından yapılmaktadır. Bu sistemlerin büyük bir bölümü bilgi ve iletişim teknolojilerinden oluşmaktadır.

Prosesler için gözetleyici denetim ve veri toplama anlamına gelen SCADA uygulaması ilk olarak 1960'lı yıllarda Kuzey Amerika'da hayata geçirilmiştir. İlk yıllarda, SCADA sistemlerinin kurulum ve bakım maliyetleri oldukça yüksek olmasına karşın, teknolojideki gelişmeler hem bu sistemlerin maliyetlerini düşürmüş hem de sistemin işletilmesi için gerekli olan iş gücü gereksinimini azaltmıştır. Bunun sonucu olarak da daha çok tercih edilir hale gelmiştir [3].

Mimari yapı olarak SCADA'yı birinci nesil monolitik, ikinci nesil dağıtık (distributed) ve üçüncü nesil ağ tabanlı (networked) olarak üç nesle ayırmak mümkündür. Birinci nesil sistemlerde ağ yapısı mevcut değildir uzak terminal birimleriyle haberleşmeler özel protokollerle yapılmaktadır. Ayrıca bu tür sistemlerde yedeklemede bulunmamaktadır.

İkinci nesil SCADA sistemlerinde; bilgiyi gerçek zamanlı paylaşan ve LAN(Local Area Network) ile birbirlerine bağlanan çoklu istasyonlar kullanılmıştır.

Üçüncü nesil olarak günümüzde kullanılan ağ tabanlı SCADA sistemleri, RTU (Remote Terminal Unit) imalatçılarına ait özel protokoller yerine açık sistem mimarisini daha çok kullanmaktadır. Bu nesil SCADA sistemlerinin kullandığı açık sistem protokolleri, LAN'dan daha ziyade WAN üzerinden fonksiyonel olarak kullanılmaktadır. Açık mimaride yazıcılar, disk sistemleri, veri kaydediciler gibi üçüncü

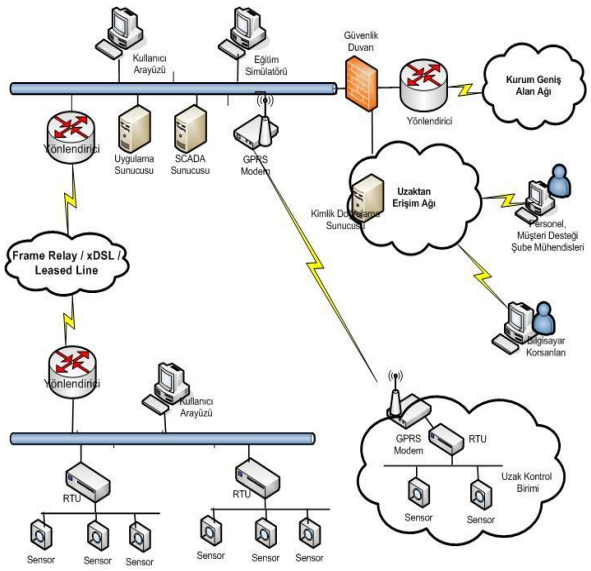
parti çevre aygıtlar sisteme daha kolay bağlanabilmektedir. WAN protokolleri (IP ve benzeri) sunucuyla iletişim ekipmanları arasındaki iletişimi sağlamaktadır. Diğer yandan bu SCADA sistemlerinin siber savaşlara ve siber terörist girişimlere açık olması gibi bir güvenlik sorununu gündeme getirdiği de aşikârdır [4].

2.1. SCADA Sunucuları

Geniş bir alana yayılmış uzak terminal birimlerinin koordineli çalışması, uzak terminal birimlerinden gelen bilgilerin yorumlanarak kullanıcılara sunulması, kullanıcıların isteklerinin uzak terminal birimlerine iletilerek kumanda fonksiyonlarının sağlanması, diğer yazılım katmanları ile entegrasyonunu SCADA sisteminde merkezi yönetim birimi yerine getirmektedir. Merkezi yönetim birimi, uzak terminal birimlerinden bilgileri alır, istenilen bilgileri düzenli olarak kayıt eder, verileri değerlendirerek operatörlerin algılayacağı sesli ve görüntülü şekle dönüştürür. Merkezi yönetim birimi; sunucu, bilgisayar destekli paket uygulamaları, insan makine iletişimi için arayüzler, ağ anahtarları, yönlendiriciler, yazıcılar, modemler, iş letme fonksiyonlarını yerine getirecek yazılımlar ve destek donanımlarından oluşur. Küçük SCADA sistemlerinde merkezi terminal birimi tek bir PC'den oluşabilir. Buna karşın daha büyük SCADA sistemleri çoklu sunucular, dağıtılmış yazılımlar ve yedekleme birimlerinden oluşur. Herhangi bir sunucu arızasında izleme ve kontrol faaliyetlerinin sürekliliğini sağlayarak sistemin bütünlüğünü artırmak için; aktif yedekleme yapısında aktif-aktif şeklinde yapılandırılan çoklu sunucular kullanılmaktadır.

2.2. Uzak Terminal Birimleri (RTU)

Uzak terminal birimleri fiziksel saha ekipmanları ile bağlantıyı sağlarlar. RTU'lar sistemdeki yerel ölçüm ve kumanda noktaları ile haberleşerek ya da I/O (giriş/çıkış) terminalleri yardımıyla yerel ekipmanlardan gelen sinyalleri değerlendirdikten sonra haberleşme hattı üzerinden merkezi terminal birimine bilgi verirler. RTU'lar aynı şekilde merkezi terminal biriminden gönderilen komutları değerlendirdikten sonra sahadaki ekipmanlara kumanda sinyalleri gönderirler. Sistemdeki röle, enerji analizörü, sayaç gibi cihazlarla RTU'lar haberleşerek, akım, gerilim, güç, tüketim gibi elektriksel bilgileri doğrudan alırlar. Aynı şekilde kesici, şalter, yük ayırıcı, solenoid gibi kumanda edilebilir ekipmanları kumanda ederler. Haberleşme imkanı olmayan saha ekipmanlarından bilgileri I/O modülleri vasıtasıyla alırlar. Sahadan gelen sonuçlar, cihazların çalışma durumları ve operatör tarafından girilen komutlar RTU tarafından saha ekipmanlarına iletilir. RTU'ların programlanabilir cihazlar olması sebebiyle merkez istasyonu üzerindeki iş lem yükünün bir kısmını üzerine alarak sistem veriminin ve performansının artmasını sağlamaktadır. RTU'lar tüm alternatifleri değerlendirmek suretiyle merkezi terminal birimine bilgi vermeksizin alarm uyarıları üretebilir ve bu durumlarda ne yapılacağına anında kendileri karar vererek yerinde müdahaleler yapabilirler. Merkezi terminal birimine sadece olayın sonucunu aktarırlar. Tipik bir SCADA sistemi ağ topolojisi Şekil 1'de görülmektedir.



Şekil 1: SCADA sistemi genel ağ topolojisi

3. İletişim Ağı

İletişim, SCADA sistemlerinin omurgasını teşkil eder. Merkezi terminal biriminin uzak bölgelerde bulunan çeşitli RTU, bilgisayar veya sistemlerle bilgi alış verişi yapması için bir iletişim hattının olması gerekir. İletişim hatlarını kablolu ve kablosuz iletişim olmak üzere iki gruba ayırmak mümkündür. Büyük SCADA uygulamalarında kablolu ve kablosuz iletişim hatlarından oluşan karma bir yapı söz konusu olabilmektedir. Direk kablo bağlantısı geniş coğrafyaya yayılmış büyük sistemler için uygulamada birtakım sorunları da beraberinde getirmektedir. Direk kablo bağlantısının mümkün olduğu kritik uygulamalarda fiber optik kablo teknolojisi, daha yüksek veri transferi ve arttırılmış güvenlik sağlaması yönünden tercih edilir. Direk kablo bağlantısının mümkün olmadığı durumlarda diğer kurumlardan hat kiralamak (Leased-line, ADSL, DSL

gibi), radyo frekans (RF), uydu iletiş im, GSM, GPRS, 3G hatlarını kullanmak iyi bir çözüm yoludur.

SCADA sistemlerinin güvenilirliğ ini ve performansını etkilemede iletişim ağ ının çok büyük rolü vardır. İletiş im ağ ı seçilirken iletişim hızı, güvenilirlik, maliyet gibi parametrelerin göz önünde bulundurularak titiz bir çalış madan sonra karar verilmesi gerekir. Bazı kritik SCADA projelerinde iletişimin sürekliliğ ini sağ lamak için yedek iletiş im hatları kullanılmaktadır. Ana haberleş me hattında bir sıkıntı olması durumunda yedek olarak bekleyen hat otomatik devreye girmektedir. Ana haberleşme hattının ve yedek hattın farklı tipte olması tercih edilir (ADSL-RF, RF-GPRS, Fiber Optik-RF gibi). [4]

4. SCADA Protokol Tipleri

Protokol; iletiş im hattı üzerinden veri alış verişinin formatını, zamanlamasını, önceliğ ini ve denetimini tanımlayan bir dizi kurallar kümesidir. Eğ er protokol iyi tasarlanmamış sa iletiş im hattı ne kadar esnek ve hızlı olursa olsun haberleşmede trafik tıkanıklığ ı ve emniyet zafiyeti ihtimali vardır. Özellikle kritik altyapılar gibi gerçek zamanda işlem yapılan uygulamalarda uzak terminal birimlerinden gelen alarm, uyarı mesajları, hızlı değ iş ime uğ rayan fiziksel veriler iletişim yolunun tıkanmasına sebep olabilir. SCADA sisteminde kullanılan iletiş im hattına bağ lı olarak kullanılan RTU ve dağ ıtılmış saha ekipmanları arasında değ iş ik haberleşme protokolleri kullanılabilmektedir. Modbus RTU, RP-570, Profi-Bus, Can-Bus gibi haberleş me protokollerini günümüzde birçok SCADA programları desteklemektedir. Günümüzde IEC60870-5-101, IEC 60870-5-104, IEC870-6, IEC 61850 ve DNP3 gibi açık iletiş im protokolleri SCADA ekipman üreticileri ve çözüm ortakları arasında giderek daha popüler olmaktadır [5].

5. Elektrik Altyapısının Güvenliği İçin Teknik ve Yönetimsel Uygulamalar

İlk geliştirilen SCADA sistemleri hem üreticiye özel protokoller kullandığı hem de diğer ağlarla bağlanmadığı için daha çok fonksiyonellik ön plana çıkmış, çok fazla güvenlik özelliği eklenmemiştir. Fakat süreç içerisinde SCADA sistemleri için standart protokollerin yaygınlaşması sistemlerin internet ya da kapalı bilgisayar ağaları üzerinden kontrol edilmesi güvenlik risklerini de artırmaya başlamıştır. Bu riskler SCADA sisteminin internete bağlılık düzeyine göre artmaktadır. Bazı kurumlar SCADA sistemlerinin internete bağlı olmadığını öne sürerek güvenli olduklarını düşünmektedir. Siber atakların arttığı günümüzde Stuxnet zararlı yazılımı bunun doğru olmadığını açıkça göstermiştir. İran nükleer araştırmalarının yapıldığı sistemler internete bağlı olmamasına karşın Stuxnet zararlı yazılımı sisteme bulaşmıştır [11]. Daha önceki yıllarda da birçok kritik altyapının bilgi sistemlerine saldırı yapılmış ve çok ciddi zararlar verilmiştir. Son yıllarda özellikle siber savunma kapsamında kritik altyapılara bilgisayar sistemleri aracılığıyla saldırılar geçekleştirilmektedir.

Kritik altyapılarda kullanılan BT sistemlerinin güvenliğinin ön plana çıkmasıyla birlikte hem teknik hem de yönetimsel güvenlik önlemleri alınmaya başlanmıştır. Bu sistemler ülke için kritik öneme sahip olduğundan kurumun alacağı önlemler yanında Kritik altyapıları işleten kurumların çalışmalarını düzenleyen ve denetleyen kurumlar tarafından gerekli düzenlemeler yapılmaktadır. Örneğin ülkemizde faaliyet gösteren bankalar için BDDK (Bankacılık Düzeleme ve Denetleme Kurumu) düzenleme ve denetleme yapmaktadır. Bu çerçevede BDDK bankaların bilgi sistemlerinde almaları gereken önlemleri yayınlamıştır[13]. Sonrasında da her yıl periyodik olarak yapılan güvenlik testlerin sonuçlarını inceleyerek. Bankaların güvenliğini kontrol etmektedir. Aynı şekilde GSM operatörlerini, internet servis sağlayıcıları, elektronik sertifika hizmet sağlayıcıları düzenleyen ve denetleyen Bilgi Teknolojileri ve İletişim Kurumu bilgi sistemleri güvenliği konusunda düzenlemeler yapmaktadır. Benzer düzenlemeleri elektrik üretim ve dağıtım sistemleri, metrolar, hava limanları, hastaneler gibi kritik altyapıları düzenleyen ve denetleyen kurumların yapması gerekmektedir. Yurt dışında birçok ülkede kritik altyapıları düzenleyen ve denetleyen kurumlar altyapı BT sistemlerin güvenli hale getirilmesi için direktifler ve kılavuzlar yayınlamaktadır.

İngiltere'de kritik altyapıların güvenliği konularında çalışma yapan CPNI (Center for Protection of National Infrastructure) proses kontrol ve SCADA sistemlerin güvenliği konusunda bir rehber yayınlamıştır. Yayınlanan rehberde aşağıdaki güvenlik önlemelerinin alınması tavsiye edilmiştir[6].

- İş risklerinin anlaşılması
- Güvenli mimarinin gerçeklenmesi
- Olayları ele alma yeteneğinin oluşturulması
- Farkındalığın artırılması ve yeteneklerin geliştirilmesi
- Üçüncü parti risklerin yönetimi
- Projelerin güvenlikle birlikte ele alınması
- Sürekli bir yönetişim modelinin kurulması

Ayrıca CPNI tarafından yayınlanan rehberde ABD, Kanada, Avustralya ve Avrupa Birliği ile bu konularda bilgi paylaşıldığı ifade edilmiştir.

2006 yılında NERC (North America Electric Reliability Concuil) ABD'de elektrik alt yapılarının

güvenli hale getirilmesi için elektrik sistemi üretim ve dağıtımdaki taraflara siber güvenlik standartları gerçekleme planını yayınlamıştır. 2010 yılı sonuna kadar bütün elektrik üretim, dağıtımı yapan kurumların, olası siber ataklara karşı, BT altyapı güvenliklerini denetlenebilir bir seviye getirmeleri istenmiştir. Yıllar içerisinde alınması gereken önlemleri belirtilmiştir [7].

NERC tarafından elektrik üreten ya da ileten kuruluşların almaları gereken güvenlik önlemleri aşağıda belirtilmiştir:

5.1. Kritik Siber Varlıkların Tanımlanması

Söz konusu kurum yönlendirme yapan, yönlendirme tablosu barındıran, uzaktan erişilebilen kritik altyapıların envanterini oluşturacaklar ve bunları düzenli olarak güncelleyeceklerdir.

5.2. Güvenlik Yönetim Kontrolleri

Siber Güvenlik Politikası: İlgili kurum, yönetimin katılımını ve kritik varlıkların güvenliğini içeren siber güvenlik politikasını yazmalı ve gerçeklemelidir. Bu politika ilgili herkes tarafından bilinmeli ve her yıl üst yönetim tarafından gözden geçirilip güncellenmelidir.

Bilginin Koruması: Ağ topolojisi, kritik BT varlıkları içeren binanın kat planları, siber güvenlik varlıklarının resimleri, felaketten kurtarma planları, olay müdahale planları, güvenlik yapılandırmaları gibi sisteme ait bilgiler ve saklandığı ortamlar korunmalıdır. Kritik altyapılardaki bilgiler sınıflandırılmalıdır. İlgili kurum kritik varlık bilgi koruma planının uyguluğunu her yıl değerlendirmeli ve bulunan eksiklikler için yapılacakları belirlemelidir.

Erişim Kontrolü: İlgili kurum, kritik siber varlık bilgilerini korumak için bu varlıklara erişimi denetim altına almalıdır. Yetkili erişim için isim, unvan ve diğer bilgileri tanımlanmalı. Her yıl erişim yetkileri gözden geçirilmeli. Yetkili kurum korunacak bilgiye erişim yapanların listesini her yıl gözden geçirip yeniden düzenlemelidir.

Değişim Kontrolü ve Konfigürasyon Yönetimi: İlgili kurum, kritik siber yazılım ve donanım varlıklarının değiştirilmesi, sisteme eklenmesi, sistemden çıkarılması, konfigürasyonunun değiştirilmesini sağlayacak değişim kontrol ve konfigürasyon yönetim sürecini oluşturmalı ve dokümante etmelidir. Aynı zamanda kritik siber varlıklara ait üretici ve satıcı değişikliklerini de izlemelidir.

5.3. Personel ve Eğitim

Farkındalık: İlgili kurum, personellerine siber ve fiziksel ortamlara yetkisiz erişim riskleri konusunda bilgilendirecek program oluşturmalı, dokümante etmeli ve güncellemelidir. Program her bir dört ayda eposta, hatırlatma notu, bilgisayar destekli eğitim, poster, intranet, broşür, sunu, toplantı gibi yollarla personeli bilgilendirmelidir.

Eğitim: İlgili kurum personellerine siber ve fiziksel ortama yetkisiz erişim riskleri konusunda eğitim programı oluşturmalı, dokümate etmeli ve gerçekleştirmelidir.

Bu eğitim kritik varlıklara erişim yapacak satıcı, teknik servis personellerine verilmelidir. Bu eğitimler politikalar, erişim kontrolleri ve prosedürleri içermelidir. Uygun rol ve sorumluluklar için minimum aşağıdaki eğitimler verilmelidir:

- Kritik siber varlıkların uygun kullanımı
- Kritik siber varlıklara fiziksel ve elektronik erişim kontrolü
- Kritik siber varlık bilgilerinin ele alınması
- Siber güvenlik olayı durumunda neler yapılacağının belirlenmesi

5.4. Elektronik Sınır Güvenliği

İlgili kurum tüm kritik varlıkların sınır güvenliği içinde kalmasını sağlamalı, sınır güvenliği ve ona olana erişim noktalarını tanımlamalı ve dokümante etmelidir.

İlgili kurum sınır güvenliği cihazlarına yapılacak elektronik erişimleri kontrol altına almalıdır. Sınır güvenliğinde kullanılan varlıklarda sadece ilgili portları ve servisleri çalıştırmalıdır.

Sınır güvenliği cihazlarına yapılan erişimleri izlemeli ve bu erişimlere ait kayıtları yedi gün 24 saat tutulmalı ve düzenlemelerin gerektirdiği süre kadar saklamalıdır.

İlgili kurum yılda en az bir defa sınır güvenliği cihazlarına açıklık analizi yapmalıdır.

İlgili kurum yasalara ve düzenlemelere uygun sistemi gerçekleyebilmek için gerekli tüm dokümantasyonu gözden geçirmeli ve güncellemelidir.

5.5. Sistem Güvenlik Yönetimi

Elektronik sınır güvenliğine yeni eklenen ve var olan siber varlıklarda yapılan değişiklikler siber güvenliği zayıflatmamalıdır. Bu kapsamda güvenlik yamaları, servis paketleri, satıcı sürümleri, işletim sistemi güncellemeleri, uygulamalar, veritabanları, üçüncü parti bellenimler dikkatli uygulanmalıdır.

Bu kapsamda ilgili kurum siber güvenlik test prosedürleri tanımlamalı, gerçeklemeli ve güncellemelidir. Yapılan testler gerçek ortamı simüle etmeli testlere ait sonuçları kayıt altına almalıdır.

İlgili kurum sadece normal işlemlerde ve acil durumlarda gerekecek portları açık tutmalıdır. Elektronik sınır güvenliğinde bulunan cihazlardaki

diğer tüm portlar kapatılmalıdır. İlgili kurum teknik nedenlerden dolayı kapatılmayan portlar veya servisler için risk azaltıcı önlemler almalı ve bunları dokümante etmelidir.

Elektronik sınır güvenliği sisteminde bulunan kritik siber varlıklara ait yamaların izlenmesi, değerlendirilmesi, testi ve yamaların yapılması için program oluşturmalıdır.

İlgili kurum antivirüs veya zararlı yazılım önleme araçlarını kullanmalıdır. Zararlı yazılım imza güncellemeleri için prosedür oluşturmalıdır.

İlgili kurum elektronik sınır güvenliği içindeki siber varlıkların siber güvenlikle ilgili olaylarının izlenmesi için gerekli izleme sistemini oluşturmalıdır. Bu sistemler güvenlik olayı olduğunda otomatik veya manuel alarm oluşturmalıdır. Oluşturulan bir kayıt yasalar ya da düzenleyici kurumun öngördüğü süre kadar saklamalıdır.

İlgili kurum elektronik sınır güvenliği varlıkları için yılda en az bir defa siber açıklık analizi yapmalıdır. Bu analizde açık değerlendirme süreci dokümante edilmeli, sadece gerekli olan servis ve portların çalıştığı kontrol edilmeli, varsayılan kullanıcı hesapları kontrol edilmelidir. Açıklık analizi sonucunda, ortaya çıkan açıkları, açıklıkları ortadan kaldırmak veya azaltmak için alınacak önlemleri dokümante etmelidir.

5.6. Olay Raporlama ve Olay Müdahale Planlama

Siber Güvenlik Olay Müdahale Planı: İlgili kuruluş siber güvenlik olay müdahale planı oluşturmalı ve sürdürmeli. Bu plan minimum aşağıdakileri içermelidir.

- Siber güvenlik olaylarını raporlanabilir ve sınıflandırılmış şekilde karakterize edecek prosedürler
- Müdahale takımındaki rol ve sorumluluklar, müdahale eylemleri, olay ele alma prosedürleri ve haberleşme planları
- Siber güvenlik olayını elektrik sektöründeki CERT ile paylaşabilecek süreç
- Herhangi bir değişiklik olması durumunda bu değişikliği plana belirli süre içinde yansıtma
- Siber güvenlik olayı ele alma prosesini yılda bir defa gözden geçirme
- Siber güvenlik olayı ele alma planını yılda en az bir defa test etme

6. Türkiye Elektrik İletim Altyapısı Kontrol Sistemi

Elektrik üretim ve dağıtım sistemlerinde SCADA/EMS sistemlerine geçilmesi çalışmaları 1980'lerin ortalarında başlamıştır. Hala yenileme ve güncelleme çalışmaları devam etmektedir. Bu çerçevede sistem kolay yönetilebilir ve izlenebilir hale gelmiştir. Elektrik üretim ve dağıtım sistemlerinin BT altyapısı ile ilgili güncel bilgilerin büyük bir bölümü TEİAŞ 2010 yılı faaliyet raporundan alınmıştır [8].

Tüm elektrik altyapısı sisteminin kontrolü Ankara Gölbaşı'nda bulunan Ulusal kontrol merkezinden yapılmaktadır. Bu merkez Genel Müdürlük binasında bulunan Acil Durum Kontrol Merkezi ile yedeklenmektedir. Hali hazırda Adapazarı, Gölbaşı, İzmir, Keban, İkitelli, Keban Samsun olmak üzere 6 adet bölgesel kontrol merkezi bulunmaktadır. Bölge kontrol merkezleri de elektrik üretim testilerinden aldıkları bilgileri ulusal kontrol merkezine iletmektedir.

2010 yılı itibari ile 235 trafo merkezi ve santral, Merkezi Kontrol Sistemine bağlanmıştır. SCADA Sistemi kapsamında uzaktan kumanda fonksiyonu pilot uygulama olarak 12 istasyonda gerçekleştirilmiş bulunmaktadır [8, 10].

EÜAŞ'a bağlı 51 Hidrolik santral, 20 Termik santral bulunmaktadır. Bunların dışında elektrik üreten birçok kurum ve kuruluştan da elektrik alınmaktadır [9].

Avrupa Elektrik Sistemine (ENTSO-E) bağlantı çalışmaları devam etmektedir. Bu çerçevede Komu ülkeler Yunanistan Bulgaristan ve ENTSO-E Güney Koordinasyon Merkezi (Swiss-Grid-İsviçre) bağlantıları gerçekleştirilmiş veri tabanlarında gerekli tanımlamalar yapılmıştır. Mısır, Irak, Ürdün, Libya, Lübnan, Filistin, Suriye ve Türkiye elektrik sistemlerinin eterkonneksiyonu konusunda çalışmalar da devam etmektedir.

Smart Grid konusunda İspanya'nın Mercados firmasından alınan danışmanlık projesi kapsamında çalışmalar devam etmektedir. Dünyada da bu konuda çok sayıda araştırma yapılmaktadır.

720 yerde bulunan 300 civarındaki sayacın uzaktan okunması için çalışmalar sürmektedir. Sayaçlardan okunan bilgiler GPRS ile taşınması için bir GSM operatörü ile anlaşılmıştır.

Amacı "elektriğin yeterli, kaliteli, sürekli, düşük maliyetli ve çevreyle uyumlu bir şekilde tüketicilerin kullanımına sunulması için, rekabet ortamında özel hukuk hükümlerine göre faaliyet gösterebilecek, mali açıdan güçlü, istikrarlı ve şeffaf bir elektrik enerjisi piyasasının oluşturulması ve bu piyasada bağımsız bir düzenleme ve denetimin sağlanması" olan EPDK'nın (Enerji Piyasası Düzenleme Kurumu) elektriğin sürekli sağlanması için düzenleme ve denetleme yetkisi bulunmaktadır. Elektrik üretim ve iletim sistemlerinin kontrol ve izlemesinde de kullanılan SCADA sistemlerinin güvenliğinin sağlanması için düzenlemeler yapıp, sistemlerin düzenli olarak denetlenmesi sağlanmalıdır.

Elektrik Piyasası Şebeke Yönetmenliği'nde TEİŞ ile kullanıcı arasında arasındaki hattın yedekliliğinden bahsedilmiş [12]. Fakat güvenlik olayları ayrıntılı ele alınmamıştır. İletişim ağı güvenlik kriterleri tanımlanmalı, uygulanmalı ve ilgili kurumlar tarafından denetlenmelidir.

7. Sonuç ve Öneriler

Elektrik üretim ve dağıtım sistemleri en önemli kritik alt yapılar arasında yer almaktadır. Dünyadaki gelişmelere paralel olarak ülkemizde de enerji sistemlerinin altyapı yönetimi ve izlenmesi büyük oranda BT teknolojileri ile bütünleşen SCADA sistemleri ile yapılmaktadır. SCADA sistemlerinin BT sistemleri ile bütünleşmesi birçok kolaylık ve esneklik sağlaması yanında ciddi güvenlik risklerini de beraberinde getirmektedir. Birçok ülke bu risklerin kapatılması veya seviyelerinin düşürülmesi için yönetimsel, teknik önlemler almakta ve yasal düzenlemeler yapmaktadır.

Enerji sistemlerinin kesintisiz, güvenli ve istenilen kalitede hizmet vermesi tüm ülkemizi yakından ilgilendirmektedir. Bu çerçevede dünyadaki birçok ülkede olduğu gibi ülkemizde de enerji üretim ve dağıtım sistemlerinin SCADA güvenliğinin sağlanması için gerekli düzenleme ve denetim mekanizmaları oluşturulup uygulanmalıdır.

8. Kaynaklar

[1] USA Presidential Decision Directive/NCS-63, "http://www.fas.org/irp/offdocs/pdd/pdd-63.htm", 1998 (25 Ocak 2011 erişilebilir durumda)

[2] OECD, Working Party on Information Security and Privacy, "Recommendations of the Council on the Protection of Critical Information Infrastructures", Ocak 2008

[3] http://www.dpstele.com/dpsnews/techinfo/scada/scada_knowledge_base.php, (25 Ocak 2011 erişilebilir durumda)

[4] Ten C., Liu C., Manimaran G., "*Vulnerability Assessment of Cybersecurity for SCADA Systems*", IEEE Transactions On Power Systems, Vol. 23, No. 4, 2008

[5] Kalapatapu R., *SCADA Protocols And Communication Trends,* ISA2004 Paper, http://www.isa.org/journals/intech/TP04ISA048.pdf (25 Ocak 2011 erişilebilir durumda)

[6] http://www.cpni.gov.uk/protectingyourassets/scada.aspx (25 Ocak 2011 erişilebilir durumda)

[7] http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf (25 Ocak 2011 erişilebilir durumda)

[8] http://www.teias.gov.tr/Faaliyet2010/TEIASfaaliyetraporu%20TURKCE.pdf (10 Ağustos 2011 erişilebilir durumda)

[9] http://www.teias.gov.tr/projeksiyon/KAPASITEPROJEKSIYONU2009.pdf (25 Ocak 2011 erişilebilir durumda)

[10] http://www.teias.gov.tr/TEIAS_Strtj_2011.pdf (10 Ağustos 2011 erişilebilir durumda)

[11] http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/zararli-yazilimlarin-yeni-hedefi-hangi-kritik-altyapi-sistemleri-olacak.html (10 Ağustos 2011 erişilebilir durumda)

[12] Elektrik Piyasası Şebeke Yönetmeliği, http://www.epdk.gov.tr/web/elektrik-piyasasi-dairesi/24 (10 Ağustos 2011 erişilebilir durumda)

[13] Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ, http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2007/09/20070914.htm&main=http://www.resmigazete.gov.tr/eskiler/2007/09/20070914.htm (6 Eylül 2011 erişilebilir durumda)

Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği

Volkan Evrin [1, 2] Mehmet Demirer [1, 3]

[1] Bilişim Hukuku Tezsiz Yüksek Lisans Programı, Hacettepe Üniversitesi, Ankara
[2] Bilgi Teknolojileri Direktörlüğü, KAREL Elektronik A.Ş., Ankara
[3] Elektrik-Elektronik Mühendisliği Bölümü, Hacettepe Üniversitesi, Ankara

[1] e-posta: volkan@evrin.net [2] e-posta: mehmet@hacettepe.edu.tr

Özetçe

Kurumların faaliyet konularında Bilgi Güvenliği başlığı ile karşılaştıkları sorunlarda süreç yönetimi yapılarından faydalanmaları artık doğal bir sonuç haline gelmiştir. Her kurumun kendi faaliyet alanına ve çalışma kültürüne uygun bir süreci seçmesi ve onun gereklerini yerine getirerek bu çalışmalarını sertifikalandırması mümkündür.

Finans ve savunma sanayisi gibi özel konular dışında kalan sağlık, haberleşme, üretim, Ar-Ge vb. pek çok sektör için ISO/IEC 27000 ailesi, Bilgi Güvenliği Yönetim Sistemi olarak genel kabul gören süreç yönetimidir. Kurumların bu süreç yönetimini bünyelerinde uygulamaları ve ISO/IEC 27001 çalışmalarını tamamlayarak belgelendirmeleri, iyi bir planlama, kapsam belirleme, risk analizi ve varlık değerlendirmesi sonucunda olmaktadır.

Bilgi Güvenliği Yönetim Sistemi, sadece bir belgelendirme değil, aynı zamanda kurumlar için çalışma kültürü haline gelmesi gereken bir süreç yönetimidir.

Anahtar Sözcükler: ISO/IEC 27000 Standart Ailesi, ISO/IEC 27001, Bilgi Güvenliği Yönetim Sistemi, BGYS, Süreç Yönetimi, Bilişim Hukuku

1. Giriş

Dünya tarihi büyük devrimlerin, keşiflerin ya da bilimsel olayların açtığı ve kapadığı çağlarla bölümlendirilmektedir. Taş devirlerinden başlayarak gelen bu sınıflandırma, 20. yy. son çeyreğinden itibaren yaşadığımız zamanı "*Bilgi Çağı – Information Age*"[1] olarak adlandırmaya başlamıştır. Bunun temel nedeni de iletişim ve bilişim teknolojilerinin çok hızlı gelişmesi ve hayatımızın her alanına girmiş olmasıdır. Bir bilgi ya da teknolojinin ortaya çıkması ile Dünya üzerinde en uzak köşeye kadar ulaşması ve yayılması için özel bir çabaya gerek kalmamıştır. Sanal dünyada ve İnternet ortamında bilginin dolaşması bağlamında coğrafi uzaklıklar ve fiziksel sınırlar artık bir anlam ifade etmemektedir. *"Bilgi"* artık her yerdedir.

Bilgi'nin değeri arttıkça ona sahip olma motivasyonu ve sahip olduktan sonra sağladığı güç de çok artmıştır. Sadece toplumlar ve devletler değil, tüm kurumlar ve hatta bireyler de bu gücün farkındadır ve "*Bilgi*"ye sahip olmak için günümüz teknolojilerinin araçlarını kullanmak istemekte ve kullanmaktadır[2]. Bu yaygın kullanım ve güce sahip olma güdüsü "*Bilgi Güvenliği*" kavramını da yanında getirmiştir. Bilgiye erişmek ne kadar değerli ise onu korumak ve ifade ettiği değerin sahibi olmak da bir o kadar önemlidir.[3] Kişisel bilgilerin mahremiyetinden kurumların ticari sırlarına kadar uzanan bu geniş bilgi yelpazesi, bireylerin İnternet, sosyal medya, iletişim araçları ve küresel bilgi paylaşım ve erişim ortamlarının değerini yadsınamaz şekilde en üst düzeye çıkarmıştır. Artık bireyler, kurumlar, toplumlar ve tüm devletler, sahip oldukları maddi ve manevi klasik değerlerinin yanına Bilgi Çağı'nın getirdiği yenilikleri ve değerleri de eklemek zorundadır.

21. yüzyılda çok hızlı ilerleyen ve gelişen iletişim teknolojileri ve bilişim altyapıları beraberinde küresel bir bilgi ortamının oluşmasını sağlamıştır. Kimse bu çemberin dışında kalmak istememektedir.[4] Fakat diğer yandan da bu kıymetli veriler ve taşıdığı bilgi değerleri, öncelikli ve hassas koruma gerektiren bir konuma gelmiştir. Bu süreçte Bilgi Güvenliği kavramları da aynı hızla gelişmeye başlamıştır. Bunun bir diğer gerekçesi de suç kavramının evrimleşmesidir. Gerek eski yöntemlerin modern araçlar ile kullanılmaya devam etmesi gerekse yeni suç tanımlarının ortaya çıkması, herkesin bilgiye güvenli erişme ve sahip olduğu bilginin değerini koruma aşamasında daha dikkatli ve donanımlı olmasını gerektirmiştir.[5]

2. Süreç Bazlı Standartlar ve Düzenlemeler

Toplumlardaki bilgi çağı ihtiyaçları İnternet'in ve iletişim araçlarının sağladığı olanaklarla gelişirken, devletler de kendi hukuk ve kamu düzenlerinde bu yeniliklerin gereklerini yapmaktadırlar. Bireyler bu aşamada devletlerin ve toplumların bu yeni çağa ayak uydurmaları için kendi talepleri ile ortaya çıkmakta, ama her zaman istediğini de

[1] Wikipedia. *Information Age. Erişim: 11.09.2011*

[2] Devlet Planlama Teşkilatı Müsteşarlığı (DPT), (2010). *Bilgi Toplumu İstatistikleri.* (s. 4-19)

[3] Pekel, A., (2010). *Bilişim Teknolojilerinde Yönetişim.* (s. 5-7)

[4] "Ürettiği bilgi ve geliştirdiği teknolojileri, ülke ve insanlığın yararına yenilikçi ürün, süreç ve hizmetlere dönüştürebilen Türkiye" vizyonu ile TÜBİTAK Bilim, Teknoloji ve Yenilik Politikaları Daire Başkanlığı (2010) tarafından yayınlanan "*Ulusal Bilim, Teknoloji ve Yenilik Stratejisi 2011-2016"* belgesi, ülkemizin bu süreçte aktif olabilmek için yapmak istediklerinin çerçevesini çizmektedir.

[5] Ünver, M., Canbay, C., Mirzaoğlu, A.G., (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler.* (s. 3-20)

alamamaktadır. Yeni kavramlar, yeni teknolojiler ve yeni yaşam şartlarına uyum sağlayabilen devletler ve toplumlar, Bilgi Çağı'nın nimetlerinden daha verimli ve sağlıklı olarak yararlanabilmektedir. Bu sürece ayak uyduramayan diğer aktörler ise küreselleşmenin dışında kalmamak adına garip bir devinimle kendilerine özel bilgi çağı değerlerini üretmektedir.

Gelişen bu altyapılar ve iletişim gücü, kurumların da yaşam döngülerinde çok önemli noktalara yerleşmeye başlamıştır. Özellikle, bilgi üreten, bilgi ile üretim yapan, hizmet götüren, finansal ve kamusal değerler ile faaliyet gösteren kurumların öncelikli olarak Bilgi Güvenliği kavramlarına uyum sağlaması gerekmektedir.[1, 2] Bilgi güvenliği süreçlerini kendi içinde özümsemeli ve kurumsal kültürünün bir parçası haline getirmelidir. Devletler bazı özel konumdaki kurumlara bunu kanuni bir zorunluluk olarak getirmekle birlikte, kurumlar da kendi değerlerini korumak ve faaliyet alanlarında öne çıkmak adına bu süreçlerden faydalanmaktadır.[3, ,4, 5]

Bilgi Güvenliği çalışmalarına başlamadan önce sorulması gereken en önemli sorulardan biri ne tür bir süreç çalışmasının yapılacağı, hangi standart ailesinin seçileceği ve bu uygulamaların hangi kapsamda ele alınacağıdır.[6] Finans sektöründe BDDK'nin getirdiği yasal mevzuat nedeni ile genel kabul gören sistem COBIT olmuştur.[7] Doğal olarak da onun çevresinde yerleşik durumda olan Risk IT, Val IT, ITAF gibi destekleyici süreç yönetimleri de öncelikli durumdur.[8] Bunların yanında SOX süreçleri de finansal aktörlerin tercihleri arasında yer almaktadır. Bu sektördeki firmaların, kendi tercihleri ile seçecekleri farklı organizasyon yapıları, resmi denetleme mekanizmaları devreye girdiğinde yetersiz ya da zayıf kalabilir.[9]

Müşteri ve son kullanıcılara dönük hizmet götüren firmaların da tercihi genelde ITIL üzerinden gitmektedir.[10] Burada, BT Hizmet Yönetimine dönük çalışmalar doğrudan faaliyet alanına katkı sağladığı için de geri dönüş hızının daha yüksek olması beklenmektedir. Bu yapı, süreç yönetimi talep eden ile hizmet götüren arasındaki uzun ilişki düzeninin temel kurallarını ve detaydaki çalışmalarını düzenlemektedir. Bilgi güvenliği süreçlerini iyi çözmüş bir yapıda eğer müşteri kavramı zayıf işlenirse, hizmet sektörünün süreç yönetiminin temelden aksaması kaçınılmaz olacaktır.

Proje tabanlı çalışan kurumlarda, PMI'nın PMBOK yapısı ve PRINCE2 çerçevesi ya da CMMI seviyesinde süreç çalışmaları ağırlık kazanabilmektedir. Bu yapıların firma kültürü içinde kullanılabilir olması için organizasyon yapısının proje yönetimine yatkın olması beklenmektedir. Zira yatay ya da dikey organizasyon şemalarında, proje yönetimi, kaynak kullanımı, üst - ast ilişkileri ve performans yönetimleri konusunda ciddi sorunlar olacaktır.

Askeri ve savunma sanayisinde çok gizli yapıdaki çalışmalarda zaten yapılacak süreç çalışmaları ve sağlanması gereken belgelendirmeler bellidir. Yapılacak çalışmalar bu süreçleri kurumun yeterliliği haline getirmektir.

Bilgi Güvenliği anlamında finans, savunma ve hizmet sektöründeki özel durumlar dışında, Sağlık, Haberleşme, Bilgi Teknolojileri, Tasarım, Ar-Ge, Üretim, gibi ana faaliyet konularında pek çok firmanın ihtiyacını karşılayacak Bilgi Güvenliği Süreç Yönetimi sistemi ISO/EIC 27000 ailesi olacaktır.[11] Gerek bilgi güvenliği süreçlerini tam karşılaması gerekse destekleyici diğer standartlar ile eksik nokta bırakmaması, bu süreç yönetimini popüler kılmaktadır. Buna ek olarak, kapsam belirlemede bu süreç ailesinin daha esnek olması da karar verme, planlama ve uygulama aşamasında büyük avantajlar sağlamaktadır.[12] Ayrıca, süreç çalışmalarında dış kaynak kullanımı ve danışmanlığın çok önemli olduğu da düşünüldüğünde, kapsamı, uygulama metodolojisi ve referansları olabilecek bir sertifikasyon, süreç çalışmalarını olumlu yönlerden destekleyecektir.[13]

1947 yılında kurulan Uluslararası Standardizasyon Organizasyonu (*International Organisation for Standardisation – ISO*) Uluslararası geçerlilikte standartlar konusunda çalışan bir kurumdur. Ayrıca, Bilgi Güvenliği ve süreçleri konusunda Uluslararası Elektroteknik Komisyonu (*International Electrotechnical Commission - IEC*) ve Uluslararası Telekomünikasyon Birliği (*International Telecommunication Union - ITU*) Bilgi ve İletişim Teknolojileri (*Information and Communications Technology - ICT*) kurumları ile işbirliği yapan hükümetler dışı bir uluslararası organdır. Aşağıda yaygın olarak kullanılan ISO güvenlik standartlarının başlık tanımları vardır:

•ISO/IEC 27000 — Bilgi Güvenliği Yönetim Sistemleri - Genel Bakış ve Tanımlar

•ISO/IEC 27001 — Bilgi Güvenliği Yönetim Sistemleri - Gereklilikler

•ISO/IEC 27002 — Bilgi Güvenliği Yönetim Sistemleri - Uygulama Kuralları

•ISO/IEC 27003 — Bilgi Güvenliği Yönetim Sistemleri - Uygulama Kılavuzu

•ISO/IEC 27004 — Bilgi Güvenliği Yönetim Sistemleri - Ölçme

[1] TÜBİTAK Bilim, Teknoloji ve Yenilik Politikaları Daire Başkanlığı (2010). *Ulusal Bilim, Teknoloji ve Yenilik Stratejisi 2011-2016.* (s. 4-6)

[2] Ünver, M., Ketevanlıoğlu, M.S., (2010). *Bilgi Teknolojisi Hizmetleri Düzenleyici Çerçeve Yaklaşımı.* (s. 37-40)

[3] Pattinson, F., (2007). *Certifying Information Security Management Systems.* (s. 9-10)

[4] Çetinkaya Kılıç, M., Gökçöl, O., (2010). *Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi.* (s. 1, 5)

[5] Pekel, A., (2010). *Bilişim Teknolojilerinde Yönetişim.* (s. 9, 15-17)

[6] *Aynı makale* (s. 7-10, 15-17)

[7] Bankacılık Düzenleme ve Denetleme Kurumu'nun tüm mevzuat bilgileri için bakınız: *Erişim: 11.09.2011* http://www.bddk.org.tr/websitesi/turkce/Mevzuat/Mevzuat.aspx

[8] ISACA, (2010). *COBIT, Val IT and Risk IT — Synergistic Relationship.*

[9] Türkyılmaz, M., (2010). *COBIT® ve Diğer Standartlar ile Karşılaştırılması.* (s. 13-23)

[10] The IT Service Management Forum (2007). *An Introductory Overview of ITIL® V3.*

[11] Çetinkaya Kılıç, M., Gökçöl, O., (2010). *Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi.* (s. 1-3)

[12] Perendi, Ü., (2008). *BGYS Kapsamı Belirleme Kılavuzu.* (s. 6-7)

[13] Ottekin, F., (2011). *BGYS ve BGYS Kurma Deneyimleri.* (s. 25)

•ISO/IEC 27005 — Bilgi Güvenliği Risk Yönetimi

•ISO/IEC 27006 — Bilgi Güvenliği Yönetim Sistemleri'nin Denetim ve Belgelendirme işlerini sağlayan kuruluşlar için şartlar

•ISO/IEC 27011 — ISO/IEC 27002'ye göre telekomünikasyon kuruluşları için bilgi güvenliği yönetim kuralları

•ISO/IEC 27031 — İş sürekliliği için bilgi ve iletişim teknolojisi hazırlık rehberi

•ISO/IEC 27033-1 — Ağ güvenliği genel bakış ve kavramlar

•ISO 27799 — ISO/IEC 27002 ile Sağlıkta Bilgi Güvenliği Yönetimi

Hazırlık Aşamasında olan belgeler:

•ISO/IEC 27007 — Bilgi Güvenliği Yönetim Sistemleri Denetimi Rehberi (yönetim sistemi odaklı)

•ISO/IEC 27008 — BGYS denetçileri (bilgi güvenliği denetimleri odaklı) için rehber

•ISO/IEC 27013 — ISO/IEC 20000-1 ve ISO/IEC 27001 bütünleştirme çalışmalarına ilişkin kılavuz

•ISO/IEC 27014 — Bilgi Güvenliği Yönetim Çerçevesi

•ISO/IEC 27015 — Finans ve sigorta sektörleri için bilgi güvenliği yönetim kuralları

•ISO/IEC 27032 — Siber Güvenlik (temelde, İnternet'te 'iyi bir komşu olmak' için rehber)

•ISO/IEC 27033 — BT Ağ Güvenliği, ISO/IEC 18028:2006'ya dayalı çok parçalı standart (Sadece Bölüm 1 yayınlandı)

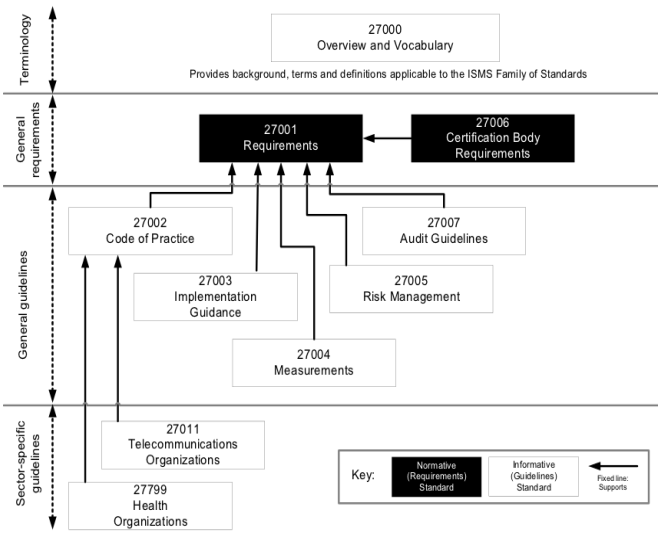
•ISO/IEC 27034 — Uygulama Güvenliği Rehberi

•ISO/IEC 27035 — Güvenlik Olay Yönetimi

•ISO/IEC 27036 — Dış Kaynak kullanımı için güvenlik rehberi

•ISO/IEC 27037 — Tanımlama, toplama ve / veya satın alma ve dijital kanıt korunması rehberi

ISO/IEC 27000:2009 : Information Security Management Systems — Overview and Vocabulary - Bilgi Güvenliği Yönetim Sistemleri - Genel Bakış ve Tanımlar: BGYS Standartlar ailesi, bazıları hali hazırda yayınlanmış veya geliştirme aşamasında olan ve birbiriyle yakın ilişkili standartlardan oluşur (Şekil 1). Bu belgeler süreçlerle ilgili önemli yapısal bileşenleri içerir. Bu bileşenler BGYS gereksinimlerini (ISO/IEC 27001) ve bunları belgelendirecek kuruluşun gerekliliklerini (ISO/IEC 27006) açıklamaya odaklanmış kural koyucu yapılardır. Diğer standartlar da bir BGYS için gerekli olan uygulama yönleri, kontrol ile ilgili kurallar ve sektöre özel rehberlik gibi çeşitli başlıkları açıklar.



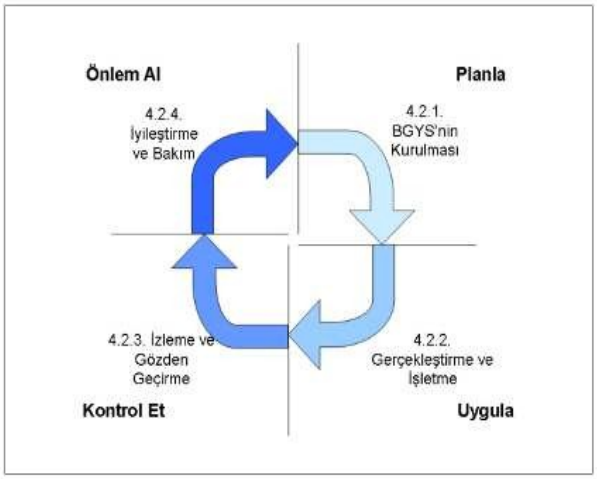
Şekil 1: ISO/IEC 27000 Standartlar Ailesi [1]

ISO/IEC 27001:2005 : Information Security Management System – Requirements - Bilgi Güvenliği Yönetim Sistemleri için Gereklilikler: Uluslararası bir standart olan ISO/IEC 27001:2005, köklerini bir *British Standards Institute* (BSI) standardı olan BS7799 Bölüm 2:2002'den elde edilen teknik içerikten türetilmiştir.[2] Bu standart, bir organizasyon içinde belgelenmiş bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmak, uygulamak, işletmek, incelemek, sürdürmek, geliştirmek ve izlemek için gereksinimleri belirtir.[3] Ayrıca, bilgi varlıklarını korumak için yeterli ve uygun güvenlik kontrollerinin seçimini sağlamak için tasarlanmıştır. Bu standart, genellikle her türlü ticari şirketler, kamu kuruluşları, vb. kuruluşlar için uygulanabilir. Standart bir kuruluşun BGYS etkinliğini artırmak amacı ile "Planla – Uygula - Kontrol Et - Önlem al (PUKÖ)" modeli olarak bilinen bir döngüsel model oluşturmaya yardım eder. PUKÖ döngüsünün dört aşaması vardır (Şekil 2):

[1] ISO/IEC 27000:2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary. (s. 12)

[2] ISO/IEC 27001:2005. Information technology — Security techniques — Information security management systems — Requirements. (s. iv – vii, 1)

[3] Taşkın, E., (2010). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi. (s. 3-4)



Şekil 2: BGYS için temel PUKÖ döngüsü.[1]

ISO/IEC 27001:2005 çoğu zaman ISO/IEC 27002:2005 ile birlikte yürütülmektedir. ISO/IEC 27001 BGYS bilgi güvenliği gereksinimlerini tanımlar ve BGYS için en uygun bilgi güvenliği denetimleri için de ISO/IEC 27002'deki ana hatları kullanır. ISO/IEC 27002, bir kuruluşun bilgi güvenliği risklerine uyum sağlaması için önerilen ve kontrol sağlayan basamaklardır. Bu kontroller zorunlu değildir. Yine de bir kurum ISO/IEC 27001 ile uyumlu sertifika almak isterse bu belgeden kesinlikle yararlanmalıdır. Belgelendirme işlemleri uluslararası geçerlilikte akredite olmuş belgelendirme kuruluşları aracılığı ile genelde bu yönetim başlıklarındaki kontrollerle yapılmaktadır.[2]

ISO/IEC 27002:2005 : Code of Practice for Information Security Management - Bilgi Güvenliği Yönetim Sistemleri için Uygulama Kuralları: Temeli *British Standards Institute* (BSI) kökenli ilk uluslararası standart olan BS7799-1'e dayanan bir standarttır (Nisan 2007'de ISO/IEC 17799:2005 yerine yayınlandı).[3] ISO/IEC 27002:2005, Bilgi güvenliği yönetimi için uygulanabilir gereklilikler anlamına gelir ve kuruluşlar için güvenlik standartları ve etkin yönetim uygulamaları geliştirmek için ortak bir temel rehber niteliğindedir.[4]

Bu standart, aşağıdaki 10 güvenlik etki alanı için kurallar ve en iyi uygulamalar için öneriler içermektedir: (a) güvenlik politikası; (b) bilgi güvenliği organizasyonu; (c) varlık yönetimi; (d) insan kaynakları güvenliği; (e) fiziksel ve çevresel güvenlik; (f) iletişim ve operasyon yönetimi; (g) erişim kontrolü; (h) bilgi sistemleri satınalma, geliştirme ve bakım; (i) bilgi güvenliği olay yönetimi; (j) iş sürekliliği yönetimi ve (k) uygunluk.

Bu 10 güvenlik etki alanı arasında, 39 kontrol hedefi ve en iyi uygulamalar için bilgi güvenliği kontrol önlemlerini içeren yüzlerce denetleme amaçlarını ve gizlilik, bütünlük ve kullanılabilirlik için tehditlere karşı bilgi varlıklarını korumaya yönelik tavsiyeler vardır.

3. ISO/IEC-27001 Süreç Çalışmaları

Bilgi Güvenliği Yönetim Sistemi (BGYS), kuruma ait kritik bilgi varlıklarının güvenliğini sağlamak amacıyla etkin risk yönetimi ile belirlenen güvenlik kontrollerinin uygulanmasına ve bu kontrollerin sürekli iyileştirilmesine dayanan bir yönetim sistemidir. Bir kurumun bilgi güvenliği anlamında bir süreç çalışmasının içine girmesi için mutlaka kötü bir senaryonun yaşanmasını beklememelidir. Faaliyet gösterdiği alanda kendisi için önemli bilgi ve çalışmalar varsa, bir an önce gerekli süreç disiplinini kurmak için çaba harcamalıdır. Bu süreç, haberleşme, sağlık, finans, Ar-Ge, savunma sanayisi gibi bilginin çok değerli olduğu sektörlerde devlet tarafından da mecburi hale getirilebilir. [5], [6] O yüzden de ciddi bir kurum, hukuki mecburiyetlerden önce kendi kararı ve iradesi ile bu çalışmalara başlamalı ve faaliyet konusunda en uygun süreç sertifikasyonlarını tamamlamalıdır.

3.1. Organizasyon ve Başlangıç

BGYS çalışmalarının başlayabilmesi için öncelikle bir kapsam çalışması yapılmalıdır.[7] Burada kurumun hangi faaliyet konularının, hangi yerleşkelerinin, hangi bölümlerinin ve hangi süreçlerinin bu yapıya dahil olacağının belirlenmesi gerekmektedir. Tanımı düzgün yapılmayan bir çalışmanın, ilerleyen süreçlerinde mutlaka eksikler veya zorluklar çıkacaktır. Bu aynı zamanda, süreç çalışmalarının planlamasında, bütçe ve iş gücü hesaplamalarında, çalışma ekiplerinin kurulmasında, belgeleme çalışmalarının ve takvimin belirlenmesinde de çok önemli bir adımdır.[8]

Kapsamı belirlenmiş bir BGYS çalışmasının karar aşamasında olması gereken bir ön şartı da Üst Yönetim'in desteğidir. Kurum yöneticilerinin, bu çalışmaların kurumsal bir ihtiyaç olduğunu, mecburiyetten değil, gerekliliken yapılması gerektiğini kabul etmesi ve alt kadrolarına bu mesajı ve kararlılığını net bir şekilde iletmesi gerekmektedir. Çünkü, sürecin en zorlu aşamalarında, gerek çalışanların motivasyonu gerekse zorlukların aşılmasında bu kararlılık anahtar rol oynayacaktır.[9]

ISO/IEC 27000 ailesi için çalışmaların başlangıcı, bu sürecin uzun soluklu bir çalışma olduğunu kabul etmekle başlayacaktır. Ve daha önemlisi, çalışmalar başarılı bir şekilde sonlandığında, ikinci perde başlayacaktır. O da bu sürecin kurum kültürü olarak sürekli yaşayacağı ve gelişeceği

[1] Ünver, M., Ketevanlıoğlu, M.S., (2010). Bilgi Teknolojisi Hizmetleri Düzenleyici Çerçeve Yaklaşımı. (s. 14)

[2] 28.09.2009 itibariyle ülkemizde 14 adet kuruluş TS ISO/IEC 27001 belgesi almıştır. (Kaynak: Ünver, M., Ketevanlıoğlu, M.S., (2010). Bilgi Teknolojisi Hizmetleri Düzenleyici Çerçeve Yaklaşımı. (s. 14)). 25 Haziran 2010 tarihi itibari ile de bu sayı 18 olmuştur (Kaynak: Ergin, H., (2010). TSE Bilgi Güvenliği Belgelendirme, s. 26)

[3] ISO/IEC 27002:2005. Information technology — Security techniques — Code of practice for information security management. (s. vii)

[4] Ottekin, F., (2011). BGYS ve BGYS Kurma Deneyimleri. (s. 3-4)

[5] *Elektronik Haberleşme Kanunu* (2008).

[6] *Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri Ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik* (2010).

[7] Önel, D., Dinçkan, A., (2007). *Bilgi Güvenliği Yönetim Sistemi Kurulumu.* (s. 5, 11)

[8] Taşkın, E., (2010). *ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi.* (s. 3-4, 9-12)

[9] Ottekin, F., (2011). *BGYS ve BGYS Kurma Deneyimleri.* (s. 19)

aşamadır. O yüzden de gerek politikaların belirlenmesinde gerekse süreç çalışmalarında, bir şekilde bitsin, belge alınsın, süreç tamamlansın psikolojisinin oluşmaması gerekir. Bu yapının, kurum aynı konuda faaliyet gösterdikçe ve yaşadıkça devam edecek bir döngü olduğu bilinmelidir.[1] Bu aşamada belirlenmesi gereken bir diğer başlık da süreç içinde görev alacak ekibin ve rollerinin belirlenmesidir. BT ekibi başta olmak üzere süreç tasarım ve yönetim tecrübesi olan Kalite ve İnsan Kaynakları gibi ekiplerden yürütücü roller için elemanlar seçilmelidir.

Bilgi Güvenliği politikalarının tasarlanması ve belirlenmiş kapsam içinde ortaya konması, BGYS çalışmalarının en büyük adımlarından olacaktır.[2] Bu politikalar, kurumun Bilgi Güvenliği anayasası olacağı için olması ve olmaması gereken temel ilkelerin, faaliyet konularının ve süreçlerinin hangi hedeflere yoğunlaşması gerektiğinin ortaya konacağı belgelerdir. Kapsaması gereken temel konular itibari ile tek bir belge olarak da yazılabilir. Hiyerarşik olarak birbirini destekleyen temel konuları başlık olarak seçen bir belge kümesi de hazırlanabilir.

BGYS için yapılacak çalışmaların kapsam, politika, kaynak planlama, çalışma takvimi ve ekip organizasyonu Üst Yönetim ile paylaşılmalı ve onların da görüşleri alınmalıdır. Temel çerçeve program ortaya çıktıktan sonra mutlaka orta ve üst kademe yöneticilerinin de görüşleri alınmalı ve süreç hakkında onlara da detaylı bilgiler aktarılmalıdır. Zira çalışmaların sağlıklı başlaması ve kurum çalışanları tarafından benimsenmesinin ilk adımı yönetim kadrolarının bu çalışmanın önemini ve gereğini kabul etmesi ile başlayacaktır. Süreç çalışmaların resmi bir açılışı mutlaka yapılmalıdır. Bu hem kurum içinde tüm çalışanların bilgilenmesi hem de çalışma ekibinin motivasyonu açısından önemli bir aşamadır.

3.2. Varlık Envanteri Oluşturma ve Risk Yönetimi

Varlık, bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurlardır.[3] İnsan, bilgi, yazılım, donanım, bina, iş araç ve gereçleri gibi işletme için bir değer ifade eden tüm unsurlar varlık olarak değerlendirilmelidir.

Bilgi güvenliği açısından bir donanımın bütünlüğünden söz etmek çok zordur. Bu sebeple asıl korunması ve yönetilmesi gereken bilgi veya süreçleri değerlendirmek, ardından bu bilgi ve süreçleri sağlayan veya barındıran donanım ve yazılımı güvenlik açısından incelemek ve sınıflandırmak daha kolay olacaktır. Diğer varlıklar düşünüldüğünde (yazılım, donanım, fiziksel varlıklar ve insan) bilgi ve süreçler en soyut kavramlardır ve güvenliğin üç temel öğesi (gizlik, bütünlük, erişilebilirlik) için derecelendirmenin kolaylıkla yapılabileceği varlık guruplarıdır.[4]

Bir organizasyonda varlıkların belirlenmesi ve varlıklara değer atanmasının yapılabilmesi için bir envantere ihtiyaç vardır. BGYS için varlık envanteri hazırlanırken öncelikle, tüm varlıkların kapsandığından emin olmak için gruplandırma yapmak varlıkların tanımlanması işini kolaylaştıracaktır. Bilgi varlıkları, yazılımsal varlıklar, fiziksel varlıklar, servisler vb. bir gruplandırma yapılabilir. Organizasyon içinde bir "varlık yönetim kılavuzu" veya "varlık envanteri yönetim kılavuzu" hazırlanmasında fayda vardır. Bu kılavuzda özellikle envantere yeni bir varlığın eklenmesi, envanterden varlık çıkarılması ve envanter sorumlusu net olarak belirtilmesi gerekir.[5]

Tehdit, herhangi bir tehdit kaynağının kasıtlı olarak veya kazayla bir açıklığı kullanarak varlıklara zarar verme potansiyelidir. Tehdit kaynağı ise varlıklara zarar verme olasılığı olan olaylar ve durumlar olarak tanımlanabilir.[6] Tehdit değerlendirmesi sırasında hiç bir tehdidin küçümsenerek göz ardı edilmesi doğru değildir. Göz ardı edilen tehdit kurum güvenliğinde zayıflık yaratabilir. Tehdit değerlendirmesi için gerekli girdi varlık sahiplerinden, kullanıcılardan, BT uzmanlarından, kurumun korunmasından sorumlu kişilerden elde edilebilir. Ayrıca tehditlerin belirlenmesinde tehdit katalogları da kullanılabilir.

Risk, *"zarara yol açan ya da zarar verme kapasitesi olan kişi ya da nesne"* olarak tanımlanmaktadır. Riskin, varlık, açıklık ve tehdit kavramları bağlamındaki bir diğer tanımı da: *"Bir kıymetteki bir açıklığın bir tehdit tarafından kullanılma ihtimalidir."* şeklindedir.[7]

Risk yönetimi, bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla koruyucu önlemlerin ve maliyetlerinin dengelenmesi ve organizasyonun hedeflerine ulaşması için gerekli kritik sistemlerin korunması gibi konularda BT yöneticilerinin yararlandığı süreçtir. Bu süreç risk analizi, risk işleme ve değerlendirme ve takip alt süreçlerinden oluşur.[8]

3.3. Güvenlik Kontrollerinin Hazırlanması, Uygulanması ve İyileştirme Adımları

BGYS konusunda temel başvuru kaynakları ISO/IEC 27001 ve ISO/IEC 27002 standartlarıdır. BGYS kurulumu öncesinde bu standartların mutlaka dikkatlice okunup anlaşılması gerekmektedir. BGYS kurulumu TS ISO/IEC 27001:2005'teki "4.2.1 BGYS'nin Kurulması" başlıkları altında detaylı olarak açıklanmaktadır.[9]

Risk işleme süreci sonuçlarına göre uygun kontrol ve kontrol hedeflerinin seçilmesi gerekir. TS ISO/IEC 27002:2005'te bu kontrollerden detaylı bir biçimde bahsedilmektedir. Bu kontroller standartta yol gösterici olması amacıyla verilmiştir. Kurum kendisine ek olarak başka kontroller de seçmekte serbesttir. TS ISO/IEC 27002:2005'te bulunan kontroller, sektör tecrübelerinden faydalanmak suretiyle, standart etki

[1] Önel, D., Dinçkan, A., (2007). *Bilgi Güvenliği Yönetim Sistemi Kurulumu.* (s. 9-10)

[2] Öztürk, G., (2008). *Bilgi Güvenliği Politikası Oluşturma Kılavuzu* .

[3] İbrişim, A., (2008). *TS ISO 27001 Bilgi Güvenliği Yönetim Sistemi Eğitim Notları.*

[4] Koç, F., (2008). *BGYS - Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu.* (s. 6-7)

[5] *Koç, F., (2008). BGYS - Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu.* (s. 8-9)

[6] İbrişim, A., (2008). *TS ISO 27001 Bilgi Güvenliği Yönetim Sistemi Eğitim Notları.*

[7] İbrişim, A., (2008). *TS ISO 27001 Bilgi Güvenliği Yönetim Sistemi Eğitim Notları.*

[8] Evrin, V., (2011). *Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği. (s. 38-43)*

[9] *TS ISO/IEC 27001 (Mart 2006). Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler.* (s. 5-7)

alanlarında olabildiğince geniş kapsamlı olarak belirlenmiş olsa da dış kaynaklı kontrollere ihtiyaç olabilmektedir. Sadece TS ISO/IEC 27002:2005'ten değil herhangi bir bilgi güvenliği kaynağından uygun kontrol seçilebileceği gibi kurumun kendine özel geliştirebileceği kontroller de olabilmektedir. Fakat gözden kaçan önemli bir kontrol hedefi veya kontrol olmadığından emin olmak için bu listeyi bir başlangıç noktası olarak kullanmakta fayda görülmektedir.[1]

Bu aşamada yazılı belge hazırlama işleri de tamamlanmalıdır. BGYS'nin kapsadığı alan için gerekli olan politikalar, yönetmelikler, prosedürler, talimatlar ve diğer kayıt amaçlı belgeler gerek kontrol süreçleri içinde gerekse belgelendirme aşamasında kullanılmaya başlanmalıdır.[2]

Son olarak risklere karşı seçilen kontrolleri içeren ve riskin ortadan kaldırılması süreçlerinin sonuçlarına dayanan, denetim hedeflerini ve kuruluşun BGYS'yle ilgili olan ve uygulanabilen denetimleri açıklayan belge olan "*Uygulanabilirlik Bildirgesi*" hazırlanır. Bu belgede seçilen kontrollerin neler olduğu ve bunların hangi gerekçelerle seçildiğini anlatmalıdır. Ayrıca, TS ISO/IEC 27001 belgesindeki kontrol listesi olan EK-A'dan seçilmeyen kontrollerin neler olduğu ile bunların seçilmeme gerekçeleri de Uygulanabilirlik Bildirgesinde verilmelidir.[3]

Başarılı ve etkin işleyen bir bilgi güvenliği bilinçlendirme süreci oluşturulabilmesi için bu alandaki görev ve sorumlulukların açık ve net bir biçimde belirlenmesi gerekmektedir. Olgunlaşmış bir bilinçlendirme süreci, bu görev ve sorumlulukların sahipleri tarafından doğru anlaşılması, bilinmesi ve uygulanması ile mümkündür. Bilgi güvenliği bilinçlendirme süreci kurum içinde en üst seviyeden en alt seviyeye kadar çalışanların katılımını gerektirmektedir.

Kullanıcılar, bilgi güvenliği bilinçlendirme sürecindeki en büyük ve önemli hedef kitledir.[4] Kurum içindeki işler yürütülürken istemeden yapılan hataları ve bilgi sisteminde oluşabilecek açıklıkları en aza indirmek onların elindedir. Kurum çalışanları, yüklenici firma personeli, yarı zamanlı personel, stajyerler, diğer kurum çalışanları, ziyaretçiler, iş ortaklarının çalışanları, destek alınan firmaların personeli, kısaca kurumun bilgi varlıklarına erişim gereksinimi olan herkes kullanıcı kategorisine girmektedir.

Yöneticiler, bilgi güvenliği bilinçlendirme ve eğitimi sürecinin gereklerine personelinin uymasını sağlamakla sorumludurlar. Bilgi güvenliği bilinçlendirme süreci kapsamında ortak sorumlulukları yerine getirmek amacıyla Bilgi Güvenliği Yöneticisi ve Bilgi Güvenliği Bilinçlendirme Süreci Yürütücüsü ile birlikte çalışmaları beklenmelidir.[5]

3.4. Kurum İçi Uyum Çalışmaları

Pek çok firma, BGYS çalışmalarından önce mutlaka farklı başlıklarda ve amaçlarda süreç çalışmalarına kendi bünyesinde yer vermiştir. ISO-9000 Kalite Süreçleri ailesi; Tesis Güvenlik Belgesi; CMMI, PMBOK gibi proje yönetim süreçleri gibi. Bu çalışmalar kurum için başlangıçta ciddi bir avantajdır, zira kurum çalışanlarının yönetmelik, iş akışı, süreç yönetimi, prosedür, talimat gibi kavramlara yakın olması beklenir. Bu başlığın BGYS için ek yükü ise geçmişte hazırlanmış ve halen aktif uygulanan bu tür sertifikasyon sistemlerinin de yeni süreç çalışması içinde gözden geçirilmesi, gerekli bütünleştirme çalışmalarının yapılması ve karşılıklı atıflarda bulunulması gerekliliğidir. Sonuçta, kurum içinde BGYS'nin ISO-9000 süreçlerinden ya da CMMI başlıklarından bağımsız çalışması hem beklenmemesi gereken bir durumdur hem de süreç mantığında olanaksız bir yaklaşımdır. Bu yüzden de kurumun sahip olduğu tüm süreç yönetimleri ve kurumsal uygulamaların BGYS içinde yer bulması ve kapsamı dahilinde karşılıklı atıflarda bulunulması gereklidir.

Bir kurum da zaman içinde gerek yönetimin oluşturduğu gerekse çalışanların yaşama geçirdiği bir firma kültürü vardır. Bu yerleşik kültür, kurumun yeni bir süreç çalışmasında duruma göre olumlu ya da olumsuz etkiler yapabilir. Yeniliğe açık, paylaşımcı ve iş birliği yapmaya yatkın yöneticilerin ve çalışanların olduğu bir kurumda BGYS gibi zorlu süreçlerin hayat bulması nispeten daha kolaydır. Bu yapının kurum için ne kadar önemli ve gerekli olduğu, bu bakış açısındaki insanlara daha çabuk gösterilebilir ve benimsetilebilir. Aksi durumlarda, her çalışan bu süreçleri, yeni bir külfet, çalışma hayatına ek yükler, özgürlüklerin kısıtlanması gibi algılayacaktır. Bu da sürecin toplam başarısında ciddi sorunlara neden olacaktır. Bu nedenle gerek BGYS'nin tanıtım, tasarım ve uygulamalarında ölçülü ve dengeli politikaların yürütülmesi, gerekse hem yönetimin hem de çalışanların tüm süreçlere sahip çıkmasını sağlayacak bilgilendirme ve empatinin sağlanması gereklidir.

BGYS çalışmalarında her bölüm ya da birim sürece katkı yapmaktadır. Fakat en önemli ekipler BT, Kalite ve İnsan Kaynakları gibi süreç yönetimlerine yakın konularda çalışan birimlerin çalışanlarından oluşmaktadır. Onların Bilgi Güvenliği farkındalığı ve bilinci konusunda herkesten bir adım önde olmaları ve süreçlere sürekli sahip çıkmaları beklenmelidir. PUKÖ döngüsü içinde oluşacak aksaklıkların ve alınacak aksiyonların ilk adresi bu ekipler olacaktır. Sürecin sorgulanması, farklı bakış açıları ile iyileştirilmesi ve geliştirilmesi yine bu ekiplerin önceliğinde olmalıdır.

3.5. Bilişim Hukuku'nun Süreçler ile Bütünleştirilmesi

Bilgi Güvenliği doğası gereği, varlıkları ortaya koymak, riskleri ve tehditleri tespit etmek, gerekli önlemleri hem gerçek ortamlarında almak hem de yazılı belgeler ile bunları somutlaştırmak durumundadır. Bilişim sistemlerinin kullanılması, bunların belli kural ve kontrollere tabi tutulması, "*bilgi*"nin korunması süreçlerinde kurumun ve çalışanlarının karşılıklı olarak haklarının korunması, ihlal edilmemesi şarttır. Doğal olarak bu süreçlerin tamamının yürürlükteki hukuk mevzuatı ile de uyumlu olması gereklidir. Bunun sağlanması için de dengeli bir politika hazırlanmalı ve tüm çalışanlar ile paylaşılmalıdır.

Bilişim sistemlerinde ve hizmetlerinde teknik bilgiler, hukuk mevzuatında neyin suç olabileceği ve neyin normal davranış olabileceği, hangi kanunların hangi konularda kurumlara veya çalışanlara haklar ve ödevler verdiğinin tüm yöneticiler ve

[1] Önel, D., Dinçkan, A., (2007). *Bilgi Güvenliği Yönetim Sistemi Kurulumu.* (s. 7-11)

[2] Evrin, V., (2011). *Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği*. (s. 46-47)

[3] Ottekin, F., (2008). *ISO/IEC 27001 Denetim Listesi.* (s. 6-58)

[4] Önel, D., (2008). *Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Kılavuzu.* (s. 9)

[5] *Aynı makale* (s. 8)

çalışanlar tarafından bilinmesi için Bilgi Güvenliği farkındalık eğitimleri düzenli olarak yapılmalıdır.[1] Bu eğitimlerde kullanıcılara BGYS süreçlerinin hangi amaca hizmet ettiği, hangi değeri ne için ve nasıl koruduğunun aktarılması ana hedef olmalıdır. Zira, bilişim ve iletişim sistemlerinin bu kadar hızlı geliştiği bir dönemde yönetici ve çalışanlar, yapması ve yapmaması gereken işlemleri bütün gerekçeleri ile bilmelidirler.[2, 3] Ancak bu şekilde BGYS sahibi kurumların çalışanları daha bilinçli olabilirler.

Bilişim hukukuna konu olan çalışmaların iki temel bakış açısı ile yapılması gerekecektir. Birincisi kurum yönetiminin gözüyle, diğeri de çalışanların hakları ve ödevleri başlıklarıyla. Kurum, sahip olduğu varlıkları korumak, bundan en yüksek faydayı sağlamak ve bunu da uzun süre devam ettirmek ister. Bu yüzden de gerek bilgi güvenliği gerekse firmanın temsil ettiği kurumsal kimliğin zarar görmemesi için önlemler alır. Devletin çıkardığı her kanun ya da yönetmelik ilgi alanına göre kurumlara yeni görev ve sorumluluklar getirebilir. Kurum tarafından tahsis edilen ve kullandırılan her teknoloji beraberinde özel yükümlülükler yaratıyor olabilir. Bu nedenle de kurum tarafından sağlanan her bilişim sisteminin ve hizmetinin kurallarının BGYS kapsamında tanımlı olması gerekmektedir. Neyin, hangi amaçla, nasıl ve ne zaman kullanılacağı bilinmelidir. Böylece, çalışanlar BGYS'nin kendilerine sunduğu olanakları ve çizdiği sınırları da bilerek çalışacaklardır. Ayrıca, denetleme yöntemlerinin ve şekillerinin de açıkça ortaya konması gerekmektedir. Bu bilgiler ve süreçler eski yeni fark etmez tüm çalışanların bilgisi dahilinde olmalı ve iş sözleşmelerinde özel maddeler ile imza altına alınmalıdır. Aynı şekilde, BGYS kapsamı içinde yapılan tüm faaliyetler, çalışanların anayasa ve kanunlardan gelen temel haklarını ve kişisel mahremiyetlerini de korumalıdır. Keyfi uygulamaların, önceden tasarlanmamış ya da duyurulmamış önlem veya denetimlerin mümkün olmaması gerekmektedir. BGYS, kurumun değerlerini, bilgisini, kurumsal kimliğini ve varlıklarını korurken aynı şekilde çalışanların da kişisel haklarını ve özel hayatlarını korumalıdır. Zira, çalışanlar da kurumun en değerli varlıkları arasındadır.

Gelişen ve ilerleyen düzenlemeler içinde Devlet eli ile yeni kanunlar ve yönetmelikler çıkarıldıkça BGYS'nin de buna uyum sağlaması gereken noktaları olacaktır. Bu çalışmalar da yine kurumsal çatı altında yapılmalı ve çalışanlar da yeterli şekilde bilgilendirilmelidir. Ayrıca BT konularında yeni çıkan teknolojiler, tehditler, kurum için zararlı olabilecek konular ve tehlikeler ortaya çıktıkça, aynı şekilde BGYS altyapıları yeniden gözden geçirilmeli ve çalışanlara gerekli teknik bilgiler düzenli olarak aktarılmalıdır. Bu da hem hukuki düzenlemeler açısından hem de teknolojik gelişmeler açısında kurum çalışanlarının, güncellenen BGYS süreçleri konusunda periyodik olarak bilgilendirilmelerini ve farkındalık düzeylerinin hep yukarıda tutulmasını sağlar.

[1] *Önel, D., (2008). Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Kılavuzu.* (s. 14-21)

[2] Eralp, Ö., (2010). *Bilgi İşlem Merkezi Yöneticilerinin Hukuki ve Cezai Sorumluluğu.*

[3] Tanrıkulu, C., (2011). *Bilgi Sistem Yöneticilerinin Hukuki Yükümlülükleri.*

3.6. Belgelendirme Çalışmaları

Bir kurum BGYS çalışmalarını genelde sertifikasyon hedefi ile yapar. Bu yüzden de önceden yaptığı tüm çalışmaları akredite edilmiş bir kuruma denetlettirerek onaylatmak zorundadır. Belgelendirme çalışmaları, Türkiye'de TÜRKAK tarafından akredite edilmiş bir kuruluşa yapılacak başvurunun alınması ile başlar.[4]

Dünya çapında organizasyon hiyerarşisi şu şekilde alt başlıklara ayrılabilir:

IAF - Uluslararası Akreditasyon Forumu gibi en üst çatı organizasyonu

EA gibi Bölgesel/Kıtasal Akreditasyon Forumları

TÜRKAK gibi Ulusal Akreditasyon Kurumları

TSE, KALİTEST gibi Belgelendirme Kuruluşları[5]

TÜRKAK, Türkiye'de tek yetkili akreditasyon kurumudur. IAF *(International Accreditation Forum)* ile MLA (*Multi Lateral Agreement*) anlaşması vardır. Bu, TÜRKAK akrediteli belgelerin dünyada tanınması anlamındadır. Türkiye'de üretim / hizmet sunan bir firmanın TÜRKAK akrediteli belgelendirme kuruluşundan belge alması, uluslararası akreditasyon kurallarının istediği bir durumdur. Çünkü belgeli firmadan hizmet alan tüketici, belgeyi veren kurum, akreditasyon kurumu vb. ilgili kuruluşlar zincirinin güven ve izlenebilirliği sağlanmalıdır.

Seçilen Belgelendirme Kuruluşunun seçimi ve değerlendirmesinde başlıca dikkat edilmesi gereken noktalar:[6]

•TÜRKAK tarafından verilmiş bir akreditasyona sahip olup olmaması,

•Dış akreditasyona sahip ise bu akreditasyonun Türkiye'yi kapsayıp kapsamadığı,

•Sertifikanın üçüncü taraflar tarafından kabul görüp görmediği,

•Belgelendirme kuruluşunun görevlendirdiği denetçilerin yetkinliği,

•Tarafsızlık ve bağımsızlığın sağlanması

•Danışmanlık ve belgelendirme ilişkisi (ISO 17021 şartları)

•Denetim ekibinin (baş denetçi ve denetçilerin) denetlenen kuruluştan bağımsız olmaları

•Belgelendirme kuruluşunun danışmanlık şirketi ile çıkar ilişkisinin olmaması (komisyon alma verme gibi)

Kurumun ISO/IEC 27001 sertifikası almak için yaptığı başvuru Belgelendirme Kuruluşu tarafından incelenir. Yeterli görülürse kurum ile belgelendirme kuruluşu arasında bir sözleşme imzalanır. Bu aşamadan sonra çalışmalar resmen başlamış olur. Bu adımı sırası ile 1. Aşama denetimleri; 2.

[4] Köse, O., (2010). *ISO/IEC 27001 Denetim ve Belgelendirmesi.* (s. 7)

[5] *Aynı makale,* (s. 39)

[6] *Aynı makale, (s. 35-38)*

Aşama denetimleri; Belgelendirme; Gözetim Denetimleri ve Belge Yenileme süreçleri geniş zaman içinde izleyecektir.[1]

4. Tartışma

İster kamu veya özel sektör olsun, isterse devlet ya da birey, Bilgi Çağı'nı yaşarken onun sunduğu yenilikleri, verimlilikleri, avantajları, özgürlükleri ve fırsatları kullanırken, kişisel, kurumsal, toplumsal ve ülkesel olarak bilgi güvenliği kavramlarını ve gereklerini de öğrenmeli ve onu da yaşam kültürü içinde tutmaya çalışmalıdır.

Kurumlar artık her türlü faaliyet alanlarında Bilgi Güvenliği süreçlerini kullanmak zorundadır. Bunu ister sertifika amacı ile yapsınlar ister kurumsal kültür olarak kullansınlar sonuç değişmeyecektir. Ticari başarı doğru zamanda doğru teknolojiyi kullanmak ya da üretmek olduğu kadar, yakın zamanda onu güvenli olarak kullanabilmeye devam edebilmek olacaktır. Çünkü bilgiye sahip olan ve bilgiyi doğru ve güvenli olarak kullanabilenlerin çağını yaşıyoruz. Bu yarışın içinde olmak isteyen her kurum, BGYS tarzı süreç yönetimleri bünyesinde kullanmak zorundadır.

Dikkat edilmesi gereken bir diğer öge de bu süreçlerin robotlaşmış yapılar ve kişiler tarafından kullanılmadığının bilincinde olmaktır. Kurumlar, çalışan süreçlerini tasarlarken ve uygularken, bunlarla beraber yaşayan çalışanlarının da haklarını ve mahremiyetlerini öncelikler listesinin üstlerinde tutmalıdır. Çalışanların sahiplenmediği hiç bir süreç bir kurum içinde uzun süre yaşayamaz. Yaşasa bile verimli olamaz. Çalışanlar da kendilerine sürekli zorluklar çıkartan, ama hiç bir katma değer sunmayan süreçleri kabullenmezler. Burada kurum çıkarları ile çalışan memnuniyetinin dengesini yakalamak zordur, ama çok önemlidir.

5. Sonuçlar

Bilgi Güvenliği'ni artık hayatımızın her aşamasında teknolojiyi ve iletişim sistemlerini kullanırken hissedeceğiz. Bu da çevremizdeki Bilgi Çağı aktörlerinin iyi tanınmasını ve amacına uygun kullanılması gerekliliğini tartışmasız olarak bize öğretecektir.

BGYS'nin sadece bir belge olmaması ve firma içinde yaşayan bir kültür olması da gerekmektedir. Gerek kurum yöneticileri gerekse çalışanlar bu bilinçle ve yaklaşım ile iş hayatlarını devam ettirmeliler. Sadece belge ya da sertifika odaklı çalışıldığında resmi süreçler belki sorunsuz halledilebilir, fakat süreçlerin katma değer olarak sunduğu bilgi ve varlık güvenliği ile kurumsal bilgi bütünlüğü bir yerde kesinlikle yara alır. Riskleri tanımlarken gösterilen hassasiyetlerin onu yaşarken de aynı olgunlukta devam ettirilmesi beklenmelidir. BGYS sertifika süreçleri yüz metre koşuları ile başarıya ulaşmak gibi görünse de PUKÖ döngüsü ile kendisini sürekli tekrar etmesi gereken bir maratondur aslında. Bu maratonda kurumların karşısına sürekli değişen ve gelişen teknolojiler, araçlar, hizmetler ve kavramlar çıkacaktır. Düzenli yapısını korurken, yeni teknolojileri de bünyesine katabilen kurumlar, günümüzde hep bir adım önde gitme şansını yakalayabilecektir.

[1] *Köse, O., (2010). ISO/IEC 27001 Denetim ve Belgelendirmesi. (s. 15-18)*

Bilgi Güvenliği felsefesinin, süreçlerinin ve kullanımının kurumların geleceği için vazgeçilmezliği kabul edilmelidir. Ancak bu şekilde, BGYS süreçleri kurum içinde bir kültür olarak yerleşebilir.

6. Kaynakça

[1] BDDK (2010). Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik. Resmi Gazete: 13 Ocak 2010. Erişim: 11.09.2011. http://www.bddk.org.tr/websitesi/turkce/Mevzuat/Mevzuat.aspx

[2] Çetinkaya Kılıç, M., Gökçöl, O., (2010). Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi. 3. Ağ ve Bilgi Güvenliği Sempozyumu 2010, Ankara.

[3] Devlet Planlama Teşkilatı Müsteşarlığı (DPT), (2010). Bilgi Toplumu İstatistikleri, Erişim: 11.09.2011, http://www.dpt.gov.tr/DocObjects/View/9776/BilgiToplumuIstatistikleri_2010.pdf

[4] Elektronik Haberleşme Kanunu (2008). Resmi Gazete, Sayı: 27050 (Mükerrer), 10 Kasım 2008. Ankara.

[5] Eralp, Ö., (2010) Bilgi İşlem Merkezi Yöneticilerinin Hukuki ve Cezai Sorumluluğu, 5. Kamu Kurumları Bilgi Teknolojileri Güvenlik Konferansı, 2010, Ankara.

[6] Ergin, H., (2010). TSE Bilgi Güvenliği Belgelendirme, Türk Standartları Enstitüsü, Ankara.

[7] Evrin, V., (2011). Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği, Hacettepe Üniversitesi Bilişim Hukuku Tezsiz Yüksek Lisans Programı Proje Raporu, Ankara.

[8] ISACA, (2010). COBIT, Val IT and Risk IT — Synergistic Relationship.

[9] ISO/IEC 27000:2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary. First edition, 2009-05-01.

[10] ISO/IEC 27001:2005. Information technology — Security techniques — Information security management systems — Requirements. First edition 2005-10-15.

[11] ISO/IEC 27002:2005. Information technology — Security techniques — Code of practice for information security management. Second edition 2005-06-15.

[12] İbrişim, Ayşegül., (2008). TS ISO 27001 Bilgi Güvenliği Yönetim Sistemi Eğitim Notları. Türk Standartları Enstitüsü, Ankara.

[13] Koç, F., (2008). BGYS - Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu. Sürüm 1.00, UEKAE, TÜBİTAK.

[14] Köse, O., (2010). ISO/IEC 27001 Denetim ve Belgelendirmesi. Bilgi Teknolojileri Yönetişim ve Denetim Konferansı (BTYD 2010), Ankara.

[15] Ottekin, F., (2008). ISO/IEC 27001 Denetim Listesi. Sürüm 1.00, UEKAE, TÜBİTAK.

[16] Ottekin, F., (2011). BGYS ve BGYS Kurma Deneyimleri. 6. Kamu Kurumları Bilgi Teknolojileri Güvenlik Konferansı, 2011, Ankara.

[17] Önel, D., (2008). Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Kılavuzu. Sürüm 1.00, UEKAE, TÜBİTAK.

[18] Önel, D., Dinçkan, A., (2007). Bilgi Güvenliği Yönetim Sistemi Kurulumu. Sürüm 1.00, UEKAE, TÜBİTAK.

[19] Öztürk, G., (2008). Bilgi Güvenliği Politikası Oluşturma Kılavuzu. Sürüm 1.00, UEKAE, TÜBİTAK.

[20] Pattinson, F., (2007). Certifying Information Security Management Systems. ATSEC Information Security Corporation .

[21] Pekel, A., (2010). Bilişim Teknolojilerinde Yönetişim. Bilgi Teknolojileri Yönetişim ve Denetim Konferansı (BTYD 2010), Ankara.

[22] Perendi, Ü., (2008). BGYS Kapsamı Belirleme Kılavuzu. Sürüm 1.00, UEKAE, TÜBİTAK.

[23] Tanrıkulu, C., (2011). Bilgi Sistem Yöneticilerinin Hukuki Yükümlülükleri. 6. Kamu Kurumları Bilgi Teknolojileri Güvenlik Konferansı, 2011, Ankara.

[24] Taşkın, E., (2010). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi. Bilgi Teknolojileri Yönetişim ve Denetim Konferansı (BTYD 2010), Ankara.

[25] The IT Service Management Forum (2007). An Introductory Overview of ITIL® V3.

[26] TS ISO/IEC 27001 (Mart 2006). Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler. Türk Standartları Enstitüsü, Ankara

[27] TÜBİTAK Bilim, Teknoloji ve Yenilik Politikaları Daire Başkanlığı (2010). Ulusal Bilim, Teknoloji ve Yenilik Stratejisi 2011-2016. Ankara

[28] Türkyılmaz, M., (2010). COBIT® ve Diğer Standartlar ile Karşılaştırılması. Bilgi Teknolojileri Yönetişim ve Denetim Konferansı (BTYD 2010), Ankara.

[29] Ünver, M., Canbay, C., Mirzaoğlu, A.G., (2009). Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler. Bilgi Teknolojileri ve İletişim Kurumu (BTK), Ankara.

[30] Ünver, M., Ketevanlıoğlu, M.S., (2010). Bilgi Teknolojisi Hizmetleri Düzenleyici Çerçeve Yaklaşımı. Bilgi Teknolojileri ve İletişim Kurumu (BTK), Ankara.

[31] Wikipedia. Information Age (t.y.). Erişim : 11.09.2011, http://en.wikipedia.org/wiki/Information_Age

BİR KURULUŞUN BİLGİ SİSTEMİ GÜVENLİĞİ İÇİN BİR YAKLAŞIM

Hakan Tan[1] Prof. Dr. A. Ziya Aktaş[2]

[1]Barikat İnternet Güvenliği Bilişim Tic. Ltd. Ankara
[2]Bilgisayar Mühendisliği Bölüm Başkanı, Başkent Üniversitesi, Ankara

[1]e-posta: hakan.tan@barikat.com.tr [2] e-posta: zaktas@baskent.edu.tr

Özetçe

Bilgisayar Mühendisliği alanındaki teknolojik gelişmeler bilgi sistemleri üzerinde işlenen ve paylaşılan bilginin boyutunu hızla artırmaktadır. Kamu kurum ve kuruluşları bu gelişmeleri takip ederek bilgi sistemleri sayılarını arttırmakta; temel görevlerini diğer kamu kurum ve kuruluşları ile bilgi paylaşım esasına göre bu sistemlerin üzerinde sürdürmekte ve vatandaşlara sunmaktadır. Özel sektörde de durum pek farklı değildir. Internet bankacılığı ile başlayan hizmetler bankacılık dışında hizmet veren firmaların artması ve güçlenmesi ile internet üzerinden her gün daha fazla kişi tarafından kullanılmaktadır. Bu trendin devam etmesi beklenmektedir. Bu nedenle bilgi sistemleri üzerindeki bilginin güvenliği ve hizmetlere erişilebilirlik bu hizmetleri veren kamu ve özel kurum ve kuruluşları için önem verilmesi gereken bir konu olmaktadır. Bu çalışmanın amacı bilgi sistemleri güvenliği kavramının araştırılarak sınırlarının tanımlanması ve mantıksal güvenlik alanında yararlı olabilecek güvenlik yazılımlarının kurum ve kuruluşlar tarafından nasıl kullanılabileceğinin özetlenmesidir.

Giriş

Çok sayıda kullanıcısı olan kamu ve özel kuruluşların ihtiyaçları ve verdiği hizmetler göz önünde bulundurulduğunda her kuruluşun iç ağlarında kendi çalışanlarına, internette ise dış kullanıcılara veya müşterilere çeşitli hizmetler sağladıkları bilinmektedir. Bu kapsamda kuruluşların çalışanlarına e-posta, dosya paylaşımları, internet erişimi, iç ağ portalleri ve üzerindeki web tabanlı uygulamalar gibi hizmetler verdikleri görülecektir. Dış dünya ile internet üzerinden verilen hizmetlerde ise mobil çalışanlara, müşterilere veya vatandaşlara çeşitli hizmetler sunulmaktadır. Birçok teknolojinin iç içe çalıştığı bu tarz ortamlarda işletim sistemleri ve bu sistemlerin üzerinde çalışan uygulamaların sahip olduğu güvenlik zafiyetleri kurumun bütün olarak güvenliğini tehdit etmektedir.

Yakın zamana kadar yürütülen bilgisayar korsanlığı aktiviteleri arkasındaki itici güç veya motivasyon ün, şan, şöhret iken, artık günümüzde bu itici güç çoğunlukla para ve nadir durumlarda da olsa ulusal çıkarlar olmaktadır. Motivasyonun niteliğindeki bu değişim yapılan saldırıların ve yazılan zararlı kodların da niteliğinde değişime sebep olması açısından oldukça önemlidir. Yüksek miktarda paranın el değiştirdiği yeni yeraltı ekonomisinin etkisi ile artık zararlı yazılımları yazanlar geçmiş zamanların tam tersine yazılımlarının kendilerini gizlemesi için çaba göstermektedirler. Bunun sebebi yarattıkları tehditlerin çözümlenmesini geciktirmek istemeleri ve bu süre zarfında yasa dışı kazançlarına devam etmek istemeleridir. Ulusal çıkarlar düşünülerek organize edilen saldırılara bakıldığında ilgili yazılımın yüksek yetenek ve bilgi seviyesi ile hazırlanmış oldukları fark edilecektir. McAfee güvenlik firmasının 2011 yılı içinde ortaya çıkardığı ve raporunu yayınladığı birden çok ülkeye ve bu ülkelerdeki kurumlara tek merkezden yapılan saldırılar ve izleme operasyonunun verileri internet ortamında gerçekleştirilen saldırıların ciddiyetini ortaya koymaktadır[1]. Aşağıdaki Tablo 1 ile bu operasyon kapsamında saldırıya uğrayan kuruluşların bulundukları sektörler gösterilmektedir[1].

Tablo 1 'Operation Shady RAT' içerisinde saldırılan ve izlenen kuruluşlar.

Sektör	Adet
Kamu	21
Enerji ve Üretim	6
Teknoloji	13
Finans	6
Sosyal Kuruluşlar	12
Savunma Sanayii	13

Burada dikkati çeken ilk konu, saldırılan kurumlar düşünüldüğünde birçoğunun arkasında ekonomik sebeplerin yatmamasıdır. Bu durum bazı devletlerin diğer devletlere karşı yaptığı siber saldırılar konusunda bir ipucu niteliğindedir. Raporda bahsi geçen

sektörlerdeki kuruluşların ortalama bir sene izlemeye ve veri kaçırılmaya maruz kaldıkları belirtilmiştir.

Bilgi Sistemleri Güvenliği

Bilgi sistemleri güvenliği erişilebilirlik, gizlilik ve bütünlük ilkeleri çerçevesinden düşünüldüğünde çok geniş bir yelpazede konuyu içeren bir alandır. Bu üç temel ilkenin hepsinin bir arada sağlanması ise bu geniş çalışma alanının her konu başlığında gerekli çalışmanın yapılması zorunluluğunu ortaya çıkarır. Örnek verilmek istenirse, bütünlüğü bozulmuş bir hasta veya finans bilgisinin erişilebilir olmasının ve gizliliğinin bir anlamı kalmamaktadır.

1.1. Güvenliği Sınıflandırmak

Vacca[2] bilgi sistemleri güvenliğini üç ana bölüme ayırmaktadır:

- Mantıksal Güvenlik
- Fiziksel Güvenlik
- Çevre Güvenliği

Mantıksal güvenlik bilgi sisteminin iletişim ağları vasıtası ile maruz kalabileceği tehditleri kapsamaktadır. Fiziksel güvenlik ise bilgi sistemlerini barındıran fiziksel altyapının güvenliğini tarif etmektedir. Fiziksel güvenliğin kapsamına sunucu ve istemci donanımları, sistem odası, sistem odasının bulunduğu bina, güç hatları gibi bileşenler girer. Çevre güvenliği ise fiziksel güvenlikle bir düşünülebilir, ayrıldığı nokta ise bilgi sistemini barındıran bina veya kampüs alanının sınırlarında alınacak güvenlik önlemleridir.

1.2. Mantıksal Güvenlik

Bu makalenin ana konusunu oluşturan mantıksal güvenlik iki alt guruba ayrılabilir:

- Uygulama Güvenliği
- Altyapı Güvenliği

Uygulama güvenliği, uygulamayı geliştiren yazılım ekibinin sorumluluğunda olan bir alandır. Burada yazılımcıların yazdıkları uygulama için geliştirme sırasında gerekli olan güvenlik seviyesine göre gereken önlemleri almaları beklenir.
Altyapı güvenliği ise bilgi sistemlerinin diğer sistemler ve kullanıcılar ile iletişim kurması esnasında alınabilecek önlemleri kapsar. Bu önlemler altyapı üzerinden geçen trafik üzerinde veya pasif olarak güvenlik personeline bilgi sağlayacak şekilde olabilir.
Bir bilgi sistemi katmanlı olarak düşünülürse yapılan sınıflandırmaların Şekil 1 de hangi katmanlara denk geldiği görülebilir[3].

Bilgi Sistemi Uygulamaları, Hizmetler	Uygulama Güvenliği
Veritabanları	
Hazır yazılımlar	
İşletim Sistemi	Alyapı Güvenliği
İç Network	
İnternet	
Fiziksel Ekipman, Personel, Tesis	Fiziksel Güvenlik

Şekil 1 Bilgi Sistemi Katmanları

Güvenlik Yazılımları

Kamu ve özel sektör kurum ve kuruluşları, güvenlik ihtiyaçlarına göre aşağıda kısaca özetlenmiş olarak verilen güvenlik yazılımlarını kullanabilirler. Güvenlik yatırımlarının kurumların ihtiyaçlarını karşılayacak şekilde yapılması önemlidir. İhtiyaçtan daha az veya daha fazla yapılan yatırım ve çabalar her zaman maddi ve manevi zararlar ile sonuçlanacaktır.

- *Güvenlik Duvarı (Firewall)*: Güvenlik duvarları üzerlerinden geçen trafik için erişim kuralları belirlemek ve uygulamak amacı ile kullanılırlar. Üzerlerinde bulunan kural tablosu yardımı ile istenmeyen yere doğru giden belirli nitelikte trafiğin geçişi engellenebilir. Ana ağ segmentleri (veya bölümleri) içinde kullanılabilmeleri sayesinde segmentler arasında erişim kuralları uygulanabilir. Dış dünya ile bağlantıyı güvenlik duvarları sağladığından mobil kullanıcıların şifreli olarak bağlantı kurmalarına olanak sağlayarak açık ağlardan geçerken verinin gizliliğinin korunmasına yardımcı olur.
- *Atak Önleme Sistemi (Intrusion Prevention System, IPS)*: Atak önleme sistemleri korunmak istenen ağ segmentlerinin bağlantıları üstüne konularak zararlı trafiğin kesilmesi sağlanır. IPS sistemleri trafik üzerinde önceden belirlenmiş saldırı imzalarına uyan trafiği ararlar ve bulduklarında, paket düşürme, TCP bağlantısını sonlandırma gibi eylemlerde bulunabilirler. Bu özelliklere ek olarak servis dışı bırakma saldırılarına karşı, istatistiksel ve manüel verilmiş sınırları işleterek koruma sağlayabilirler.
- *Web Uygulama Güvenlik Duvar (Web Application Firewall):* Web uygulama güvenlik

duvarları IPS lere benzer bir görev üstlenir. Web hizmetlerinin çok yaygın kullanılması sebebi ile üretilen bu sistemler web hizmetlerine ve web sunucularına gelebilecek saldırıları önleyecek trafik imzaları bulundururlar. Bu özelliklerine ek olarak yazılım geliştirilirken önlem alınmamış konularda ek koruma getirebilirler. Web ara yüzünde bilgi girişi yapılan alanlar üzerinde istenilen kontrollerin veya girdi doğrulamasının yapılması bir örnek olarak verilebilir.

- *Veritabanı Güvenlik Duvarı (Database Firewall)* : Veri tabanı güvenlik duvarları veritabanına gelen sorguları inceler ve olası zararlı aktiviteleri tespit edebilir. Kullanıcı davranışlarını öğrenerek profil dışına çıkma durumlarında uyarı üretebilirler. Web ve veritabanı güvenlik duvarının beraber kullanımı ile kullanıcıların web üzerinde yaptıkları işlemlerin veritabanı üzerinde yarattığı iz düşümü takip edilebilir. Bu sayede uygulamaların veritabanına bağlandığı tek bir kullanıcı yerine gerçek kullanıcıların kimlik bilgileri ile eşleştirme yapılarak veritabanı operasyonları gerçek kişilere bağlanabilir.
- *E-Posta Güvenliği (E-mail Security Gateway)*: Kurum sistemlerine dışarıdan gelen spam ve zararlı kodların önlenmesinde kullanılırlar. Ağ seviyesinde internete açık bir şekilde mail sunucu (Mail transfer agent, MTA) görevi ile de kullanılabilir. Aynı zamanda mail sunucuların üzerinde çalışan çeşitleri de vardır.
- *Yük Dengeleyici (Load Balancer)*: Yük dengeleyiciler erişilebilirliği en üst seviyede tutmak için yoğun istek gelen sunucular arasında yük paylaştırırlar. Eğer bu bir web sunucu ise SSL(secure sockets layer)'i kendi üstlerinde sonlandırarak sunucuları kriptolama yükünden kurtararak performans artışı sağlarlar.
- *URL Filtresi ve Antivirus (Web Security Gateway)*: Kurum ağında çalışan istemcilerin internet erişimlerini düzenlemek amacı ile kullanılırlar. Bazı sitelere erişimin engellenmesi hem güvenlik hem de kurum politikası gereği istendiği durumlarda erişimi engelleyebilirler. Bu işlevi yaparken vekil sunucu şeklinde çalışıyorlarsa gelen trafik üzerinde zararlı yazılım taraması da yapabilirler.
- *Web Cache Vekil Sunucusu (Caching Proxy Server)*: Kaşe (Cache) sunucuları URL filtreleri ile aynı sistemde olabildikleri gibi ayrı olarak da kullanılabilir. İnternetten çok defa aynı dosyanın indirilmesi durumunu engellemek amacıyla çok indirilen dosyaları üzerlerinde tutarak internet bant genişliği tasarrufu sağlarlar. Bu da erişilebilirliği artıracaktır.
- *Transparan İçerik Yönlendiriciler (Transparent Redirection)*: Karmaşık ve büyük ağ yapılarında istemcilerin URL filtre gibi trafiğin yönlendirilmesi gereken yerlerde kullanıcı sistemleri üzerinde ayar yapılmadan gönderilmesini sağlayabilirler. Bu özellik ile kullanım kolaylığı sağlarken aynı zamanda da ayarların eksik yapılması ihtimalini ortadan kaldırarak her kullanıcının istenen vekil sunucuları kullanmasını garanti altına alırlar.
- *Zafiyet Tarama Sistemleri (Vulnerability Scanner)*: Böyle bir sistem işletim sistemleri üzerindeki ve işletim sisteminde çalışan uygulamalar üzerindeki zafiyetleri otomatik taramalar ile bulur. Aynı zamanda yama eksikleri veya kurum politikasına aykırı yapılandırılmış sistemleri de tespit edebilir.
- *Risk Analiz ve Önceliklendirme Sistemi (Risk Management Systems)*: Zafiyet tarama sistemlerinden sistem zafiyetlerini, güvenlik duvarı, ağ anahtarları ve yönlendiricileri gibi cihazlardan da yapılandırma ayarlarını toplayarak bir ağ modeli oluşturur. Oluşturulan ağ modeli üzerinden risk risk analizi yapılır ve önceliklendirilir. Bu sayede kısıtlı personel kaynaklarının nerelerde ilk önce kullanılması gerektiği ve en çok risk altında bulunan sistemler gibi bilgiler elde edilir
- *Kayıt Toplama ve Korelasyon Sistemi (Security Information and Event Management, SIEM):* Birçok güvenlik sistemi üzerlerinde meydana olaylar için çeşitli ortamlarda olay kayıtları tutarlar. Bu olay kayıtları her sistemin üzerinde olduğundan diğer sistemlerdeki olaylar ile ilişkilendirme işlemi çok zor olmaktadır. SIEM sistemleri dağıtık halde olan bu kayıtları bir yerde toplayarak korelasyon yapılabilir hale getirirler. Yazılan mantıksal kurallar sayesinde gerçek zamanlı korelasyon yapılabilir ve normalde tespit edilemeyen güvenlik olayları tespit edilebilir.
- *Ağ erişim kontrolü (Network Access Control)*: Ağ erişim kontrolü sistemleri kurum politikalarına uymayan sistemlerin ağa dahil olmalarını engellemek amacı ile kullanılır. Bu sayede yabancı sistemlerin ve güvenlik durumu uygun olmayan sistemlerin iç ağı tehdit etmesi önlenir.
- *Sıfır Gün Zararlı Yazılım Tespit Sistemi (Zero Day Malware Protection System, Malware sandboxing)*: İmza tabanlı zararlı yazılım tespit sistemleri (Antivirüs) imza veri tabanlarında olmayan zararlı yazılımları yakalayamamaktadır. Günümüzde artan bir hacimde zararlı yazılımlar yazıldığından imza

veritabanlarında yer almaları uzun süreler almaktadır ve bu arada geçen zamanda sistemler savunmasız kalmaktadırlar. Bu sistemler genelde şüpheli yazılımları ağ seviyesinde yakalayarak test sistemlerinde çalıştırırlar(Sandboxing). Çıkan sonuçlara göre imzasız olarak zararlı tespit edilen yazılımlar engellenebilir[4].

- *Ağ izleme ve Performans Analiz Sistemi (Network Performance Management)*: Böyle bir sistem ağ trafiği üzerinden uygulama ve ağ performansı hakkında bilgi toplar. Bu sayede performans kaybı olaylarında bilgilendirme yapabilir ve bu durumlarda sorunun kaynağı ile alakalı detaylı bilgiyi ilgili personele sağlar[5].
- *Veri Kaçaklarını Önleme Sistemi (Data Loss Prevention)*: Sistemler üzerinde bulunan hassas verinin izinsiz kurumlar dışına çıkartılmasına engel olur. Hem ağ hem de istemci seviyesinde çalışan modelleri vardır. İstemci üzerinde çalışan sistemlerde taşınabilir medya gibi kaynaklardan kaçakların önlenmesi için aygıt kontrolü yapan bileşenleri bulunur. Yazıcılar, CD-DVD yazıcı ve okuyucular, USB depolama cihazları örnek olarak verilebilir.
- *Ağ Tabanlı Adli Bilişim Sistemi (Network Forensics)*: Bu sistemler pasif olarak ağ trafiğini yakalayarak trafik üzerinde derin paket incelemesi yapabilme olanağı sağlarlar [6]. Bu sayede sistemde meydana gelen olaylar ve sorunlar detaylı şekilde incelenebilir. Trafik kayıt edildiği için veri kaçaklarını önleme sistemlerine kaçak olması durumunda çıkan verinin niteliği hakkında bilgi sağlayarak yardımcı olurlar.
- *Tek Yönlü Veri Transfer Cihazları (One Way Data Transfer)*: Genelde internete kapalı ağlara veri transferi yapılırken dışarı veri sızıntısını engellemek amacı ile kullanılırlar. Donanım tabanlı ürünler iki tarafa da kullanılan protokol çalışırmış gibi gösterirken donanım üzerinde bir yön haricinde ters yöne veri iletişimi fiziksel olarak engellerler[7].
- *İstemci Güvenlik Ürünleri (Endpoint Security)*: İstemci üzerinde çalışan güvenlik ürünleri ağ seviyesinde çalışanlara destek olacak şekilde ek bir katman olarak görev yaparlar. Antivirus, IPS, Veri kaçakları önleme yazılımı, disk şifreleme örnek olarak verilebilir.

Güvenlik Risk Yönetimi

1.3. Risk Değerlendirmesi

Önceki bölümde kısaca özetlenen güvenlik yazılım ürünlerinin doğru seçimi ancak güvenlik risk değerlendirmesi yapıldıktan sonra yapılabilir. Risk değerlendirmesinin adımları sırası ile:

- Varlıkların tespiti ve değerlerinin belirlenmesi;
- Varlıklar zarar gördüğü zaman kurumun yaşayacağı zararın belirlenmesi;
- Tehditlerin ve tehditlerin olma olasılıklılarının belirlenmesi;
- Alınabilecek önlemlerin belirlenmesi;
- Hangi önlemlerin uygulanacağı kararı için fizibilite çalışması yapılması ve sonucuna göre uygun görülen güvenlik önlemlerinin uygulanması.

Güvenlik risk değerlendirmesi ilk defa yapıldıktan sonra periyodik olarak tekrarlanması gerekmektedir. Yaşam döngüsü şekilde yapılan risk değerlendirmeleri sistemlerin kullanılması, tasarımının yapılması veya uygulanmasını etkileyecektir[3].

1.4. Zafiyet ve Sızma Testleri

Oluşturulan güvenlik mimarisi ile birlikte sistemin beklenen şekilde çalıştığı durumda alınan güvenlik önlemlerinin etkinliğinin belirlenmesi önemli bir konudur. Sistem altyapısına ve işletim sistemlerine entegre edilmiş güvenlik önlemleri her ne kadar belirli bir seviyede güvenlik getirse de asıl önemli olan, bu yazılımları kullanan, yapılandıran ve sürekli izleyen güvenlikten sorumlu personeldir. Bu sebeple sızma veya penetrasyon testi olarak anılan, sistemin son haline iç ağdan ve dış ağdan test saldırıları düzenlenir. Açıklıklar bulunmaya çalışılır ve bulunan açıklıklar raporlanır. Periyodik olarak yapılan sızma testleri ile güvenlik sistemlerinin yapılandırmaları ve etkinlikleri istenilen seviyede tutulmaya çalışılır.

Sızma testlerine ek olarak hizmet veren sunucuların ve üzerlerinde koşan uygulamaların açıklarının da tespit edilmesi ve alınabilecek bir önlem varsa alınması gerekir. Zafiyet testleri, sızma testleri gibi insanlar tarafından yapılabileceği gibi, bu işe özel olarak yazılmış otomatik araçlar kullanılarak da yapılabilir. Otomatik araçlar kullanıldığında bu testler daha sık yapıldığından kurum sistemlerinin zafiyet durumları geçen zaman göre incelenebilir ve iyileşme ya da kötüleşme durumlarından ilgili kişiler haberdar edilebilir.

Tasarım

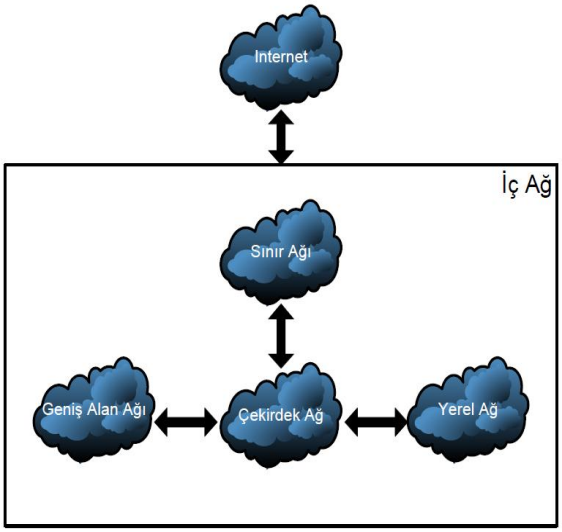
Bilgi sistemlerinin tasarım ve gerçekleştirilmelerinde mimari olarak katmanlı mimariler ile modüler yapının avantajlarından faydalanılır. Fakat bu sadece esnek yapının avantajlarını değil aynı zamanda güvenlik önlemlerinin alınmasında da kolaylık ve olanak sağlar . Web ara yüzü, uygulama sunucusu ve veritabanı sunucusu şeklinde tasarlanmış bir bilgi sisteminde bileşenler arası çalışmada bahsedilen güvenlik bileşenleri kullanılabilir.

Bu makalede yukarıda bahsedilen şekilde tasarlanmış bir uygulama ile servis veren ve aynı ağda kullanıcılarını da barındıran sanal bir kurum için

güvenlik önlemlerinin tasarlandığı bir yüksek lisans tez çalışması özetlenmiştir[8]. Güvenlik mimarisi tasarlanırken genel ağ segmentleri birbirlerinden güvenlik duvarları ile ayrılmıştır. En genel olarak aşağıdaki ağ segmentleri (bölümleri) belirlenmiştir:

- Internet
- Sınır Ağı
- Yerel Ağ
- Çekirdek Ağ
- Geniş Alan Ağı

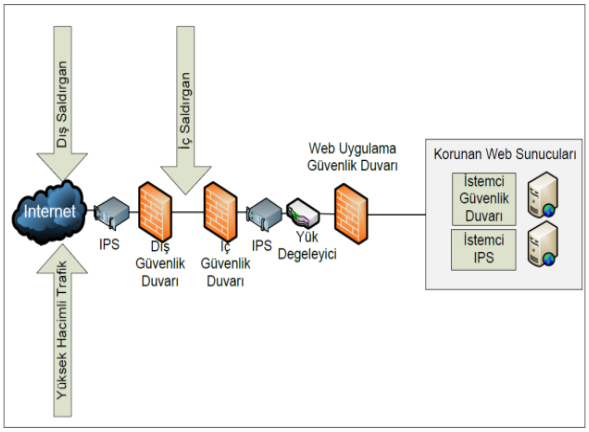
Bu ağ bölümleri arası geçişler erişim kuralları ile düzenlenmiştir. En az yetki prensibi ile gerekli erişimler dışındaki tüm erişimlerin engellendiği varsayılmaktadır. Şekil 2 de yukarıda belirtilen ağlar arası iletişim yolları mantıksal olarak görülmektedir. Internet haricinde diğer kesimler kurum iç ağı olarak kabul edilmiştir.



Şekil 2 Genel Ağ Segmentleri

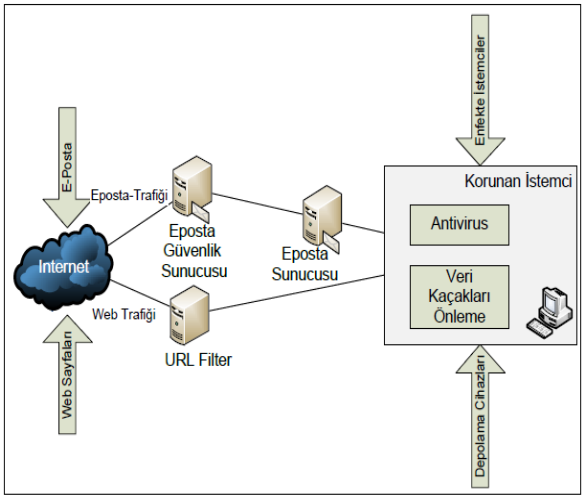
Sınır ağı internetten doğrudan ulaşılması gereken e-posta sunucuları, DNS sunucuları gibi sistemlerin bulunduğu bölümdür. Çekirdek ağda dışarıdan doğrudan erişilmeyecek tüm sunucular bulunur. Yerel ağ ile geniş alan ağında da kullanıcı sistemleri bulunmaktadır. Geniş alan ağı mobil kullanıcıları ya da uzak ofisleri temsil etmektedir.

Tanımlanan ağ segmentlerinde güvenlik önlemleri için katmanlı güvenlik mimarisi tanımlanmıştır. Katmanlı güvenli mimarisi saldırgan ve hedef arasına birden fazla güvenlik önlemi koyarak sağlanır. Bu sayede katmanlar arasından gelebilecek tehditler sonraki katmandaki güvenlik önlemleri ile engellenebilir. Şekil 3 ile korunmak istenen bir web sunucu ile internet arasında alınan önlemler mantıksal bir şema ile gösterilmiştir. Bu senaryoda internet tarafından başlamak gerekirse öncelikle dış güvenlik duvarı tarafından istenmeyen yöndeki trafik kesilecektir. Bilinen ataklara karşı koruma sağlayan IPS sistemleri ile hem internet tarafından hem de diğer ağlardan gelecek trafik engellenebilmektedir. Bu önlemlere ek olarak yük dengeleyici ile erişilebilirlik artırılmakta web uygulama güvenlik duvarı ile de daha karmaşık web tehditlerine karşı koruma sağlanmaktadır. En son katman savunma olarak istemci IPS ve istemci güvenlik duvarı kullanılmıştır. Bulunduğu ağdan gelecek olası bir saldırı bahsedilen ağ cihazlardan geçmeyeceği tek savunma olarak istemci güvenlik ürünleri kalmaktadır. Uygulanan bu katmanlı yapı ile saldırıların gelebilecekleri tüm yerler ve nitelik olarak bilinen saldırıların birçoğu engellenebilecektir.



Şekil 3 Katmanlı Savunma için Mantıksal Yapı

Şekil 4 içinde ise istemcilere bulaşabilecek zararlı yazılımların geliş vektörlerine göre alınmış önlemler görülebilir.



Şekil 4 Zararlı Yazılım Geliş Yolları ve Önlemler

Zararlı yazılımlar için de katmanlı mimari kullanılmıştır. İstemcide çalışması gereken zararlı yazılımların geliş vektörleri internet den eposta ve internet kullanımı, depolama cihazları ve diğer enfekte sistemler olarak özetlenebilir. Eposta ve web için güvenlik yazılımları vekil sunucu şeklinde konumlandırılarak zararlı yazılım taraması yapmaktadırlar. Sistemlere ağ üstünden geçmeyen yollar ile gelmesi durumu için Veri Kaçakları Önleme Yazılımlarında bulunan ya da tek başına kullanılabilen

aygıt yönetme yazılımı ile depolama aygıtlarının kullanılması yasaklanmıştır. Bu sayede depolama cihazları ile istemciye zararlı yazılım bulaşması engellenmiştir. Bu yolların dışında, ortamda bulunan diğer bir enfekte sistem de kendini başka sistemlere göndererek yayılmayı seçebilir. Burada da antivirus yazılımı zararlı kodu imzalarında var ise engelleyecektir.

Sonuç

Kamu ve özel sektörde sayısı ve boyutu hızla artan bilgi sistemlerinin gerektiği oranda güvenliğinin sağlanması günümüzde büyük önem kazanmıştır. Katmanlı savunma mimarisi ile birden çok katmanda güvenlik kontrolü yapılabilir. Katmanlı yapı ile birden fazla savunma noktaları oluşturularak saldırganları yavaşlatmak ve her atak vektörünü karşılayacak bir önlem konuşlandırılmış olabilmektedir.
Bu makalede altyapı güvenliğinin artırılması özellikle ele alınmıştır. Fakat diğer güvenlik alanları da aynı zamanda oluşturulmalıdır. İnsan faktörü ve fiziksel güvenlik toplam güvenlik mimarisinde vazgeçilemeyecek noktalardır.
Herhangi bir kurum ve kuruluş için güvenlik yatırımları yapılmadan önce risk analizi çalışması yapılarak ancak gerektiği kadar güvenlik yatırımı yapılması uygun bir yaklaşım olacaktır.

Teşekkür

Yazarlar, bilgi sistemleri güvenliği alanına katkıda bulunan tüm meslektaşlarına teşekkürlerini sunarlar.

Kaynakça

[1] Alperovitch, D. “Reveald: Operation Shady RAT”, McAfee, 2011.
[2] Vacca, J. “Computer and Information Security Handbook” Morgan Kaufmann, 2009.
[3] Sommerville, I. “Software Engineering”, Addison-Wesley, 2007.
[4] FireEye Web MPS Datasheet, http://www.fireeye.com/resources/pdfs/FireEye_Web_MPS_ds.pdf
[5] Riverbed Cascade, http://www.riverbed.com/us/products/cascade/
[6] Packet Capture, Wikipedia, http://en.wikipedia.org/wiki/Packet_capture, 09.2011.
[7] Unidirectional Network, Wikipedia, http://en.wikipedia.org/wiki/Unidirectional_network
[8] Tan. H. “Kurum ve Kuruluşların Bilgi Sistemi Güvenliği ve Bir Uygulama”, Yüksek Lisans Tezi (Danışman: Prof. Dr. A. Z. Aktaş), Başkent Ü. Bilgisayar Müh. Bölümü, 2011.

Atlamalı Aralık Yayın Şifreleme Sisteminde Bedava Alıcıların İyi Yerleştirilmesi

Murat Ak[1] Ali Aydın Selçuk[2]

[1,2]Bilgisayar Mühendisliği Bölümü, Bilkent Üniversitesi, Ankara
[1]e-posta: muratak@cs.bilkent.edu.tr [2] e-posta: selcuk@cs.bilkent.edu.tr

Özetçe

Yayın şifreleme (YŞ) sistemlerinin amacı, çoklu bir alıcı kümesine yapılan yayınlarda sadece yayını satın almış olan alıcıların deşifre edebileceği şekilde bir şifreleme yapmaktır. Bu sistemdeki kaygılardan birisi yayının olabildiğince az sayıda kopyasının şifrelenmesidir çünkü her yeni şifreleme daha fazla bant genişliği gerektirmektedir. Alıcı kümesi kısıtlı miktarda bedava alıcıya izin verilmek suretiyle rahatlatılırsa şifreleme sayısı dikkate değer biçimde azaltılabilmektedir. Bu makalede literatürdeki en iyi performansa sahip YŞ metotlarından birisi olan Atlamalı Aralık metodu için bedava alıcıların optimal bir şekilde yerleştirilmesi problemi irdelenmiş, optimal yerleştirme algoritmasının yanısıra oldukça hızlı ve isabetli sonuç veren bir bulgusal metot da sunulmuştur.

1. Giriş

Yayın şifreleme (YŞ), büyük alıcı nüfusuna veri transferinde yayının sadece yayına erişim hakkı olan *imtiyazlı* bir alıcı kümesinin deşifre edebileceği şekilde şifrelenmesini amaçlayan kriptografik bir metoddur. Bu teknik genellikle ödemeli TV, içerik koruma, güvenli ses akışı, ve İnternet çoklu gönderimi gibi güvenlikli multimedya uygulamalarında kullanılmaktadır. Tipik olarak, YŞ sistemleri şöyle hayata geçirilir: Cihazlar kullanıcıya satılmadan önce birtakım anahtarlar içerisine gömülür. Yayın yapılacağında ise yayını deşifre edebilmesi gereken tüm kullanıcıların en az bir anahtarı bu yayını açabilecek, yayını açamaması gereken kullanıcılarınsa hiçbir anahtarı yayını açamayacak şekilde bir anahtar kümesi bulunarak şifrelemeler bu anahtarlarla yapılır. Değişik uygulamalarda alıcı küme büyüklüğü, donanım, bant genişliği gibi bazı kaygılar ön plana çıkabilir. Fakat, YŞ sistemlerinde en önemli kaygıların başında kullanıcıda tutulması gereken anahtar sayısı ve yapılması gereken şifreleme dolayısıyla yayınlanması gereken farklı şifreli yayın sayısı gelmektedir.

YŞ sistemlerinde iki ana değerlendirme kriteri vardır. Bunlardan birisi alıcı tarafında tutulması gereken anahtar sayısı, diğeri ise gönderi fazlalık maliyetidir. Günümüze dek önerilmiş en iyi performansa sahip YŞ sistemlerinden ilki Altküme Farkı (AF) metodu [21], ve türevleridir [11], [12]. AF metodu günümüzde de popüler hale gelmiş olup, yeni nesil DVD standardı gibi bazı uygulamalarda halen kullanılmaktadır. Daha sonra ise benzer parametrelere sahip başka YŞ sistemleri önerilmiştir. Bunlardan birisi de Jho vd. [16] tarafından önerilen Atlamalı Aralık (AA) metodudur.

Bir YŞ sisteminde, izinsiz kullanıcıların hiçbirinin yayını açamaması gerektiği genel bir kural olarak varsayılsa da, Abdalla vd. [2] bu varsayımın bazı uygulamalar için gereğinden fazla sıkı olduğunu, ve gönderi maliyetinin bu kural gevşetilerek ciddi ölçüde düşürülebileceğini farketmişlerdir.

1.1. İlgili Çalışmalar

YŞ problemi ilk defa Berkovitz [5] tarafından 1991 yılında ortaya atılmıştır. Daha sonra Fiat ve Naor'un modeli [10] ise YŞ'nin ilk formal modeli olarak kabul edilmiştir. Bu makalede ortaya dayanıklılık kavramını atmış, k-dayanıklılığı k tane izinsiz kullanıcının bir araya gelmesine karşın bilgi elde edememeleri şeklinde tanımlamışlardır. Önerdikleri en iyi metod, n toplam kullanıcı sayısı olmak üzere, her kullanıcının $O(k \log k \log n)$ anahtar tutmasını ve yayın merkezinin $O(k^2 \log^2 k \log n)$'lik mesajlar göndermesini gerektirmektedir.

1999 yılında, Wallner vd. [25] ve Wong vd. [26] birbirlerinden bağımsız biçimde Mantıksal Anahtar Hiyerarşisi'ni (MAH) önerdiler. MAH bir YŞ metodu değildi fakat kullandığı anahtar dağılım şekli YŞ sistemleri için çok uygundu. Bu fikre göre kullanıcılar bir ağacın yapraklarıyla, ağaç içerisindeki her düğüm ise bir anahtarla ilişkilendirilir. Daha sonra her kullanıcıya kök düğümden kendisine ulaşıncaya kadarki yoldaki düğümlerin anahtarları verilir. Bu yöntem Abdalla vd. [2] tarafından YŞ sistemleri için kullanılınca kullanıcılarda tutulan anahtar miktarı logaritmik mertebelere yani $O(\log n)$'e indirilmişti.

Kilometre taşı makalelerinde Naor vd. [21], iki metod önerdiler: Tam Altküme (TA) ve Altküme Farkı (AF) metodları. TA metodu aslında MAH fikrinin YŞ'ye uygunlanmasının güzel bir formalleştirilmesinden başka bir şey değildi. İzinsiz kullanıcı sayısı r olmak üzere, gönderi maliyeti $O(r \log(n/r))$ oluyordu. AF metodu ise $O(\log n)$ olan kullanıcı başına anahtar sayısını $O(\log^2 n)$'ye çıkarma karşılığında gönderi maliyeti $O(r)$'ye indirmeyi başarmıştı. Daha sonra AF'nin farklı türevleri önerildi. Önemli iki türevden birincisi olan Tabakalı AF (TAF), Halevy ve Shamir [12] tarafından önerildi. İdeal kullanımıyla, TAF $O(\log n \log\log n)$'lik bir gönderi maliyetini $O(r \log\log n)$'lik anahtar tutulmasıyla sağlıyordu. İkinci önemli türev olan Katmanlı AF (KAF) ise Goodrich vd. [11] tarafından önerildi. KAF ise $O(r \log n / \log\log n)$'lik gönderi maliyeti $O(\log n)$'lik anahtar tutumuyla sağlıyordu. Benzer sistemlerin [10],[12],[21] analizleri için [13]'e bakınız.

AF metodunun ve türevlerinin önerilmesinin ardından benzer performanslara sahip, Atlamalı Aralık (AA) gibi başka metotlar da önerildi. Jho vd. [16] tarafından önerilen AA metodu da altküme kaplama türünde bir YŞ sistemidir ve farklı bir altküme yapısına sahiptir. Bu sistemde altkümeler tüm kullanıcılar bir doğru üzerinde hayal edilmek kaydıyla, belirli sayıda atlama (yani boş bırakılarak atlanmış kullanıcı pozisyonları) içerebilen belirli bir azami uzunluğa sahip

aralıklar olarak tasarlanmıştır. Bununla birlikte bir şifrelemeyle daha fazla kullanıcıyı kaplayabilmek için tabakalı biçimde düşünülmüştür. Bunun da ötesinde, gönderi maliyetini bir miktar daha düşürebilmek için basamaklı bir türevi de önerilmiştir. Aslında bu son haliyle AA metodu AF metodunun bir genellemesi olarak ortaya çıkmaktadır.

Tüm bunlarla aynı zaman zarfında açık anahtarlı YŞ sistemleri de önerilmiştir. Bunlardan Boneh vd. [6] çiftdoğrusal fonksiyonlar ve çiftdoğrusal Diffie-Hellman üs kararı problemini kullanmıştır. Öte yandan, Boneh ve Hamburg [7] kimliğe dayalı YŞ sistemleri için zemin teşkil eden bir çalışma gerçekleştirdiler. Son zamanlarda, kimliğe dayalı ve açık-anahtar YŞ sistemlerine yoğun bir ilgi ile yaklaşıldı ve çeşitli çalışmalar yapıldı [8], [9], [17], [19], [22].

Aynı zamanda bir gevşetme olarak da görülebilecek olan bedavacı fikri ilk defa Abdalla vd. [2] tarafından önerildi. Bu makalede, bedavacıları etkili biçimde kullanma problemi derinlemesine irdelendi ve bu konunun temelleri atılmış oldu. Ramzan ve Woodruff [23], yakın zamanda TA metodu için bedavacıların kullanımı problemine bir eniyileme algoritması verdiler. Algoritmaları, dinamik programlamaya dayanıyordu. Daha yakın bir zamanda ise Ak vd. [4] aynı problemin AF metodu için olanını çözdüler.

1.2. Katkılar

Bu makalede, AA metodu için bedava alıcıları en etkili biçimde seçerek gönderi maliyetini olabildiğince azaltma problemini ele alıyoruz. İlk olarak, bu metotta, bedavacıların en iyi nasıl yerleştirilebileceğini bulan optimal bir algoritma veriyoruz. Daha sonra ise çok daha hızlı çalışmasına rağmen optimale yakın sonuç veren Yukarıdan Aşağıya (YA) adında bulgusal bir prosedür ortaya koyuyoruz. Son olarak da deneysel sonuçları sunuyoruz.

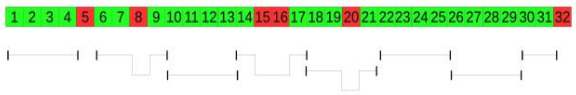
1.3. Yerleşim

Öncelikle 2. bölümde AA metodunu kullanılan şekliyle tanıtıyoruz. 3. bölümde çalışılan problemi formal biçimde ortaya koyuyoruz. 4. bölümde eniyileme algoritmasını, 5. bölümde bulgusal prosedürümüzü açıklıyoruz. 6. bölümde deneysel sonuçları sunduktan sonra 7. bölümdeyse sonuçları yorumlayarak makaleyi bitiriyoruz.

2. Atlamalı Aralık (AA) Metodu

AA metodunda altkümeler, içlerinde *sınırlı sayıda* boşluk bulunan *sınırlı uzunlukta* aralıklar olarak tasarlanmıştır. İşte AA metodundaki başlıca iki parametre olan *a* ve *b* sırasıyla bu azami aralık uzunluğu ve azami boşluk sayısını temsil etmektedir. Dolayısıyla, kullanıcılar hayali bir doğru üzerinde düşünüldüğünde, söz konusu altkümeler, bu parametrelerle oluşacak olan atlamalı aralıklarda bulunan kullanıcıların oluşturduğu altkümelerdir. Bu altkümeler, $S_{i,j;B}$ ile gösterilecektir. Bu gösterimde *i* aralığın başlangıcını, *j* ise sonunu temsil eden sayılar, *B* ise bunlar arasındaki boşlukları ifade eden azami *b* büyüklüğünde bir sayı kümesidir. Örneğin, $S_{3,9;5,8}$ altkümesi denince 3, 4, 6, 7, 9 numaralı kullanıcılar anlaşılmalıdır (Şekil 1). Örnek bir kaplama kümesi ise Şekil 2'de gösterilmiştir.

Şekil 1:Örnek AA altkümesi.



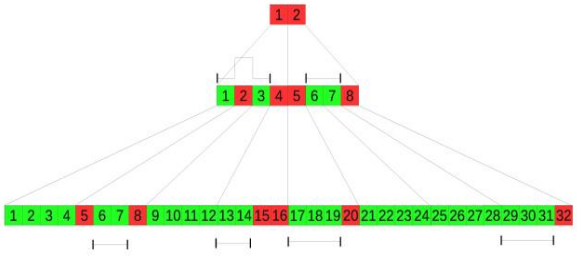
Şekil 2: Örnek AA kaplama kümesi.

Bu şekilde yazılabilecek olan altküme sayısı oldukça çok olsa da orijinal makalede tek yönlü fonksiyonlar kullanılarak kullanıcıda tutulması gereken anahtar sayısı düşürülmüştür. Bu makalede incelenen problem tutulan anahtar sayılarından bağımsız olduğu için bu konuda detaya inmeyi gerekli bulmuyoruz.

Altkümeler bu şekilde tasarlandıktan ve anahtarlar bunlara göre dağıtıldıktan sonra, yayın yapılacağında tek yapılması gereken, imtiyazlı küme için bir kaplama bileşimi bulmaktır. Bu ise en baştan başlayarak tam olarak imtiyazlı kullanıcıları alacak şekilde teker teker gerekli altkümeleri alarak yapılabilecek basit bir işlemdir.

2.1. Katmanlı AA Metodu

Dikkat edilirse, kullanıcıların çoğunun imtiyazlı olması durumunda yukarıda anlatılan temel yöntemde kaplama birçok yanyana atlamasız altküme içerecektir. Dolayısıyla [16] metoda katmanlar ekleyerek bu sorunu çözme yoluna gitmiştir. Bu metotta temel fikir şöyledir: Her katmandaki *a* tane kullanıcı, bir üst katmanda tek kullanıcı olarak düşünülür. Böylece her biri bir üstündekinin *a* katı sayıda kullanıcı içeren $\lfloor \log_a n \rfloor + 1$ tane katman oluşur. Üst katmandaki aralıklar da aynen sıfırıncı katmandaki gibi düşünülür. Örnek bir kaplama Şekil 3'de verilmiştir.



Şekil 3: Örnek katmanlı AA kaplama kümesi.

Katmanlı AA metodunda aralıklar bulundukları katmanı ifade eden yeni bir parametreye daha sahiptirler. $S_{\ell;i,j;B}$ şeklinde ifade edilen bir aralık, ℓ'inci katmandaki $S_{i,j;B}$ aralığını ifade eder.

Kolayca görülebilir ki, katmanlı AA metodunda en iyi kaplamayı bulmak için en üst katmandan başlayarak aşağıya doğru tek katmanlıda olduğu gibi kaplamalar yapılarak inilmesi, bir katman bitince alt katmanlarca kaplanması gerekmeyeceğinden kaplanmış olanların kaplanmış olarak

işaretlenmesi yeterlidir. Bunun en küçük kaplama olduğu aşikardır çünkü bir katmandaki en uzun aralık bir üst katmanda sadece bir düğüme denk gelmektedir.

Jho vd. [16] bunların üzerine basamaklama yöntemini de kullanmışlardır ki böylelikle farklı katmanlardaki aralıkların birbirine eklenmesiyle elde edilen aralıklar da altküme yapısına dahil olmuştur. Fakat bu, ancak % 0.1'den az izinsiz bulunduğunda faydalı olduğundan makalenin olabildiğince açık olması için ele alınmamış, katmanlı AA metodu üzerinde yoğunlaşılmıştır.

3. Problem Tanımı

Tüm altküme kaplama metotlarında olduğu gibi, AA metodunda da belirli sayıda bedavacıya izin verilmek suretiyle gönderi maliyetini düşürmek mümkündür. Burada ortaya çıkan soru şudur: Belirli bir oranda bedavacıya izin verildiği takdirde gönderi maliyeti olabildiğince etkili ve verimli bir biçimde nasıl düşürülebilir?

Problem tanımında ve makalenin geri kalanında kullanacağımız gösterimler şu şekildedir: Tüm kullanıcıların kümesini U, izinsizlerin kümesini R, imtiyazlıların kümesiniyse P ile göstereceğiz. Ayrıca $n = |U|$, $r = |R|$, $p = |P|$ olarak tanımlanacak. Bedavacıların izinsizlere oranını c_f ile gösteriyoruz. İzin verilecek olan toplam bedavacı sayısını ise f ile göstereceğiz. Dolayısıyla $f = r \cdot c_f$ olacak. Bölüm 2.1'de anlatıldığı şekilde, tüm kaplayıcı altkümelerin kümesine S diyeceğiz. Hatırlanacağı üzere katmanlı AA metodunda altkümeler $S_{\ell,i,j,B}$ şeklinde gösteriliyordu. Değişkenleri bu şekilde isimlendirdikten sonra problemi ise şöyle tanımlıyoruz:

$$P \subseteq \bigcup_{S_{\ell;i,j;B} \in C} S_{\ell;i,j;B} \quad \text{ve} \quad \left| \bigcup_{S_{\ell;i,j;B} \in C} S_{\ell;i,j;B} \setminus P \right| \leq f = c_f \cdot r$$

olacak şekilde en küçük $C \subseteq S$'yi bulunuz. Bir başka deyişle, imtiyazlı kullanıcıları tamamen kapsayacak, fakat izinsiz kullanıcılardan en fazla f tanesini içerecek en küçük kaplamayı bulunuz.

4. Optimal Yöntem

Bu bölümde yukarıdaki problem için dinamik programlama ile eniyileme algoritmasını sunacağız.

4.1. Gösterimler

Algoritmaya geçmeden önce kullanacağımız gösterimleri ortaya koyacağız.

Algoritmanın üzerinde çalışacağı temel veriyapısı KA (kullanıcı ağacı) ismiyle iki boyutlu bir matris olacaktır. $KA[k]$, k'ıncı düğüm katmanı olan KA'nın k'ıncı satırını, $KA[k][i]$ ise $KA[k]$ katmanındaki i'inci düğümü gösterecektir. KA veriyapısı aslında Şekil 3'deki yapıyı ifade eder. Aynı zamanda her düğümün bir alt katmandaki sol ve sağ çocuklarına işaretçileri algoritmada ".sol" ve ".sağ" şeklinde eklentilerle gösterilecektir. Ayrıca, ".im" ve ".iz" de düğüm altındaki sırasıyla imtiyazlı ve izinsiz kullanıcı sayısını ifade edecektir. Örneğin, Şekil 3'ye göre, $KA[1][4]$.sol = 13, $KA[1][4]$.im = 2 olmalıdır.

Dinamik programlamanın dolduracağı veriyapısı ise dört boyutlu *maliyet* matrisi olacaktır. *maliyet*$[k][s][e][f]$, k'ıncı katmandaki (s,e) aralığını en çok f adet bedavacı ile kaplamanın minimum maliyeti olsun. Algoritma, $0 \leq k \leq \lfloor \log_a n \rfloor + 1$, $0 \leq i \leq j \leq |KA[k]|$ ve $0 \leq fr \leq f$ değerleri için *maliyet* tablosunu dolduracaktır.

Bunların yanısıra, algoritmada azami a uzunluğunda en çok b atlama içeren olası tüm atlamalı aralık kombinasyonları AA ile gösterilecektir. AA içerisindeki herhangi bir eleman için A değişkeni kullanılıp, A.*atla* ile A'nın içindeki atlama aralıklarının (atlanılan düğüm veya düğüm dizilerinin) kümesi kastedilecektir. Mesela A = $S_{3,9;5,8}$ aralığı için A.*atla* = {[5,5],[8,8]} olacaktır. Fakat A = $S_{3,9;5,7,8}$ olsaydı A.*atla* = {[5,5],[7,8]} olacaktı. Bu aralıkların başları ve sonları ise *.baş* ve *.son* eklentileri ile gösterilecektir. Örneğin *at* = [7,8] ise *at.baş* 7, *at.son* 8 olacaktır.

4.2. Algoritma

Bu bölümde, izinsiz kullanıcılardan belli bir bedavacı oranına izin vererek gönderi maliyetini en çok düşüren algoritmayı vereceğiz. Sözkonusu eniyi kaplama algoritması Algoritma 1'de, yardımcı prosedürü `MaliyetBul` ise Algoritma 2'de verilmiştir.

Algoritma 1. `Eniyileme`
Girdiler: c, a, U, P,R, c_f
1: $k_a \leftarrow \lfloor \log_a n \rfloor + 1$
2: $KA \leftarrow$ `KullanıcıAğacıOluştur`
3: $AA \leftarrow$ `AtlamalıAralıkKombinasyonlarınıYaz`
4: $f \leftarrow c_f \,.\, |R|$
5: **eğer** $f \geq |R|$ **ise**
6: **döndür** 1
7: $k \leftarrow$ **0'dan** k_a**'ya kadar**
8: $son \leftarrow |KA[k]|$**'dan 0'a kadar**
9: $baş \leftarrow son$**'dan 0'a kadar**
10: $fr \leftarrow$ **0'dan** f**'ye kadar**
11: *maliyet*$[k][baş][son][fr] \leftarrow$ `MaliyetBul`$(k,baş,son,fr)$
12: **döndür** *maliyet*$[k_a][0][0][f]$

Eniyi kaplama algoritması şöyle çalışmaktadır: Öncelikle `KullanıcıAğacıOluştur` prosedürü kullanıcıları katmanlar halinde bir veriyapısı (KA) şeklinde düzenler.

Daha sonra kaç tane bedavacıya izin verileceği, verilen c_f oranından hesaplanır. Öncelikle bir kısayol olarak, eğer bedavacı sayısı izinsizlere eşit olabiliyorsa, bir başka deyişle sözkonusu oran 1 ise, herkesi birden en üst düğüm ile alarak yanıt kaplama büyüklüğü olarak 1 döndürülür.

Aksi halde tablo şu şekilde doldurulur:
En alt katmandan başlanıp en üst katmana doğru ilerlenir. Her katmanda olabilecek her ikili arası için belli sayıda

bedavacıya izin verildiği takdirde elde edilecek kaplama büyüklükleri hesaplanacak şekilde döngüler hazırlanır ve sözkonusu her aralık ve bedavacı sayısı için **`MaliyetBul`** prosedürü çalıştırılır. Tablo dolduğunda, yanıt en üst katmanın ilk ve tek düğümünün tablodaki maliyetidir.

`MaliyetBul` Algoritmasını vermeden önce incelenen aralığın maliyetini bulurken belli bir başlangıç düğümü *s* ve belli bir atlamalı aralık *A* için yapılan hesaplamayı *MinMlyt* fonksiyonu ile şöyle buluyoruz:

$$MinMlyt(s,A) = \min_{fsol+fsağ+falt=fr} \left\{ \begin{array}{l} 1 + maliyet(k-1, baş.sol, s.sol-1, fsol) \\ + maliyet(k, s+|A|, son, fsağ) \\ + \min_{falt=fr-fsol-fsağ} \left\{ \sum_{at\in A.atla} maliyet(k-1, at.baş.sol, at.son.sağ, f_{at}) \right\} \\ \qquad \sum_{at\in A.atla} f_{at} = falt \end{array} \right\}$$

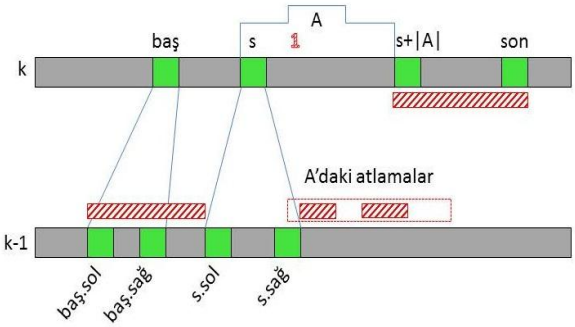
MinMlyt fonksiyonu, aşağıdaki **`MaliyetBul`** algoritmasında, temel bir yapıtaşı olarak kullanılacaktır.

Algoritma 2. `MaliyetBul`
Girdiler: *k, baş, son, fr*

```
1: eğer Σ_{i=baş}^{son} KA[k][i].iz < fr ise
2:     döndür sonsuz
3: eğer Σ_{i=baş}^{son} KA[k][i].im = 0 ise
4:     döndür 0
5: eğer baş = son ise
6:     eğer fr = KA[k][baş].iz ise
7:         döndür 1
8:     eğer fr < KA[k][baş].iz ise
9:         eğer k > 0 ise
10:            çsol ← KA[k][baş].sol
11:            çsağ ← KA[k][son].sağ
12:            döndür maliyet[k–1][çsol][çsağ][fr]
13: döndür min_{baş≤s≤son, A∈AA} {MinMlyt(s, A)}
```

`MaliyetBul` prosedürü girdilerinden anlaşılacağı üzere belli bir katmandaki belli iki düğüm arasına belli sayıda bedavacı verilmesi durumunda burayı kaplamak için gerekecek maliyeti hesaplayıp tabloya yazmakla görevlidir. Bu prosedür iki kısma ayrılabilir: Birincisi temel durumları inceleyen ilk 12 satır, ikincisi ise tablodan yararlanarak özyinelemeli çağrıyı yapan 13. satırdır.

Temel durumlarda, basit kurallar ile hesaplanabilen temel maliyetler tabloya işlenir. Örneğin bir aralığa buradaki izinsiz kullanıcılardan daha fazla bedavacı verilmişse tabloya sonsuz maliyet işlenir. Bir aralıkta hiç imtiyazlı yok ise ve verilen bedavacı sayısı 0 ise tabloya 0 maliyet işlenir. Veya tek düğümlük bir aralık ise verilen bedavacı sayısının yetip yetmemesine göre 1 maliyet işlenir veya alt katmanın tablo kaydından maliyet aktarılır.



Şekil 4: MinMlyt hesabının gösterimi. Taralı alanların her biri MinMlyt hesabındaki toplanan terimlerden birisine karşılık gelmektedir.

Eğer durum temel bir durum değilse, daha önce hesaplanmış tablo değerlerinden minimum maliyet hesaplanır. Burada yapılan, tüm maliyetlerin daha önce hesaplanıp tabloya yazılmış olmasından yararlanarak bu maliyetler arasında en düşük maliyeti bularak tabloya yazmaktır.Şekil 4'te belli bir başlangıç noktası *s* ve aralık *A* için minimum maliyeti bulan *MinMlyt* işlemi görsel olarak açıklanmaktadır. Algoritmada sadelik için *KA*[*k*-1][*baş*].sol yerine *baş*.sol, *KA*[*k*–1][*s*].sol yerine *s*.sol, *KA*[*k*][*s*+|*A*|] yerine *s*+|*A*|, *KA*[*k*][*son*] yerine *son* gibi kullanımlar yapılmıştır.

Sonuç bulunurken tüm $0 < f r < f$ değerlerini ele almaya gerek kalmamaktadır çünkü *maliyet*[*k*][*s*][*e*][*f*], en çok *f* adet bedavacıya izin verilen durumdaki minimum maliyeti ifade ettiği için, *maliyet*[*k*][*s*][*e*][*f*] değerlerinin *f* ile artmayan olması garantilenmiş olmaktadır. Böylece sadece *f* için ortaya çıkan sonuç yeterlidir.

Dikkat edileceği üzere yazmış olduğumuz eniyileme algoritması kaplamanın büyüklüğünü bulmaktadır. Fakat bedavacıların yerleşimleri de tabloda gerekli iz sürme bilgileri tutularak kolayca bulunabilir.

4.3. Performans üzerine

Eniyileme algoritması en düşük maliyetli bedavacı yerleşimini bulmasına karşın, çalışma hızı düşük olmaktadır. Doldurulan dinamik programlama tablosunun boyutları $\log(n)\times n\times n\times f$ dir. Her ne kadar tablonun tümü doldurulmasa da kuramsal olarak $O(\log(n)\ n^2\ f)$ defa MaliyetBul prosedürü çağrılmaktadır. Bu prosedürün çalışma hızı da $O(n \binom{a}{b})$ olacağı için toplam zaman maliyeti $O(\log(n)\ n^3\ f \binom{a}{b})$ olacaktır.

Zaman maliyetini azaltmak için çeşitli stratejiler uygulanabilir. Bunlardan birisi şudur: Herhangi bir katmanda tamamen imtiyazlı kullanıcılar içeren bir düğüm var ise, en iyi çözümlerden birinin bu düğümü bu katmanda kaplaması gerektiği aşikardır. Bu durumda bir alt katmanda bu düğümün solundan başlayıp sağında biten aralıkların hesaplanması

gereksizdir. Dolayısıyla bu aralıklara ilişkin maliyetlerin gerek hesaplanması, gerek tabloya yazılması gerekse maliyet hesap ederken bakılmasına gerek kalmamaktadır. Ne var ki bu sadece ortalama karmaşıklığı azaltmakla beraber en kötü durum karmaşıklığı aynı kalmaktadır.

5. Yukarıdan Aşağıya: Açgözlü bulgusal yöntem

Bu bölümde eniyileme algoritmasına göre çok daha hızlı çalışırken gönderi maliyetini da oldukça iyi ölçüde düşüren bulgusal bir yöntem sunuyoruz. Bu bulgusal yöntem temel olarak şöyle çalışır: En üst katmandan başlamak suretiyle en alt katmana kadar `KatmanKapla` prosedürüyle her katmanı kaplayarak ilerler. (Bkz. Algoritma 3.) Herhangi bir katman içinse `KatmanKapla` prosedürünün işleyişi Algoritma 4'te verilmiştir.

Algoritma 3. `YukarıdanAşağı`
Girdiler: c_f
1: $k_a \leftarrow \lfloor \log_a n \rfloor + 1$
2: $KA \leftarrow$ `KullanıcıAğacıOluştur`
3: $AA \leftarrow$ `AtlamalıAralıkKombinasyonlarınıYaz`
4: $f \leftarrow c_f \cdot r$
5: $d_f \leftarrow f / p$
6: $C \leftarrow \{\}$
7: $k \leftarrow k_a$'**dan** 0'**a kadar**
8: `KatmanKapla`(k, d_f)
9: **döndür** $|C|$

`YukarıdanAşağı` prosedürü öncelikle kaç bedavacıya izin verilebileceğini bulur. Daha sonra bu sayıyı toplam imtiyazlı sayısına bölerek kaç imtiyazlı kullanıcıyı kaplamak için kaç bedavacıya izin verilebileceğine dair bir oran bulur. Bu yeni orana d_f diyoruz. Daha sonra en üst katmandan en alt katmana kadar her katmanı bu orana göre ele alması için `KatmanKapla` prosedürünü çağırır.

Algoritma 4. `KatmanKapla`
Girdiler: k, d_f
1: $sıra \leftarrow 0$
2: $sıra \leq |KA[k]|$ **olduğu sürece**
3: **sırayla tüm** $sıra$ ile başlayan $A \in AA$ **için**:
4: **eğer** $izinsiz(A)/imtiyazlı(A) \leq d_f$ **ise**
5: $C \leftarrow C \cup A$
6: `KaplandıİşaretleA`
7: $sıra \leftarrow sıra + |A| - 1$
8: **döngüyüDurdur**
9: $sıra \leftarrow sıra + 1$

`KatmanKapla` prosedürü belirli bir katman için şöyle çalışır: En baştan başlayarak belli bir *sıra* düğümünden başlayan olabilecek atlamaları aralıklara birer birer bakar ve d_f oranını sağlayan bir atlamalı aralık bulunur bulunmaz bu aralığı kaplamaya ekler ve bu aralığın bir ardındaki düğümden devam eder. Eğer hiçbir atlamalı aralık d_f'yi sağlamazsa *sıra*'yı bir sağa kaydırır; ta ki bu katmandaki tüm düğümler bitene kadar. Bu prosedürde atlamalı aralıklar alındığı takdirde kaplanacak olan izinsiz kullanıcı sayısı $izinsiz(A)$, imtiyazlı kullanıcı sayısı ise $imtiyazlı(A)$ notasyonuyla gösterilmiştir. Benzer şekilde, $izinsiz(C)$ de halihazırda kaplanmış küme olan C'deki izinsiz kullanıcı sayısını, bir başka deyişle halihazırdaki bedavacı sayısını ifade etmektedir.

Bu yöntemle elde edilen sonucun c_f oranının izin verdiği ölçüde bedavacıyı aşmasının mümkün olamayacağı ise d_f'in hesaplanma şeklinden dolayı kesindir. Çünkü öncelikle cf oranını sağlayacak bedavacı sayısı, f, bulunmakta, d_f ise bu sayının imtiyazlılara bölümüyle elde edilmektedir. Yöntemde kaplanan tüm A aralıkları bağımsız olarak d_f oranını sağladıkları için bu aralıkların tamamının toplamı ele alındığında aynı oranın korunacağı ortadadır.

5.1. Performans üzerine

`YukarıdanAşağı` bulgusal metodu, oldukça hızlı ve akla yatkın olmasına karşın, küçük bir sorun vardır. İzin verilen bedavacı sayısının az olması katmanlı yapının sağlayabileceği faydayı sınırlı kılmaktadır.

Bu sorunun üstesinden gelmek için *tolerans* adında yeni bir parametre tanımlıyoruz ve Algoritma 4, 5. satırdaki açgözlü seçimi yaparken sadece d_f yerine $tolerans \cdot d_f$ çarpımını kullanıyoruz. Elbette bununla beraber aralığın alınması durumunda toplam bedavacı sayısının geçilip geçilmeyeceği de kontrol ediliyor ve eğer geçecekse bu aralık alınmıyor. Dolayısıyla, Algoritma 4'ün 4. Satırı şu şekilde değişiyor:

4: **eğer** $izinsiz(A)/imtiyazlı(A) \leq tolerans \cdot d_f$ ve $izinsiz(A) + izinsiz(C) \leq f$ **ise**

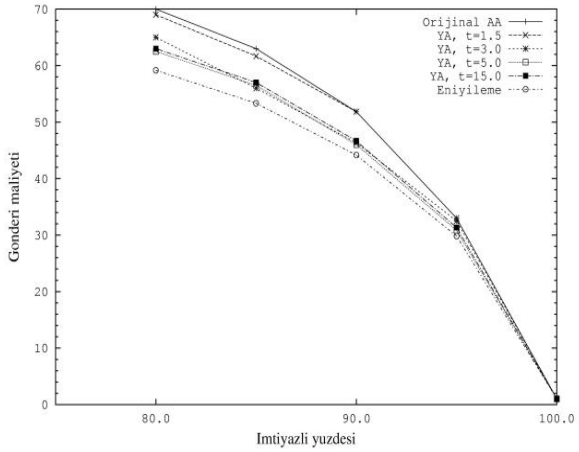
Bu değişikliğin gönderim maliyeti düşürmedeki etkisi Deneyler bölümünde görülebilir.

`YukarıdanAşağı` bulgusal metodunda $\log(n)$ defa `KatmanKapla` prosedürü çalıştırıldığı ve bu prosedürde sırayla mümkün olan tüm atlamalı aralıklar kontrol edildiği için, en kötü durumda çalışma hızı $O(\log(n)\, n \binom{a}{b})$ olmaktadır.

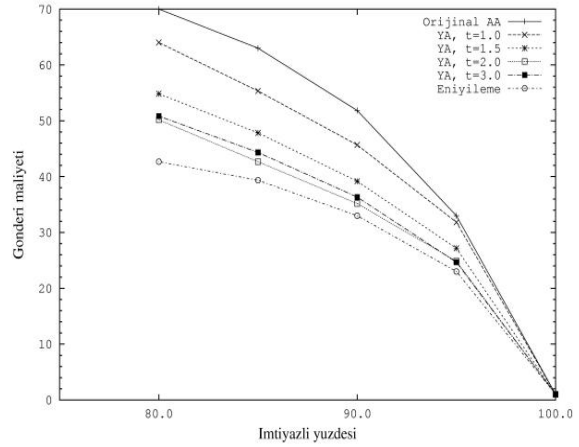
6. Deneyler

Bu bölümde önerilen çözümlerin deneysel değerlendirmesi sunulacaktır. Şekil 5, 6, 7, 8'deki grafiklerde, imtiyazlı oranı %70 ila %100 arasında değişen 1024 kullanıcılık popülasyonlarda a = 4, 8, 16; b = 1, 2 parametreleri ile yapılan deneylerin sonuçları gösterilmektedir. Grafikler, imtiyazlı kullanıcı yüzdesinin fonksiyonu olarak gönderi maliyetlerini, normal AA yöntemi ile karşılaştırmaktadır. Şekiller incelendiğinde görülebilir ki eniyileme algoritması izin verilen bedavacı oranına bağlı olarak, gönderi maliyetinde dikkate değer bir azalma sağlamaktadır. Şekil 8'de görülebilir ki 0.3'lük bir bedavacı oranıyla gönderi maliyeti yarıdan aza indirilebilmektedir.

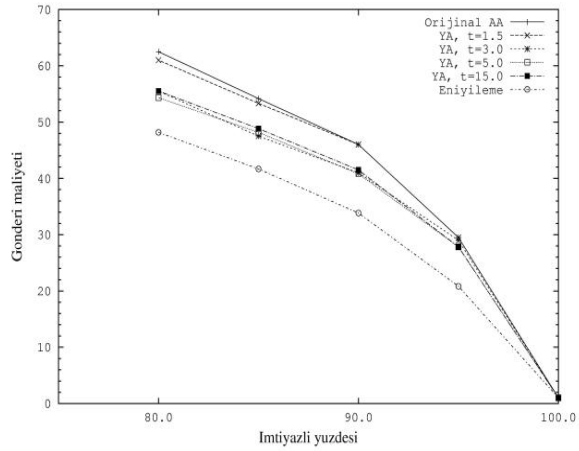
Öte yandan, çok daha pratik olan yukarıdan aşağıya açgözlü bulgusal yöntemi ile eniyileme algoritmasına oldukça yakın sonuçlar elde edilebildiği de gözden kaçmamaktadır. Grafiklerin hemen hepsinde bulgusal yöntemin optimalin sağladığı avantajın yarıdan fazlasını sağlayabildiği görülmektedir.



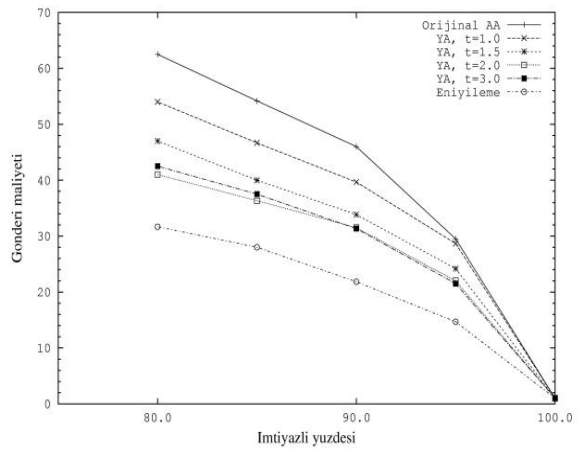
Şekil 5: a=8, b=1, c_f=0.1 için orijinal AA, farklı tolerans değerleri için **YukarıdanAşağı** *metodu, ve eniyileme algoritmasının sonuçları.*



Şekil 6: a=8, b=1, c_f=0.3 için sonuçlar.



Şekil 7: a=8, b=2, c_f=0.1 için sonuçlar.



Şekil 8: a=8, b=2, c_f=0.3 için sonuçlar.

7. Sonuç

Bu makalede AA metodunda bedavacıların, gönderi maliyetini düşürmek için en etkili bir biçimde nasıl kullanılabileceği incelenmiştir. Eniyileme algoritmasının yanısıra parametrelendirilmiş bulgusal bir prosedür olan **YukarıdanAşağı** da önerilmiştir. Eniyileme algoritmasının kuramsal zaman karmaşıklığı O(log(n) n^3 $f\left(\begin{matrix}a\\b\end{matrix}\right)$), bulgusal **YukarıdanAşağı**'nınki ise O(log(n) n $\left(\begin{matrix}a\\b\end{matrix}\right)$)'dir. Bu yöntemlerin gönderi maliyetinde sağladıkları düşüş ise deneylerle ortaya konmuştur. Halen **YukarıdanAşağı** metodu ile aynı mertebede hıza sahip olup en iyi sonuca daha yakın bir yöntem bulma problemi açıktır.

8. Kaynakça

[1] AACS - Advanced Access Content System, http://www.aacsla.com, 2007.

[2] M. Abdalla, Y. Shavitt, and A. Wool. Key management for restricted multicast using broadcast encryption. *IEEE/ACM Trans. Networking*, 8(4):443--454, 2000.

[3] W. Aiello, S. Lodha, and R. Ostrovsky. Fast digital identity revocation. In *CRYPTO'98*, volume 1462 of *LNCS*, pages 137--152. Springer-Verlag, 1998.

[4] M. Ak, K. Kaya, A. A. Selcuk. Optimal Subset-Difference Broadcast Encryption with Free Riders. *Information Sciences* Volume: 179, Issue: 20, Publisher: Elsevier Inc., Pages: 3673--3684

[5] S. Berkovits. How to broadcast a secret. In *EUROCRYPT'91*, volume 547 of *LNCS*, pages 535--541. Springer-Verlag, 1991.

[6] D. Boneh, C. Gentry, and B. Waters. Collusion resistent broadcast encryption with shorter ciphertexts and private keys. In *CRYPTO'05*,

volume 3621 of *LNCS*, pages 258--275. Springer-Verlag, 2005.

[7] D. Boneh and M. Hamburg. Generalized identity based and broadcast encryption schemes. In *ASIACRYPT'08*, volume 5350 of *LNCS*, pages 455--470. Springer-Berlin, 2008.

[8] V. Daza, J. Herranz, P. Morillo, and C. Ráfols. Ad-hoc threshold broadcast encryption with shorter ciphertexts. *Electronic Notes in Theoretical Computer Science*, 192(2):3--15, 2008.

[9] C. Delerableé and D. Pointcheval. Dynamic threshold public key broadcast encryption. In *CRYPTO'08*, volume 5157 of *LNCS*, pages 317--334. Springer-Verlag, 2008.

[10] A. Fiat and M. Naor. Broadcast encryption. In *CRYPTO'93*, volume 773 of *LNCS*, pages 480--491. Springer-Verlag, 1993.

[11] M. T. Goodrich, J. Z. Sun, and R. Tamassia. Efficient tree based revocation in groups of low-state devices. In *CRYPTO'04*, volume 3152 of *LNCS*, pages 511--527. Springer-Verlag, 2004.

[12] D. Halevy and A. Shamir. The LSD broadcast encryption scheme. In *CRYPTO'02*, volume 2442 of *LNCS*, pages 47--60, London, UK, 2002. Springer-Verlag.

[13] J. Horwitz. A survey of broadcast encryption, 2003. Manuscript.

[14] N. Jho, E. Yoo, J. Cheon, and M. Kim. New broadcast encryption scheme using tree-based circle. in Proc. of ACM Digital Rights Management Workshop, 2005, pp.37-44.

[15] N. Jho, J. Hwang, J. Cheon, M. Kim, D. Lee, and E. Yoo, "One-way Chain Based Broadcast Encryption Schemes," Proc. of EUROCRYPT 2005, LNCS 3494, pp. 559-574, 2005

[16] J. Cheon, N. Jho, M. Kim, and E. Yoo, "Skipping, Cascade, and Combined Chain Schemes for Broadcast Encryption," IEEE Transaction on Information Theory 54(11), pp. 5155-5171, 2008

[17] M. Kusakawa, H. Hiwatari, T. Asano, and S. Matsuda. Efficient dynamic broadcast encryption and its extension to authenticated dynamic broadcast encryption. In *CANS'08*, volume 5339 of *LNCS*, pages 31--48. Springer-Verlag, 2008.

[18] S.-T. Li. A platform-neutral live IP/TV presentation system. *Information Sciences*, 140(1-2):33 -- 52, 2002.

[19] Y. R. Liu and W. G .Tzeng. Public key broadcast encryption with low number of keys and constant decryption time. In *PKC'08*, volume 4939 of *LNCS*, pages 380--396. Springer-Verlag, 2008.

[20] J. Lotspiech, S. Nusser, and F. Pestoni. Broadcast encryption's bright future. *Computer*, 35:57--63, 2002.

[21] D. Naor, M. Naor, and J. Lotspiech. Revocation and tracing schemes for stateless receivers. In *CRYPTO'01*, volume 2139 of *LNCS*, pages 41--62. Springer-Verlag, 2001.

[22] J. H. Park, H. J. Kim, M. H. Sung, and D. H. Lee. Public key broadcast encryption schemes with shorter transmissions. *IEEE Transactions on Broadcasting*, 54(3):401--411, 2008.

[23] Z. Ramzan and D. Woodruff. Fast algorithms for the free riders problem in broadcast encryption. In *CRYPTO'06*, volume 4117 of *LNCS*, pages 308--325. Springer-Verlag, 2006.

[24] C. B. S. Traw. Protecting digital content within the home. *Computer*, 34:42--47, 2001.

[25] D. M. Wallner, E. J. Harder, and R. C. Agee. Key management for multicast: Issues and architectures, 1999. Internet draft.

[26] C. K. Wong, M. Gouda, and S. S. Lam. Secure group communication using key graphs. In *SIGCOMM'98*, pages 68--79, September 1998.

Tekil Değer Ayrışımı Tabanlı Yeni Bir Kırılgan Resim Damgalama

Veysel Aslantaş[1] Mevlüt Doğru[2]

[1]Bilgisayar Mühendisliği Bölümü, Erciyes Üniversitesi, Kayseri
[2]Milli Emlak Gen. Müd. Bilgi İşlem Daire Başk., Maliye Bakanlığı, Ankara

[1]e-posta: aslantas@erciyes.edu.tr [2]e-posta: mevlut_dogru@milliemlak.gov.tr

Özetçe

Bu çalışmada Tekil Değer Ayrışımı (Singular Value Decomposition - SVD) tabanlı yeni bir kırılgan damgalama tekniği geliştirilmiştir. Ölçekleme faktörü kullanılarak her bir satırı ölçeklenmiş olan damga resmin, bloklara ayrılmış orijinal resmin her bir satırdaki tekil değerlerine gömülmesiyle damgalanmış resim elde edilmiştir. Önerilen metotta, resmin kalitesini değiştirmeden olabildiğince yüksek saydamlık için ölçekleme faktörü deneysel olarak test edilerek belirlenmiştir. Damgalanmış resme keskinleştirme, yeniden ölçekleme ve döndürme gibi çeşitli saldırılar uygulanarak kırılganlık tespit edilmiştir. Deneysel sonuçlar, orijinal resim ile damgalanmış resmin aynı olduğunu, dolayısıyla da damgalı resmin maksimum saydamlığa ulaştığını göstermektedir.

1. Giriş

Son yıllarda bilgisayar alanındaki gelişmelerle birlikte sayısal ses, resim, video ve metin gibi çoklu ortam dokümanlarının kullanımı ve dağılımı yaygınlaşmıştır. Yüksek hızlı internetin de etkisiyle bu dokümanların kolaylıkla değiştirilebilmesi ve kopyalanabilmesi, telif hakkının korunmasının önemini ortaya koymaktadır.

Sayısal damgalama; ses, resim ve video gibi sayısal verilerin korunmasında yaygın olarak kullanılan tekniklerden biridir. Bu teknikte amaç, bir sayısal verinin damga olarak başka bir sayısal verinin içine gizlenmesidir. Gizlenen bilginin ürün ile birlikte taşınması, gerektiğinde geri elde edilerek kullanılması amaçlanır. Telif hakkının korunması, doküman arşivleme, dokümana ait bilgilerin saklanması ve dijital parmak izi korunması gibi birçok işlemler için sayısal damgalama kullanılmaktadır. Damgalama teknikleri genel olarak; uzaya, görülebilirliğe ve kalıcılığa göre sınıflandırılabilir [1-3].

Damganın gömüleceği uzaya göre damgalama teknikleri, piksel ve frekans uzayı teknikleri olarak iki guruba ayrılmaktadır. Piksel uzayı tekniklerinde damgalama işlemi doğrudan orijinal resmin piksellerine eklenerek gerçekleştirilirken, frekans uzayı tekniklerinde ise SVD, Ayrık Fourier Dönüşümü (Discrete Fourier Transform - DFT), Ayrık Kosinüs Dönüşümü (Discrete Cosine Transform - DCT) ve Ayrık Dalgacık Dönüşümü (Discrete Wavelet Transform - DWT) gibi dönüşüm teknikleri aracılığıyla frekans uzayı katsayılarına damga eklenerek gerçekleştirilmektedir [1,3,4]. Genellikle, frekans uzayı metotları birçok saldırıya karşı piksel uzayı metotlarına göre daha dayanıklıdır [3,5-7].

Damganın görülebilirliğine göre damgalama teknikleri, görünür ve görünmez (saydam) damgalama olmak üzere iki guruba ayrılmaktadır. Görünür damgalar, televizyon yayınlarına eklenmiş logolar gibi insan gözüyle rahatlıkla görülebilmektedir. Bu damgalar orijinal verinin içerisinden kolaylıkla çıkarılabilmektedir. Görünmeyen damgalar ise insan görme sisteminde algılanamayacak şekilde sayısal verinin içerisine eklenen damgalardır [3,8].

Damganın kalıcılığına göre damgalama teknikleri; dayanıklı, kırılgan ve yarı-kırılgan olmak üzere üç gurupta sınıflandırılabilir [4,6]. Dayanıklı damgalamada damga; filtreleme, kesme ve gürültü ekleme gibi çeşitli saldırılara karşı aynı şekilde korunabilir olmalıdır. Kırılgan damgalamada; damgalanmış resme basit bir işlem uygulandığında damga kolaylıkla yok olmalı ya da bozulmalıdır. Bu tür damgalar genellikle veri doğrulama amacıyla kullanılır [4,6,8,9]. Yarı-kırılgan damgalamada ise; damgalanmış resim kayıplı sıkıştırmada kuantalanmış gürültünün eklenmesi gibi belirli saldırılara maruz kaldığında damga bundan etkilenmemeli ancak içerik değişikliği gibi saldırılara karşı damga yok olabilmelidir [6,9]. Kırılgan damgalama yönteminde damgalanmış resimdeki damga insan gözüyle fark edilemez. Güvenlik açısından doğrulama amacına uygun olarak da resimler yetkisiz kişiler tarafından değiştirilmemelidir. Bunun için, kırılgan damgalama yöntemi kullanılarak orijinal verinin bozulup bozulmadığı hakkında bilgi alınabilmektedir.

SVD, damgalama dahil olmak üzere bir çok nümerik uygulamalarda güçlü bir nümerik analiz tekniği olarak kullanılmaktadır. Bu çalışmada, gri seviye resimler için SVD tabanlı kırılgan bir damgalama tekniği önerilmiştir. Ölçekleme faktörü (Scaling factor - SF) kullanılarak her bir satırı ölçeklenmiş damga resmin, bloklara ayrılmış orijinal resmin her bir satırdaki tekil değerlerine (Singular Value - SV) eklenmesiyle damgalanmış resim elde edilmektedir. Literatürde, en

yüksek saydamlığa ulaşacak şekilde ölçekleme faktörünün belirlenmesinde farklı yapay zekâ teknikleri kullanan kırılgan damgalama [10-12] teknikleri mevcuttur. Bu çalışmada ise ölçekleme faktörü deneysel olarak test edilerek belirlenmiştir. Deneysel sonuçlar, saydamlık açısından geliştirilen tekniğin başarılı olduğunu göstermektedir.

2. SVD Tabanlı Damgalama

SVD'nin görüntü işleme uygulamalarındaki temel amaçları; resmin tekil değerlerini küçük saldırılar olduğunda önemli değişimlere karşı kararlı tutmak ve tekil değerlerin resmin gerçek cebirsel özelliklerini göstermesini sağlamaktır.
SVD ile MxN boyutlarındaki bir A matrisi $A=USV^T$ olacak şekilde üç ayrı matrisin çarpımına eşitlenebilir. Burada MxN boyutlarındaki U ve NxN boyutlarındaki V^T ortogonal matris, NxN boyutundaki S ise köşegen matristir. Köşegen elemanları dışındaki elemanları sıfır olan S matrisi, A matrisinin tekil değerleri olarak adlandırılır [13-15].

2.1. Damga Gömme

Orijinal resim (I) ile damganın (W) boyutlarının NxN olduğu ve k'nın da ölçekleme faktörü olduğu varsayılırsa, SVD ile damgalama için aşağıdaki adımlar sırasıyla uygulanmıştır.

- Orijinal resim, 32x32'lik resim bloklarına bölünür.
- Her bir bloğa SVD uygulanır.

$$I = USV^T \quad (1)$$

- S matrisine k ölçekleme katsayısı ile çarpılan damga eklenir.

$$S_M=S+kW \quad (2)$$

- Damgalanmış resim blokları hesaplanır.

$$I_W = US_MV^T \quad (3)$$

- Damgalanmış resim blokları birleştirilerek damgalanmış resim (I'_W) elde edilir.

2.2. Damga Çıkarma

Genel olarak damga çıkarma işlemi gömme işleminin tersi olarak ifade edilebilir. Damga çıkarma esnasında, damgalanmış resimden çıkarılan damga ve çıkarılan resim üzerinde bozulmaların olması muhtemeldir. SVD ile damgalanmış resimden damga çıkarma işlemi için aşağıdaki adımlar sırayla uygulanmıştır.

- Damgalanmış resim bloklarına (muhtemelen bozulmuş) SVD uygulanır.

$$I_W = U'S'_MV'^T \quad (4)$$

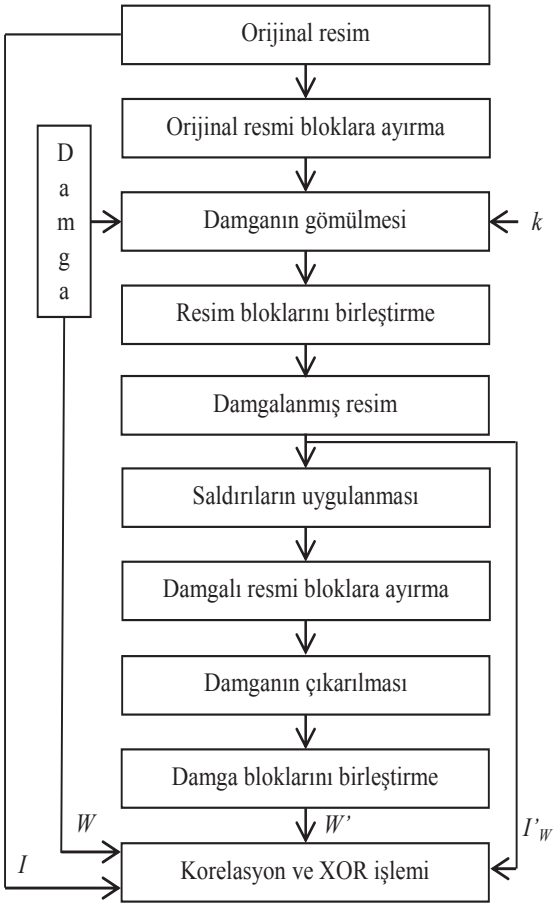
- Orijinal resmin S matris blokları SI olarak birleştirilir.
- Damga (muhtemelen bozulmuş) bloklar halinde çıkarılır.

$$W_S= (S'_M-SI) / k \quad (5)$$

- Damga blokları birleştirilerek çıkarılan damga (W') elde edilir.

3. SVD Kullanılarak Geliştirilen Kırılgan Damgalama

Geliştirilen SVD tabanlı damga gömmenin blok diyagramı Şekil 1'de gösterilmektedir. Gömme işlemi, SF kullanılarak bölüm 2.1'de verilen bilgilere göre bloklara ayrılmış orijinal resmin her bir satırdaki tekil değerlerinin değiştirilerek yeni tekil değerlerinden oluşan damgalanmış resmin elde edilmesiyle yapılmaktadır. Saldırıya uğramış veya uğramamış damgalanmış resimden damgalar da bölüme 2.2'de verilen bilgilere göre çıkarılmıştır. Bu işlemler sonucunda çıkarılan ikili (binary) damganın piksellerinde SF'nin etkisiyle değişimler olabileceğinden, çıkarılan damganın piksel değerleri 0.5'den daha küçük olanlar 0'a ve 0.5'den daha büyük olanlar da 1'e çekilerek yeniden ikili damga elde edilmiştir.



Şekil 1: SVD tabanlı damga gömmenin blok şeması.

İki boyutlu korelasyon değeri sayesinde orijinal resim ile damgalanmış resim ($corr_I = corr\ (I, I'_W)$) arasındaki benzerlik, XOR lojik operatörü sayesinde de aşağıdaki formüle göre orijinal damga ile çıkarılan damga arasındaki benzerlik hesaplanmıştır.

$$xor_W = \sum(\sum(xor(W, W'))) \quad (6)$$

Çeşitli veri doğrulama işlemleri için farklı damgalama uygulamaları kırılganlık testi gerektirebilir. Bu çalışmada damganın kırılganlığını test edebilmek için literatürde kullanılan beş farklı saldırı türü uygulanmıştır. Bunlar; keskinleştirme (KS), yeniden ölçekleme (YO), döndürme (DN), median filtreleme (MF) ve gausian gürültüdür (GG). Damgalanmış resimlere bu saldırılar uygulanarak çıkarılan damgalara göre kırılganlık tespit edilmiştir. Geliştirilen modelin esnekliğinden dolayı farklı saldırılar da uygulanabilir.

4. Deneysel Sonuçlar

Geliştirilen metodu değerlendirmek için damga olarak Şekil 2'de gösterilen 64x32 boyutundaki ikili resim; kaynak resim olarak da 256x256 boyutlarındaki Şekil 3'de gösterilen Lena ve Şekil 4'de gösterilen Baboon resimleri kullanılmıştır. Şekil 2'de gösterilen damga resmi üretilirken öncelikle 32x32'lik resmin 32x16'lık iki bloktan sağ taraftaki blok, soldaki 32x16'lık bloğun altına yerleştirilmiştir. Daha sonra, elde edilen 64x32'lik yeni damga resminin sağ tarafındaki 64x16'lık kısmı siyah yapılmıştır.

Test aşamasında yöntemin saldırılara karşı kırılganlığını ölçmek için KS (3x3), YO (bilineer: 256→128→256), DN (bilineer: 30^0), MF (3x3) ve GG (ortalama=0, varyans=0,01) işlemleri uygulanmıştır. Saldırılar sonrasında Lena ve Baboon damgalanmış resimlerinden çıkarılan damgalar Şekil 5' de verilmiştir. Bu resimlerden, orijinal damgaya göre çıkarılan damganın tamamen bozulduğu görülmektedir.

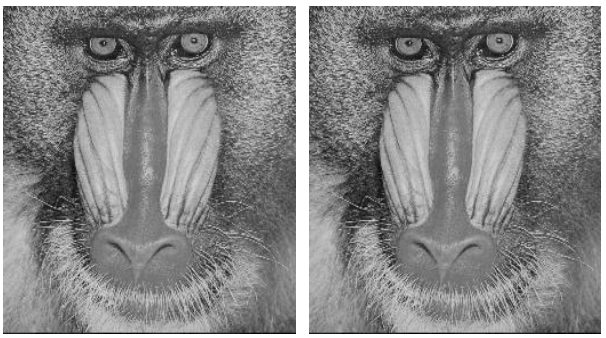
Maksimum saydamlık için başlangıçta (0-1) aralığında rastgele seçilen SF değeri, deneysel testler sonucunda Şekil 3 ve Şekil 4'de gösterilen kaynak resimlere göre en uygun (0.1-0.4) aralığı olarak belirlenmiştir. SF; 0.4'den daha büyük bir değer seçilirse saydamlığın azalmasına neden olurken, 0.1'den daha küçük bir değer seçilirse MF saldırısından sonra çıkarılan damgadaki bozulmayı azaltmaktadır.

Ölçekleme faktörü 0.1 seçilerek kaynak resimlere göre elde edilen korelasyon ve XOR değerleri Tablo 1'de verilmiştir. Buradaki xor_W değeri, 64x32'lik orijinal damga ve çıkarılan damga resimlerinin sağ tarafındaki 64x16'lık siyah kısımları atıldıktan sonra piksel değerleri 0 ve 1'lerden oluşan 64x16 boyutundaki orijinal ve çıkarılan damga resimlerine göre hesaplanmıştır. Tablo sonuçları incelendiğinde, farklı kaynak resimlerin her ikisinde de $corr_I$ değerinin 1 çıkması maksimum saydamlığın sağlandığını göstermektedir. Saldırıya uğramış damgalanmış resimden çıkarılan damganın orijinal damgaya

Şekil 2: Damga resmi.

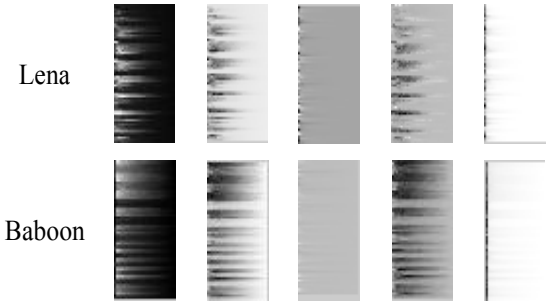
(a) (b)

Şekil 3: (a) Orijinal Lena resmi, (b) Damgalanmış resim.



(a) (b)

Şekil 4: (a) Orijinal Baboon resmi, (b) Damgalanmış resim.



(a) KS (b) YO (c) DN (d) MF (e) GG

Şekil 5: Saldırılar sonrası damgalanmış resimlerden çıkarılan damga.

Tablo 1: Farklı resimlere göre elde edilen korelasyon ve XOR değerleri.

	$corr_I$	xor_W					
		Saldırısız	KS	YO	DN	MF	GG
Lena	1	0	407	618	501	591	612
Baboon	1	0	412	615	555	616	612

benzerliğini minimize ederek de saldırılara karşı en iyi kırılganlık elde edilmiş olacağından, xor_W değerinin 0'dan daha büyük çıkması gerekmektedir. Bu değer, saldırı uygulamadan 0 çıkarak damgalar arası tamamen benzerliği, kullanılan her iki kaynak resimde yaklaşık aynı olmak üzere saldırının türüne göre (407-612) arasında değişerek de bu tekniğin kırılgan bir damgalama olduğunu göstermektedir. Buradan, geliştirilen SVD tabanlı damgalama tekniğinin hem saydamlık hem de kırılganlık açısından başarılı olduğuna ulaşılmaktadır.

5. Sonuçlar

Bu çalışmada SVD tabanlı yeni bir kırılgan resim damgalama tekniği sunulmuştur. Ölçekleme faktörü kullanılarak her bir satırı ölçeklenmiş damganın, bloklara ayrılmış orijinal resmin her bir satırdaki tekil değerlerine gömülmesiyle damgalanmış resim elde edilmiştir. Önerilen metotta, resmin kalitesini değiştirmeden olabildiğince yüksek saydamlık için ölçekleme faktörü deneysel testler ile elde edilmiştir. Deneysel sonuçlar, orijinal resim ile damgalanmış resmin ve saldırı uygulamadan çıkarılan damga ile gömülen damganın tamamen aynı olduğunu göstermektedir. Orijinal resim ile damgalanmış resmin aynı olması, damgalanmış resmin en yüksek saydamlığa ulaştığını göstermektedir.
Kırılgan damgalama tekniği sayısal verilerin bozulup bozulmadığının testi için kullanıldığından kırılganlığın tespiti için KS, YO, DN, MF ve GG saldırıları damgalanmış resme uygulanmıştır. Saldırılar sonucunda çıkarılan damgalar incelendiğinde, damganın bozulduğu tespit edilmiştir. Geliştirilen modelin esnekliğinden dolayı farklı saldırılar da uygulanarak metodun başarısının değişmediği gözlemlenebilir.

6. Kaynakça

[1] Hartung, F., Kutter, M., "Multimedia watermarking techniques", Proc. IEEE 1999; 87: 1079–107.
[2] Petitcolas, F.A.P., Anderson, R.J., M.G. Kuhn, "Information hiding—A survey", Proceedings of IEEE 1999; 87:1062–78.
[3] Potdar, V., Han, S., Chang, E., "A Survey of Digital Image Watermarking Techniques", Proceedings of the 3rd international IEEE conference on industrial informatics (INDIN 2005), Perth Western Australia, 10-12 Aug. 2005.
[4] Lee, S.J., Jung, S.H., "A Survey of Watermarking Techniques Applied to Multimedia", ISIE 2001, Pusan, Korea, 272-277.
[5] Aslantas, V., "A singular-value decomposition-based image watermarking using genetic algorithm", Int. J. Electron. Commun. (AEU), 386-394, 2008.
[6] Aslantas, V., "An optimal robust digital image watermarking based on SVD using differential evolution algorithm", Optics Communications 282, 769–777, 2009.
[7] Arya, D., "A Survey of Frequency and Wavelet Domain Digital Watermarking Techniques", International Journal of Scientific & Engineering Research, Vol. 1, Iss. 2, Nov. 2010.
[8] Shieh, C., et al., "Genetic Watermarking Based on Transform-domain Techniques", Pattern Recognition Society, 37(3), 555-565, 2004.
[9] Hassan, M.H., Gilani, S.A.M., **"**A Semi-Fragile Watermarking Scheme for Color Image Authentication", World Academy of Science, Engineering and Technology 19, 2006.
[10] Aslantas, V., Ozer, S., Ozturk, S., "A Novel Clonal Selection Algorithm Based Fragile Watermarking Method", LNCS, 4628, pp. 358-369, 2007.
[11] Aslantas, V., Ozer, S., Ozturk, S., "A Novel Fragile Watermarking Based on Particle Swarm Optimization", IEEE Int. Conf. on Multimedia and Expo, Hannover, Germany, 269-72, 2008.
[12] Aslantas, V., Ozer, S., Ozturk, S., "Improving the performance of DCT-based fragile watermarking using intelligent optimization algorithms" Optics Commun., Vol. 282, No 14, 2806-2817, 2009.
[13] Aslantas, V., "An SVD Based Digital Image Watermarking Using Genetic Algorithm", International Conference on Information Sciences, Signal Processing and its Applications, Sharjah, U.A.E., 2007.
[14] Aslantas, V., "Optimal SVD based Robust Watermarking using differential evolution algorithm", Proceedings of the World Congress on Engineering 2008, Vol I, London, U.K., 2008.
[15] Liu, R., Tan, T., "An SVD-based watermarking scheme for protecting rightful ownership." IEEE Trans. Multimedia, Vol. 4, No. 2, 2002.

Bilişim Güvenliği : Kullanıcı Açısından bir Durum Tespiti

Atila Bostan[1] İbrahim Akman[2]

[1,2] Bilgisayar Mühendisliği Bölümü,Atılım Üniversitesi, Ankara

[1]e-posta: abostan@atilim.edu.tr [2]e-posta: akman@atilim.edu.tr

Özet

Bilişim teknolojisinde güvenliği sağlama konusunda, kullanıcı farkındalığı ve kazanılmış davranış alışkanlıkları, en zayıf noktalar olarak kabul edilmenin yanında, vazgeçilmez bileşenleri oluşturmaktadır. Bilgisayar ve iletişim güvenliğini yüksek seviyede sağlamak amacıyla mevcut teknolojilerin kullanımı için yoğun bir uğraş verilmekteyken, yeterli güvenlik seviyesine erişmede kullanıcılar ve onların gerçek hayat uygulamaları önemli rol oynamaktadır. Bu çalışmada, güvenlik farkındalığı ve uygulamaları konusunda 466 katılımcı üzerinde yaptığımız anket çalışması sonuçlarına dayalı olarak, kullanıcıların bilgisayar ve web güvenliği konusundaki hassasiyet ve farkındalıkları ile yaş, cinsiyet, bilgi ve iletişim teknolojileri kullanım deneyimi ve eğitim seviyesi ilişkisini belirlemeye çalıştık.

Giriş

Otomatik veri işleme tekniklerinden faydalanarak iş süreçlerinin geliştirilmesi ve modernizasyonu, bilgisayar ağlarını kullanmayı neredeyse alternatifsiz bir teknoloji haline getirmiştir. Günümüzde orta ve büyük ölçekli firmalar hem kendi iş süreçlerinin idaresi ve takibi için hem de müşterilerine verdiği hizmeti ve tanıtımı yaygınlaştırabilmek için bilgisayar ağlarından faydalanmaktadır. Her ne kadar sadece firma/kurum içi bilgisayar ağı kullanımı mümkün olsa da firma dışı sistemler ile entegrasyon, İnternet gibi çok yaygın bir ağın sağladığı ortam ve hizmetlere ulaşma ihtiyacı (firma/kurum fonksiyonlarını etkin olarak yerine getirebilmek için), İnternet ağına çevrim-içi erişmeyi gerektirmektedir. İnternet gibi genele açık ve kontrolü zor bir ortama bağlantı kurmak şüphesiz beraberinde bir çok güvenlik ihtiyacını da gündeme getirmektedir. İş süreçlerinde gizliliği ve kişiselliği sağlamak için bilginin emniyetli ve güvenli metotlarla işlenmesi gereklidir. Bu özellikler genellikle ağ ve bilgi güvenliği olarak adlandırılmaktadır. Sayısal ortamlarda güven ifadesi aktörlerin kimliğinin onaylanmasını içerirken, gizlilik ifadesi ise yetkisiz erişimin/dinlemenin, içerik değiştirmenin ve hizmet kesintisinin engellenmesi konularını kapsamaktadır.

Bilgi sistemleri güvenliğinin başarısı büyük oranda son kullanıcı davranışları ve farkındalığına bağlıdır [1]. Güvenlik mekanizmaları insanlar tarafından tasarlandığı, uygulandığı, işletildiği ve aynı zamanda yine insanlar tarafından ihlal edildiği için, bu sistemlerin tasarımında insani faktörleri göz önüne alınmalıdır [2]. Bilgisayar ve iletişim güvenliğini en yüksek seviyede sağlamak için mevcut teknolojilerin kullanımı konusunda yoğun bir uğraş verilmekteyken, son yapılan araştırmalar güvenlik ihlallerinin yıllar bazında artış gösterdiğini ortaya koymaktadır. Computer Security Institute'un 2008 [3] ve 2009 [4] raporları, kötü amaçlı yazılım bulaşması, e-posta yemlemesi ve web aldatma yöntemlerini en çok izlenen ihlaller olarak belirtmektedir. Güvenlik ihlallerinin çoğunda temel unsur olarak, kullanıcı davranışlarındaki farkındalık eksikliği belirtilmektedir. Buna rağmen gerçek güvenlik uygulamalarında, kullanıcı farkındalığı eğitimlerinin en az önem verilen konu olduğu tespit edilmiştir [1]. Hatta, kullanıcılar güvenli kullanımı temin edecek tedbirlerin teknik olarak farkında olsalar bile, yanlış/hatalı davranışta bulunabilmektedirler. Güvenli kullanımı temin etmede teknik farkındalığın yeterli olmadığını ve kullanıcıların her zaman bilgileri/inançları doğrultusunda davranmadıklarına işaret eden araştırmalar mevcuttur [5,6]. Uygulamalarda güvenli kullanım yöntemlerinin, kullanıcılar tarafından, kazanılması, içselleştirilmesi ve alışkanlık haline getirilmesine ihtiyaç vardır [6]. Bilgi güvenliği mekanizmalarını geliştirirken, kullanıcı davranışları ve güdülerine odaklanılmasının gerekli olduğu konusunda araştırmacılar çoğunlukla hemfikirdir [7,8,9]. Diğer taraftan, güvenlik mekanizmalarının etkinliğini değerlendirebilmek için, deneysel laboratuar ortamlarından ziyade, gerçek hayat uygulamaları incelenmelidir [8].

Sunulan bu çalışmada, kullanıcıların sayısal ortam güvenliği konusunda farkındalık seviyelerinin yanında, gerçek hayat güvenlik uygulamalarını incelemeyi esas aldık. 466 katılımcı ile 12 sorudan oluşan bir bilgi güvenliği farkındalığı anketi gerçekleştirdik. Anketi, iş süreçleri ve bilgi paylaşımında en çok kullanılan araçlar olmaları sebebi ile, kişisel bilgisayar güvenliği ve bu konudaki davranış şekilleri/kalıpları, ve güvenli web konuları ile sınırlı tuttuk. Bunun paralelinde, katılımcıların demografik bilgilerini aldığımız dört sorunun haricinde anketteki sorular bilgi ve iletişim teknolojileri kullanımı, kişisel bilgisayar kullanımında gerçek hayat uygulamaları, güvenli web kullanımında farkındalık ve davranış alışkanlıkları olmak üzere iki ana başlık altında gruplandırıldı.

Metodoloji

Ulusal ve uluslararası literatüre incelendiğinde bilişim üzerine yapılan çalışmalarda yaş, cinsiyet, eğitim ve deneyimin önemli demografik faktörler arasında yer aldığı görülmektedir. Örneğin, eserlerinde Rahim, Rahaman, Seyal [10], Lau, [11] yaş, cinsiyet, eğitim ve deneyimin bilişim etiği konusunda bireylerin davranışları konusunda anlamlı etkisi olduğunu göstermişlerdir. Benzer şekilde Levy [12] ve, Lian ve Lin [13] yapmış oldukları çalışmada cinsiyet, eğitim, yaş gibi demografik faktörlerin bilişim teknolojilerinin sağladığı fırsatlardan yararlanma üzerinde önemli etkileri bulunduğunu saptamışlardır. Diğer iki çalışmada ise Colley ve Maltby [14] ve Yang ve Tung [15] İnternet çalışmalarında sosyo-demografik faktörlerin göz önüne alınması gerektiği ve bu türden çalışmaların halen araştırılmaya muhtaç olduğu belirtilmiştir. Nitekim, Zhang [16] ve Jaeger [17] yapmış oldukları çalışmalarda kişilerin bazı demografik özelliklerinin bilişim alanında çeşitli faktörler ve algılamalar üzerinde anlamlı etkileri olduğu sonucuna varmışlardır.

Yukarıda verilen nedenlerle, bu bildiride, seçilmiş sosyo-demografik faktörler ile seçilmiş bilgisayar ve web kullanım güvenliği farkındalığı arasındaki ilişki incelenmektedir. Çalışmada kullanılacak olan sosyo-demografik faktörler bağımsız değişkenler olarak ele alınmak üzere

1) yaş (değişken adı: yaş),
2) Cinsiyet (değişken adı: cins),
3) Eğitim (değişken adı: eğit),
4) Deneyim (değişken adı: dene)

kalemlerinden oluşmaktadır. Bağımlı değişkenler ise bilgisayar ve web güvenliği farkındalığı altında iki temel kategoride ele alınmıştır. Bu kategoriler altında yer alan değişkenler ile bunlara karşılık gelen hipotezler aşağıda verilmektedir.

Bilgisayar Güvenliği: Bu kategoride yer alan değişkenler:

1) Kişinin bilgisayar güvenliği konusunda bilgi düzeyi (Y_1),
2) Kişinin kullanılan bilgisayar üzerinde önemli bilgi saklayıp saklamadığı (Y_2),
3) Kişinin bilgisayarında bulunan bilgileri yedekleme sıklığı (Y_3),
4) Kişinin bilgisayarında güvenlik taraması sıklığı (Y_4),
5) Kişinin bilgisayarında lisanslı bir virüs koruma sistemi kullanıp kullanmadığı (Y_5)

Bu çerçevede kurulan hipotezler aşağıda verilmektedir (Tablo 1-Tablo 4).

Tablo 1: Yaş ve Bilgisayar güvenliği hipotezleri

Hipotez	Tanım
$H1_{yaş,Y1}$	Yaş ile kişinin bilgisayar güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
$H1_{yaş,Y2}$	Yaş ile kişinin kullanılan bilgisayar üzerinde önemli bilgi saklayıp saklamadığı arasında anlamlı bir ilişki vardır.
$H1_{yaş,Y3}$	Yaş ile kişinin bilgisayarında bulunan bilgileri yedekleme sıklığı arasında anlamlı bir ilişki vardır.
$H1_{yaş,Y4}$	Yaş ile kişinin bilgisayarında güvenlik taraması sıklığı arasında anlamlı bir ilişki vardır.
$H1_{yaş,Y5}$	Yaş ile kişinin bilgisayarında lisanslı bir virüs koruma sistemi kullanıp kullanmadığı arasında anlamlı bir ilişki vardır.

Tablo 2: Cinsiyet ve Bilgisayar güvenliği hipotezleri

Hipotez	Tanım
$H1_{cins,Y1}$	Cinsiyet ile kişinin bilgisayar güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
$H1_{cins,Y2}$	Cinsiyet ile kişinin kullanılan bilgisayar üzerinde önemli bilgi saklayıp saklamadığı arasında anlamlı bir ilişki vardır.
$H1_{cins,Y3}$	Cinsiyet ile kişinin bilgisayarında bulunan bilgileri yedekleme sıklığı arasında anlamlı bir ilişki vardır.
$H1_{cins,Y4}$	Cinsiyet ile kişinin bilgisayarında güvenlik taraması sıklığı arasında anlamlı bir ilişki vardır.
$H1_{cins,Y5}$	Cinsiyet ile kişinin bilgisayarında lisanslı bir virüs koruma sistemi kullanıp kullanmadığı arasında anlamlı bir ilişki vardır.

Tablo 3: Eğitim ve Bilgisayar güvenliği hipotezleri

Hipotez	Tanım
$H1_{eğit,Y1}$	Eğitim ile kişinin bilgisayar güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
$H1_{eğit,Y2}$	Eğitim ile kişinin kullanılan bilgisayar üzerinde önemli bilgi saklayıp saklamadığı arasında anlamlı bir ilişki vardır.
$H1_{eğit,Y3}$	Eğitim ile kişinin bilgisayarında bulunan bilgileri yedekleme sıklığı arasında anlamlı bir ilişki vardır.
$H1_{eğit,Y4}$	Eğitim ile kişinin bilgisayarında güvenlik taraması sıklığı arasında anlamlı bir ilişki vardır.
$H1_{eğit,Y5}$	Eğitim ile kişinin bilgisayarında lisanslı bir virüs koruma sistemi kullanıp kullanmadığı arasında anlamlı bir ilişki vardır.

Tablo 4: Deneyim ve Bilgisayar güvenliği hipotezleri

Hipotez	Tanım
$H1_{dene,Y1}$	Deneyim ile kişinin bilgisayar güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
$H1_{dene,Y2}$	Deneyim ile kişinin kullanılan bilgisayar üzerinde önemli bilgi saklayıp saklamadığı arasında anlamlı bir ilişki vardır.
$H1_{dene,Y3}$	Deneyim ile kişinin bilgisayarında bulunan bilgileri yedekleme sıklığı arasında anlamlı bir ilişki vardır.
$H1_{dene,Y4}$	Deneyim ile kişinin bilgisayarında güvenlik taraması sıklığı arasında anlamlı bir ilişki vardır.
$H1_{dene,Y5}$	Deneyim ile kişinin bilgisayarında lisanslı bir virüs koruma sistemi kullanıp kullanmadığı arasında anlamlı bir ilişki vardır.

Web web güvenliği : Bu kategoride yer alan değişkenler:

6) Kişinin web sayfaları güvenliği konusunda bilgi düzeyi (Y_6),
7) Kişinin güvenli web sitelerinin nasıl ayırt edileceği konusundaki bilgisi (Y_7),
8) Kişinin web siteleri sertifika hatası kavramı hakkında bilgisinin olması (Y_8),

Belirtilen değişkenlere karşılık gelen hipotezler aşağıdaki tablolarda verilmektedir (Tablo 5-Tablo 8).

Tablo 5: Yaş ve web güvenliği hipotezleri

Hipotez	Tanım
$H2_{yaş,Y6}$	Yaş ile kişinin web sayfaları güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
$H2_{yaş,Y7}$	Yaş ile kişinin güvenli web sitelerinin nasıl ayırt edileceği konusundaki bilgisi arasında anlamlı bir ilişki vardır.
$H2_{yaş,Y8}$	Yaş ile kişinin web siteleri sertifika hatası kavramı hakkında bilgisi arasında anlamlı bir ilişki vardır.

Tablo 6: Cinsiyet ve web güvenliği hipotezleri

Hipotez	Tanım
$H2_{cins,Y6}$	Cinsiyet ile kişinin web sayfaları güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
$H2_{cins,Y7}$	Cinsiyet ile kişinin güvenli web sitelerinin nasıl ayırt edileceği konusundaki bilgisi arasında anlamlı bir ilişki vardır.
$H2_{cins,Y8}$	Cinsiyet ile kişinin web siteleri sertifika hatası kavramı hakkında bilgisi arasında anlamlı bir ilişki vardır.

Tablo 7: Eğitim ve web güvenliği hipotezleri

Hipotez	Tanım
$H2_{eğit,Y6}$	Eğitim ile kişinin web sayfaları güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
$H2_{eğit,Y7}$	Eğitim ile kişinin güvenli web sitelerinin nasıl ayırt edileceği konusundaki bilgisi arasında anlamlı bir ilişki vardır.
$H2_{eğit,Y8}$	Eğitim ile kişinin web siteleri sertifika hatası kavramı hakkında bilgisi arasında anlamlı bir ilişki vardır.

Tablo 8: Deneyim ve web güvenliği hipotezleri

Hipotez	Tanım
$H2_{deney,Y6}$	Deneyim ile kişinin web sayfaları güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
$H2_{deney,Y7}$	Deneyim ile kişinin güvenli web sitelerinin nasıl ayırt edileceği konusundaki bilgisi arasında anlamlı bir ilişki vardır.
$H2_{deney,Y8}$	Deneyim ile kişinin web siteleri sertifika hatası kavramı hakkında bilgisi arasında anlamlı bir ilişki vardır.

Araştırma Yöntemi

Önerilen hipotezlerin test edilmesi amacıyla bir taslak anket formu hazırlanmıştır. Bu anket formu uygulanmadan önce bir pilot çalışma gerçekleştirilmiş ve ayrıca konunun uzmanı olan kişilerle görüşülmüştür. Tüm bu çalışmalar sonucunda elde edilen görüş ve öneriler anket formuna olabildiğince yansıtılmaya çalışılarak bu form son haline getirilmiştir. Anket formu Tablo 9'da özetlenmektedir. Bu tablodan da görüleceği gibi, anket formu 12 soru içermektedir. Bu soruların tanımları ve karşılık gelen cevap değerleri ile değişken sembolleri yine Tablo 9'da verilmektedir.

Anket Elektrik Mühendisleri Odası (EMO) tarafından değişik ortamlarda vatandaşlarla yüzyüze görüşmelerle uygulanmış olup sonuçta 466 adet cevaplanmış anket elde edilmiştir. Önceki bölümlerde verilen hipotezlerin (Tablo 1-Tablo 8) analizi için çoklu doğrusal regresyon modeli kullanılmıştır. Bu model aşağıda özetlenmektedir.

$$Y_i = a_{0i} + a_1\,yaş + a_2\,cins + a_3\,eğit + a_4\,dene \quad i=1,2\ldots..,8$$

Gerektiğinde değişkenler arasındaki ikili ilişkileri incelemek amacıyla %5 yeterlilik düzeyinde Ki-kare (χ^2) test yöntemi de kullanılmıştır.

Tablo 9: Anket formu özeti

Soru	Değişken	Tanım	Cevap alternatifleri
1	Yaş	Yaşınız?	<21, 21-30, 31-40, 41-50, 51-60, >60
2	Cinsiyet	Cinsiyetiniz?	erkek/kadın
3	Eğit	Eğitim durumunuz?	doktora/yüksek lisans, lisans, ön lisans, öğrenci (üniversite), Lise ve altı
4	Dene	Bilişim deneyiminiz (yıl)?	yok, 1-5, 6-10, 11-15, 16-20, >21
5	Y_1	Bilgisayar güvenliği bilgi düzeyiniz nedir?	çok fazla, fazla, orta, az, hiç yok (10. soruya geçiniz)
6	Y_2	Kullandığınız bilgisayarda sizin için önemli bilgi bulunduruyor musunuz?	evet/hayır
7	Y_3	Bilgisayarınızda bulunan bilgileri yedekleme sıklığınız nedir?	çok sık (ayda 2 veya daha çok), sık (ayda 1), orta (2-6 ayda 1), az (yılda 1), yedekleme yapmıyorum
8	Y_4	Bilgisayarınızda güvenlik taraması yedekleme sıklığınız nedir?	çok sık (ayda 5 veya daha çok), sık (ayda 3-4), orta (ayda 2), az (ayda 1), güvenlik taraması yapmıyorum
9	Y_5	Bilgisayarınızda lisanslı bir virüs koruma sistemi kullanıyor musunuz?	evet/hayır
10	Y_6	Web sayfaları güvenliği bilgi düzeyiniz nedir?	çok fazla, fazla, orta, az, hiç yok (12. soruya geçiniz)
11	Y_7	Güvenli web sitelerini nasıl ayırt edersiniz?	Ayırt edemem, erişirken aldığım uyarı ile, site içerisinde güvenlik logosunun varlığıyla, web tarayıcının göstereceği küçük kilit sembol ile
12	Y_8	Web siteleri sertifika hatası kavramı hakkında bilginiz var mı?	evet/hayır

Tanımlayıcı Bulgular

Anket katılımcılarının demografik özellikleri Tablo-10'da sunulmuştur.

Tablo 10: Katılımcı Demografik Özellikleri

Değişken	Miktar	Oran (%)
Yaş		
<21	95	20
21-30	211	45
31-40	94	20
41-50	49	11
51-60	12	3
>61	5	1
Cinsiyet		
Erkek	255	55
Kadın	205	44
Belirtmemiş	6	1
Eğitim Durumu		
Lise	125	27
Öğrenci(Üniversite)	113	24
Ön Lisans	22	5
Lisans	151	32
Doktora/Y.Lis.(Master)	21	5
Diğer	34	7
Bilgi ve İletişim Teknolojileri Kullanım Deneyimi		
Deneyimim yok	52	11
1-5 Yıl	154	33
6-10 Yıl	170	36
11-15 Yıl	78	17
16-20 Yıl	7	2
>= 21 Yıl	5	1

Anket katılımcılarının yaş gruplarına dağılımı incelendiğinde katılımcıların çoğunluğunun 40 yaşından daha genç olduğu görülmektedir. En büyük katılım oranı %45 ile 21-30 yaş grubunda izlenirken, 40 yaş ve daha geç grupların toplamı %85'tir. Katılımcıların cinsiyetlere göre dağılımları incelendiğinde erkeklerin kadınlara nazaran %11 oranında daha fazla temsil edildiği göze çarpmaktadır. Erkek (%50.98) ve kadın (%38.54) katılımcıların büyük çoğunluğu 21-30 yaş grubundan oluşmaktadır. Her iki grupta 40 yaş üzeri katılımcı oranı ise erkekler için %13.33, kadınlar için %14.17 olup benzer dağılım göstermektedir. Ancak, yaş ve cinsiyet dağılımları arasındaki %5 yeterlilik düzeyinde ilişki anlamlı bulunmamıştır (χ^2=10.500; sd=5; p-değeri=0.062).

Lisans seviyesinde eğitim sahibi olanların oranı %32 ile en büyük katılımcı kategorisini oluştururken, bunu %27 ve %24 ile sırasıyla lise ve üniversite öğrencisi kategorileri takip etmektedir. Bu dağılım, katılımcı yaş dağılımı ile paralellik gösterdiği izlenmekte ve aralarındaki ilişkinin tutarlı olduğu gözlenmektedir (χ^2=79.710; sd=4; p-değeri=0.000). Buna karşılık, eğitim ve cinsiyet değişkenleri arasında ise anlamlı bir ilişki bulunamamıştır (χ^2=2.605; sd=1; p-değeri=0.107).

Katılımcıların Bilgi ve İletişim Teknolojileri Kullanım Deneyimleri konusundaki yanıtları incelendiğinde, 6-10 yıllık deneyim kategorisinin %36 ile en büyük kesimi oluşturduğu, bu kategoriyi %33'lük bir oranla 1-5 yıllık deneyim gurubunun izlediği görülmektedir. Anket katılımcıları arasında Bilgi ve iletişim teknolojileri kullanım deneyimi 1-10 yıl arasında olan miktar %69 ile büyük bir kesimi oluşturmaktadır. Bu bulgunun katılımcı yaşları ile beraber yorumlanması neticesinde, genç kuşağın bu teknolojileri daha çok kullandığı yönündeki yaygın kanaatin bu çalışma bulguları ile de desteklendiği görülmektedir. Bu paralelde yaş ve bilişim deneyimi arasında istatistiksel olarak anlamlı bir ilişki bulunmuştur (χ^2=29.60; sd=4; p-değeri=0.000). Diğer taraftan erkek ve kadın katılımcıların büyük çoğunluğunun (erkek=%43; kadın=%41) en az önlisans mezunu olduğu görülmektedir. Eğitim ve bilişim deneyimi için yapılan test sonuçları bu değişkenler arasında beklendiği gibi anlamlı bir ilişki bulunduğunu göstermektedir (χ^2=127.210; sd=20; p-değeri=0.000). Tüm bunlara ek olarak erkek ve kadın katılımcıların büyük çoğunluğunun bilişim deneyimlerinin 1-10 yıl arasında olduğu (erkek=%69; kadın=%71) görülmektedir. Ancak, cinsiyet ve bilişim deneyimi incelendiğinde test sonuçları bu değişkenler aralarındaki ilişkinin anlamlı olmadığını göstermektedir (χ^2=3.304; sd=4; p-değeri=0.508).

Analiz Sonuçları
Yukarıda verilen 32 hipotez (Tablo 1 - Tablo 8) %5 yeterlilik derecesinde incelenmiş ve aşağıda verilen sonuçlara ulaşılmıştır.

Bilgisayar Güvenliği: Yapılan regresyon analiz sonuçları Tablo 11'de verilmektedir.

Tablo 11: Bilgisayar güvenliği farkındalığı regresyon analiz sonuçları

Bağımsız değişken	Bağımlı değişken	Hipotez	Alpha değeri	p-değeri*
Yaş	Y1	$H1_{yas, Y1}$	- 0.379	0.000*
Cins	Y1	$H1_{cins,Y1}$	- 0.329	0.000*
Eğit	Y1	$H1_{eğit, Y1}$	0.115	0.000*
Deney	Y1	$H1_{dene,Y1}$	0.499	0.000*
Yaş	Y2	$H1_{yas, Y2}$	- 0.208	0.000*
Cins	Y2	$H1_{cins,Y2}$	- 0.105	0.080
Eğit	Y2	$H1_{eğit, Y2}$	0.049	0.039*
Deney	Y2	$H1_{dene,Y2}$	0.138	0.000*
Yaş	Y3	$H1_{yas, Y3}$	- 0.306	0.000*
Cins	Y3	$H1_{cins,Y3}$	- 0.244	0.022*
Eğit	Y3	$H1_{eğit, Y3}$	0.176	0.000*
Deney	Y3	$H1_{dene,Y3}$	0.382	0.000*
Yaş	Y4	$H1_{yas, Y4}$	- 0.440	0.000*
Cins	Y4	$H1_{cins,Y4}$	- 0.207	0.041*
Eğit	Y4	$H1_{eğit, Y4}$	0.144	0.000*
Deney	Y4	$H1_{dene,Y4}$	0.391	0.000*
Yaş	Y5	$H1_{yas, Y5}$	- 0.254	0.000*
Cins	Y5	$H1_{cins,Y5}$	- 0.103	0.060
Eğit	Y5	$H1_{eğit, Y5}$	0.066	0.002*
Deney	Y5	$H1_{dene,Y5}$	0.144	0.000*

*istatistiksel olarak 5% düzeyinde yeterlilik belirtir.

Bu tabloda verilen alpha değerleri ile %5 istatistiksel derecesinde yeterlilik testi için kullanılan p-değerleri incelendiğinde aşağıda verilen hususlar göze çarpmaktadır.

- Cinsiyet ile kişinin çalıştığı bilgisayarda kendisi için önemli bilgiler bulundurması ($H1_{cins,Y2}$) hususu hariç (p-değeri= 0.080) diğer tüm bağımsız değişkenlerin bilgisayar güvenliği farkındalığı kategorisi altında verilen faktörlerle %5 yeterlilik düzeyinde istatistiksel olarak anlamlı ilişkisi olduğu görülmektedir.

- Yaş ve cinsiyet ile bağımlı değişkenler arasındaki ilişki negatif bulunmuştur. Buna karşılık eğitim düzeyi ve deneyim ile yine bilgisayar güvenliği kategorisi altında verilen faktörler arasındaki ilişki pozitif bulunmuştur. Diğer bir deyişle kadınların ve daha ileri yaştakilerin bilgisayar güvenliği hakkındaki hassasiyetleri azalmaktadır. Buna karşılık kişilerin eğitim ve deneyim düzeylerinin artışı ile bu hassasiyetler ve farkındalık daha üst düzeye çıkmaktadır.

Web Güvenliği: Bu grup için regresyon analiz sonuçları Tablo 12'de verilmektedir. Buna göre

Tablo 12: Web güvenliği farkındalığı regresyon analiz sonuçları

Bağımsız değişken	Bağımlı değişken	Hipotez	Alpha değeri	p-değeri*
Yaş	Y6	$H2_{yaş, Y6}$	- 0.374	0.000*
Cins	Y6	$H2_{cins,Y6}$	- 0.217	0.019*
Eğit	Y6	$H2_{eğit, Y6}$	0.153	0.000*
Deney	Y6	$H2_{dene,Y6}$	0.437	0.000*
Yaş	Y7	$H2_{yaş, Y7}$	- 0.629	0.356
Cins	Y7	$H2_{cins,Y7}$	- 2.230	0.106
Eğit	Y7	$H2_{eğit, Y7}$	0.792	0.145
Deney	Y7	$H2_{dene,Y7}$	1.420	0.032*
Yaş	Y8	$H2_{yaş, Y8}$	- 0.223	0.000*
Cins	Y8	$H2_{cins,Y8}$	0.002	0.979
Eğit	Y8	$H2_{eğit, Y8}$	0.099	0.000*
Deney	Y8	$H2_{dene,Y8}$	0.187	0.000*

*istatistiksel olarak 5% düzeyinde yeterlilik belirtir.

Tablo 12'de verilen alpha değerleri ile %5 istatistiksel derecesinde yeterlilik testi için kullanılan p-değerleri incelendiğinde aşağıda verilen hususlar göze çarpmaktadır.

Kişilerin yaş, cinsiyet, eğitim ile güvenli web sitelerini ayırt edebilmesi ($H2_{yaş,Y7}$, $H2_{cins,Y7}$, $H2_{eğit,Y7}$) hususu (karşılıklı olarak p-değeri$_{yaş,Y7}$ = 0.356; p-değeri$_{cins,Y7}$ = 0.106; p-değeri$_{eğit,Y7}$ = 0.145) arasındaki ilişki anlamlı bulunmamıştır. Benzer şekilde cinsiyet ile web siteleri sertifika hatası kavramı hakkında bilgisinin olup olmaması hususu ($H2_{cins,Y8}$) arasındaki ilişki de istatistiksel olarak %5 yeterlilik düzeyinde anlamlı değildir (p-değeri$_{cins,Y8}$ = 0.979). Bunun dışında kalan diğer tüm bağımsız değişkenlerin web güvenliği kategorisi altında verilen faktörlerle %5 yeterlilik düzeyinde istatistiksel olarak anlamlı ilişkisi olduğu görülmektedir.

- Eğitim ve deneyim ile web güvenliği kategorisinde yer alan tüm bağımlı değişkenler arasındaki ilişki pozitif bulunmuştur. Diğer bir deyişle bilgisayar güvenliği kategorisine benzer şekilde kişilerin eğitim ve deneyim düzeylerinin artışı ile web konusundaki hassasiyetler ve farkındalık daha üst düzeye çıkmaktadır. Benzer şekilde kişinin cinsiyet ve web siteleri sertifika hatası kavramı hakkında bilgisinin olup olmaması arasındaki ilişki de anlamlı olmamakla birlikte pozitif bulunmuştur. Bu ise kadınların erkeklere oranla web siteleri sertifika hatası hakkında daha hassas olduklarına işaret etmektedir. Buna karşılık yaş, cinsiyet ile web sayfaları güvenliği hakkında bilgi düzeyi, güvenli web sitelerini ayırt edebilme özelliği arasındaki ilişki negatif bulunmuştur. Bu ise erkeklerin ve daha genç yaştakilerin bu konularda daha yetkin olduklarını göstermektedir. Benzer şekilde yaş ve web siteleri sertifika hatası bilgi düzeyi arasında negatif bir ilişki saptanmıştır. Bu is erken yaştakilerin web sayfası sertifika hatası bilgi düzeyinin daha fazla olduğunu göstermektedir.

Sonuçlar

Bilişim teknolojilerinin bulunduğumuz çağın yükselen değeri olduğu ve teknolojideki hızlı gelişmeler sonucunda, bilişim teknolojilerinin yaşantının tüm alanlarını etkilediği bilinmektedir. Ancak bilişim teknolojilerinde yaşanan bu gelişmelerin başta güvenlik olmak üzere çeşitli sorunları da beraberinde getirdiği açıktır. Güvenlik sorunları arasında ise ağ ve bilgi güvenliği ilk sırayı almakta olup bilişim teknolojileri kullanıcısının bu konu ile ilişkisi önem kazanmaktadır.

Bu çalışmada bilişim teknolojileri kullanıcılarının demografik özellikleri ile bilgisayar ve web güvenliği konuları arasındaki ilişkiler incelenmiştir. Bu amaçla EMO'nun önemli desteği ve 466 katılımcıyla bir anket çalışması gerçekleştirilmiştir. Elde edilen verilerin analizleri sonucunda;

- Yaşın artması ile bilgisayar güvenliği konusundaki hassasiyetin azaldığı,
- Kadınların erkeklere oranla bilgisayar güvenliği konusunda daha hassas olduğu,
- Eğitim seviyesi yükseldikçe bilgisayar güvenliğinde daha hassas davranıldığı,
- Bilgi ve iletişim sistemleri kullanım deneyiminin artması ile bilgisayar güvenliği konusunda hassasiyet ve farkındalığın da arttığı,
- Yaşın artması ile web güvenlik uygulamaları farkındalığının da arttığı,
- Erkeklerin güvenli web kullanımı konusunda kadınlardan daha yetkin olduğu,
- Eğitim seviyesi yükseldikçe web güvenliği konusunda hassasiyet ve farkındalığın da arttığı
- Bilgi ve iletişim sistemleri kullanım deneyimin artışı ile güvenli web kullanımında hassasiyetin arttığı

tespit edilmiştir.

Yapılan tespitlerde en öne çıkan husus yaş ilerledikçe bilgisayar güvenliği konusunda hassasiyet azalmasına karşılık web güvenliği konusunda farkındalık ve duyarlılığın artmasıdır. Benzer şekilde kadınlar bilgisayar güvenliğine erkeklerden daha çok dikkat ederken erkekler de web güvenliğinde kadınlardan daha dikkatli davranmaktadır. Bilgi ve iletişim teknolojileri kullanım deneyimi ve Eğitim seviyesi ise hem bilgisayar güvenliği hem de web güvenliği bağımlı değişkenleri ile yöndeş ilişkilidir.

Ulaşılan sonuçlar paralelinde, bilgisayar güvenliği ve web güvenliğinde hassasiyet ve farkındalık seviyesini yükseltmek, kullanıcılardan kaynaklanan güvenlik açıklarını en aza indirebilmek amacı ile, kullanıcıların bilgi ve iletişim teknolojisi kullanım deneyimlerinin çeşitlendirilerek artırılmasının ve kullanıcı eğitim seviyesinin yükseltilmesinin olumlu etki yaratacağı sonucuna ulaşılmıştır.

Teşekkür

Elektrik Mühendisleri Odası'na bu çalışmanın veri toplanması ve bu verinin sayısallaştırılması aşamalarında göstermiş oldukları desteklerden ötürü teşekkür ederiz.

Referanslar

[1] D'Arcy J. and Hovav A. Deterring Internal Information Misuse, Communications of the ACM, October 2007, Vol. 50 No.10

[2] Adams A. and Sase M. A. Users Are Not The Enemy, Communications of the ACM, December 1999, Vol. 42 No.12

[3] Computer Crime & Security Survey, Computer Security Institute, İnternet adresi http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf, (son erişim tarihi 11 Haziran 2011).

[4] 14th Annual CSI Computer Crime & Security Survey, Comprehensive Addition, Computer Security Institute, İnternet adresi http://gocsi.com/sites/default/files/pdf_survey/CSI%20Survey%202009%20Comprehensive%20Edition.pdf, (son erişim tarihi 11 Haziran 2011).

[5] Palfreyman K. and Rodden T. A Protocol For User Awareness And World Wide Web, Computer Supported Cooperative Work'96, Cambridge MA, USA, 1996 ACM 0-89791-765-0/96/11

[6] Gross J. B. and Rosson M. B. Looking for Trouble: Understanding End-User Security Management, CHIMIT'07, March 30-31, 2007, Cambridge MA, USA. 2007 ACM 1-59593-635-6/97/0003

[7] Stanton J. M. and Stam K. R. Mastrangelo Paul, Jolton Jeffrey, Analysis of End User Security Behaviors, Computers & Security, March 2005, sayfa 124-133

[8] Herzberg A. and Jbara A. Security and Identification Indicators for Browsers against Spoofing and Phishing

Attacks, ACM Transactions on Internet Technology, September 2008, Vol. 8, No. 4, Article 16.

[9] West R. The Psychology of Security, Communications of the ACM, April 2008, Vol. 51 No.4

[10] Rahim, M. M., M.N. Rahaman and Seyal, A.H. "Software piracy among academics: an empirical study in Brunei Darussalam", Information Management & Computer Security (2000), 8 (1), 14-26.

[11] Lau, E.K.W. "An empirical study of software piracy", Business Ethics: An European Review,2003-12 (3), 233-245.

[12] Levy K. Overcoming the Digital Divide. Panel Discussion (2002): E-Government and Citizen Centered Government Round Table. İnternet adresi http://www.epa.gov/customerservice/2002conference/levy.pdf. (son erişim tarihi 25.07.2006)

[13] Lian J.W. and Lin T.M. Effects of consumer characteristics on their acceptance of online shopping: Comparisons among different product types, Computers in Human Behavior (2008). 24(1): 48-65.

[14] Colley, A. & Maltby, J.. Impact of the Internet on our lives: male and female personal perspectives. Computers in Human Behavior, 24(2008), 2005-2013.

[15] Yang, Shu Ching & Tung Chieh-Ju, Comparison of Internet addicts and non-addicts in Taiwanese high school. Computers in Human Behavior (2007), 23, 79-96.

[16] Zhang, Y. Age, gender, and Internet attitudes among employees in the business world. Computers in Human Behavior, 21(2005), 1-10.

[17] Jaeger P.T. The endless wire: e-government as global phenomenon. Government Information Quarterly, 2003-20, 323-31.

2. KISIM:
SİSTEM VE AĞ GÜVENLİĞİ

HTML5 Güvenliği

Yeni Nesil Web Tehditleri

Emre Çakır

BEAM Teknoloji AŞ, Ankara

e-posta: emre@beamteknoloji.com

Özetçe

HTML5, süregelen tarayıcı savaşlarındaki "Kim daha fazla HTML5 destekliyor?" bölümünün etkisiyle ve özellikle sosyal paylaşım sitelerinin HTML5 standardının getirdiği yeni özellikleri kullanıcılarına sunmak için sabırsızlanmasıyla birlikte İnternet dünyasında har geçen gün daha fazla yer buluyor. Yarış ortamında geliştirilen ve piyasaya sürülen tarayıcılar ile henüz taslak halde bulunan bir standart kılavuzluğunda geliştirilen web uygulamalarının testlerini yapma yükümlülüğü de çoğu zaman durumdan habersiz İnternet kullanıcılarına kalıyor. Günümüzde birçok önemli verinin İnternet üzerinde depolandığı, taşındığı ve paylaşıldığı gerçeğini göz önünde bulundurursak, henüz taslak halde bulunan HTML5 standardının düzgün yorumlanmaması ve/veya uygulanmaması İnternet kullanıcılarının güvenliği konusunda ciddi bir tehdit oluşturuyor. Bu makale, güvenlik hassasiyeti olmadan geliştirilen HTML5 standardında tanımlanan yeni özelliklerin sebep olabileceği zafiyetleri incelemekte ve kullanıcıları bu zafiyetlere maruz bırakmamak için uyulması gereken güvenli web yazılımı geliştirme prensiplerini içermektedir.

1. Giriş

Halen Web uygulamalarını geliştirmek için kullanmakta olduğumuz HTML4 standardının geliştirilmesi 1997'de tamamlanmış olup W3C tarafından 1999 yılında geliştiricilerin kullanımı için önerilmiştir[1]. O günden bu bugüne gerek yazılım dünyasındaki gerekse donanım dünyasındaki gelişmeler göz önünde bulundurulduğunda kullanıcıların İnternetten beklentileri belirgin bir şekilde artmıştır. Yazılım geliştirme ortamlarının yeteneklerinin artması, internet bağlantı hızlarının belirgin bir şekilde yükselmesi, İnternet erişiminin cep telefonlarına kadar ulaşması bu dünyada yer sahibi olmak isteyen üreticilerin ortam gereksinimlerini arttırmış; bankacılık, eğitim, alışveriş, iletişim, paylaşım gibi birçok aktivitenin İnternet üzerine taşınması yeni ihtiyaçlar ortaya çıkarmıştır. İnternet dünyasında bu köklü değişimler yaşanırken, uygulamaların üzerine kurulduğu standart aynı kalmış ve yakın dönemlerde çoğu zaman geliştiricileri kısıtlayan bir kurallar bütünü haline gelmiştir. Yeni gelişen ihtiyaçlar Adobe® Flash, JAVA Applet, Microsoft® Silverlight gibi yan çözümlerle giderilmeye çalışılırken bu birbirinden bağımsız üretici çözümleri İnternet üzerinde standarttan uzaklaşmayı arttırarak, İnterneti birlikte çalışamayan ve de çalışamayacak olan uygulamalar yığını haline getirmeye başlamıştır. Son dönemde hızlıca yükselen sosyal paylaşım siteleri ve özü gereği bu sitelerin paylaşım ve birlikte çalışırlığa yönelik yapıları İnternet için yeni bir standart ihtiyacını tepe noktasına çıkartmıştır.

HTML standardın İnternetin yeni gereksinimlerini karşılaması amacıyla güncellenmesi için WHATWG (Web Hypertext Application Technology Working Group) 2004 yılında çalışmalarına başlamış ve çok geçmeden W3C de bu sürece dâhil olmuştur[2]. İnternetin yeni anayasası statüsündeki HTML5, Mayıs 2011 itibariyle yeni önerilere kapısını kapatmış ve 2014 yılı W3C tarafından standardın önerileceği tarih olarak belirlenmiştir[3].

HTML5 standardının 2014 yılına kadar önerilmeyeceği, 2014 yılına kadar HTML5 zafiyetlerinden kaynaklanacak tehditlere maruz kalmayacağımız manasına gelmemektedir. HTML5 WHATWG ve W3C önderliğinde ve koordinasyonunda geniş bir topluluk tarafından açık bir şekilde geliştirilmekte ve taslak standardın geçirdiği bütün evreler geliştiricilere sunulmaktadır. An itibariyle elimizdeki taslağın bazı kısımları olgunlaşmışken bazı kısımlarında geliştirme henüz devam etmektedir. Bu geliştirmeye aktif bir şekilde katılan tarayıcı üreticileri, bir yandan standardı gerçeklemeye devam ederken bir yandan da karşılaştıkları sorunları WHATWG ve W3C ile paylaşmakta, standart da bu şekilde birçok açıdan evrimleşmektedir. Bu süreç sırasında da daha önce bahsedilen sebeplerden dolayı, tarayıcı üreticileri taslak gerçeklemelerini yeni sürümlerinde piyasaya sürmekte ve HTML5 ile geliştirilmiş web uygulamaları bugün aktif olarak bütün popüler tarayıcılarda kısmi destekle çalışmaktadır.

Bu makale henüz taslak halde bulunmasına rağmen İnternette aktif olarak kullanılabilen HTML5 standardının düzgün yorumlanmadığında ve/veya düzgün gerçeklenmediğinde yol açabileceği zafiyetleri ve İnternet kullanıcılarını bu zafiyetlere maruz bırakmamak için uyulması gereken güvenlik prensiplerini sunmaktadır. Makalenin 2. kısmında HTML5 standardında tanımlanan belli başlı yenilikler, bu yeniliklerin gereksinimleri ve yol açabileceği olası zafiyetlerle güvenli

web yazılımı geliştirme prensipleri sunulacaktır. 3. kısımda bu güvenlik prensiplerinin bir özeti ve HTML5 güvenliği üzerine çalışacaklar için öneriler bulunacak ve son kısımda HTML5 güvenliği çalışmasından çıkarılan sonuçlara yer verilecektir.

2. HTML5 Yenilikleri

2004 yılında çalışmalarına başlanan HTML5 standardı, İnternetin var olan ve yakın gelecekte var olacak ihtiyaçlarını karşılamak üzere geniş bir topluluğun önerileri doğrultusunda geliştirilmiş ve bu geliştirme süreci 2011 yılı Mayıs ayında son halini almıştır. Bu süreç sırasında Web 2.0 olarak da bilinen ve temelde enteraktif ve birlikte çalışabilir bir ağ inşa edilmesi için gereken değişiklikler HTML standardına eklenmiştir. Bu temel değişiklikler ve karşıladığı gereksinimler aşağıdaki konu başlıklarında incelenmektedir.

2.1. Alanlar Arası İletişim (Cross Domain Messaging)

Web sitelerinin güvenlikli bir şekilde birlikte çalışabilirliği Web 2.0 gelişmeleri ile ihtiyaç duyulmaya başlanan en temel gereksinimlerinden biridir. Bu süreçte tarayıcılar, gizlilik ve güvenlik gereksinimlerinden dolayı farklı alanlardaki kaynakların birbirleriyle kuralsız bir şekilde haberleşmelerini engellemiştir[4,5]. HTML4 standardında bahsedilmeyen bu ihtiyaç HTML5 desteklenene kadar yan yollarla çözülmeye çalışılmış; bu da ya genel-geçer çözümler üretmeyi zorlaştırmış ya da çok ciddi güvenlik zafiyetlerine sebep olmuştur. HTML5 standardında tanımlanana kadar kullanılan çözümler aşağıdaki gibi özetlenebilir:

- **Flash Alanlar-Arası İletişim Politikası:** Adobe® Flash, bu ihtiyacı güvenli bir şekilde karşılayabilmek için bir kaynaklar-arası iletişim politikası dosyasında güvenilir kaynakları tanımlamış ve kullanıcıya gönderilen bu dosya sayesinde tarayıcıların bağlantı yapabilecekleri alanları sınırlamıştır[6]. Bu protokol DNS-yeniden sorgulama saldırılarına karşı zafiyet göstermektedir[7].

- **JavaScript Alanlar-Arası İletişim Protokolü:** XSS saldırılarına sebebiyet verebileceğinden dolayı alanlar arası gönderilen AJAX istekleri tarayıcılar tarafından uzunca bir süre engellenmiştir. W3C tarafında bu iletişimi sağlayabilecek protokol[8] tanımlandıktan sonra web uygulamaları belirlenen protokoller doğrultusunda tarayıcılar aracılığıyla birbirleriyle iletişim kurmaya başlamıştır.

Barth ve arkadaşları bu yukarıda belirtilen metotların gerçeklemeleri üzerinde yaptıkları çalışmalarda çeşitli zafiyetler tespit etmiş ve sağlayabileceği güvenlik seviyesinden dolayı HTML5 mesajlaşma modeli olan **postMessage** ara yüzünün kullanılmasını tavsiye etmiştir[9].

postMessage ara yüzü, alanlar-arası iletişim ihtiyacını karşılamak üzere HTML5 standardına eklenmiş bir ara yüzdür. Tarayıcılar tarafından gerçeklenmesi gereken bu ara yüz sayesinde, istemci tarafında çalışan JavaScript kodu, sunucuya gitmeden başka alanlarla iletişim kurabileceklerdir. Basit bir şekilde tanımlanan bu ara yüzde doğrulanması gereken gereksinimler;

- **Gizlilik:** Ara yüzde mesaj gönderen taraf mesajın alıcısı olan (targetOrigin) alanları belirtebilmelidir.

- **Kimlik Doğrulama:** Ara yüz ile gelen mesajda mesajın göndericisi olan alan bildirilmelidir.

HTML5 standardını desteklediğini iddia eden tarayıcı tarafından garanti edilmelidir. Bu şekilde alanlar-arası güven probleminde tarayıcı garantör olarak devreye girerek güven sorununu çözecektir.

2.1.1. postMessage Arayüzü

- **Mesaj Gönderme:** window.postMessage ara yüzü standartta şöyle tanımlanmıştır:

postMessage(message, targetOrigin);

Bu fonksiyonun çağrılması sonucunda tarayıcı *targetOrigin* ile belirtilmiş alanlara bu mesajı ulaştırmakla yükümlüdür. *targetOrigin* parametresi "*" karakteri kabul etmekte ve bu karakter verildiğinde tarayıcı mesajı bütün pencerelere iletmektedir.

- **Mesaj Alma:** postMessage ara yüzünden gelecek mesajları almak için pencerenin mesaj olay dinleyicisi tanımlanmalıdır.

window.addEventListener('message',receive,false)

receive fonksiyonu içerisinde gelen mesajlar işlenebilir ve gerekli aksiyonlar gerçekleştirilebilir.

2.1.2. HTML5 Alanlar-arası İletişim Zafiyetleri

HTML5 alanlar-arası haberleşme problemini tarayıcıyı garantör olarak basit bir şekilde çözmeyi başarmış fakat çözerken web uygulaması geliştiricilere "giden mesajın gizliliğini sağlamak" ve "gelen mesajda göndericinin kimlik doğrulamasını yapmak" sorumluluklarını yüklemiştir. Bu doğrulamaların önceki uygulamalarda olduğu gibi merkezi bir şekilde yönetilememesi, her mesajda tekrar edilmesi

gerekliliği de güvenlik zafiyetine sebebiyet verebilecek bir eksiklik olarak görünmektedir. Protokolün *targetOrigin* tanımlanırken "*" joker karakterine izin vermesi yine geliştiriciler tarafından yanlış uygulanacak ve veri gizliliğine yönelik sızmalara sebebiyet verecektir. Bu iletişimin düzgün bir şekilde gerçeklenmiş olmaması durumunda iletişim üzerinde aşağıdaki saldırı senaryolarının uygulanması mümkün olacaktır:

- **Mesaj Bütünlüğüne Yönelik Saldırılar:** Gönderici kimliğinin kontrol edilmemesi durumunda postMessage ara yüzü kullanılarak yapılacak sorgulara asıl gönderici yerine kötü niyetli bir saldırgan tarafından cevap verilebilir. Bu dönen cevabın alıcı tarafında işlenişine göre istemci makinede rastgele kod çalıştırılmasına kadar varabilecek bir saldırı senaryosunun uygulanması mümkündür.

- **Gizliliğin İhlaline Yönelik Saldırılar:** postMessage fonksiyonu "*" joker karakteri ile birlikte çağrıldığında tarayıcı gönderilen mesajı yetkili alıcıya değil de bütün dinleyicilere ulaştıracağından, mesajın içeriği kötü niyetli saldırganlar tarafından açık edilebilecektir.

2.1.3. HTML5 ile Alanlar-arası İletişim Güvenliği

postMessage ara yüzü kullanılırken mesajın alıcısı düzgünce tanımlanmalı ve pencereye iletilen mesajlar işlenmeden önce gönderici mutlaka kontrol edilmelidir. Bu mesajlarda girdi doğrulaması mutlaka yapılmalı, "*" joker kartı kesinlikle kullanılmamalıdır.

Protokolün bir başka zafiyeti olan bu kontrollerin her mesajlaşmada uygulanması gerekliliği konusunda da gerekli önlemler alınmalı, *postMessage* fonksiyon çağrılarının güvenliği mutlaka kod gözden geçirme aktivitesine eklenmelidir.

Hanna ve arkadaşları bu zafiyet için "mesuliyet ekonomisi" önerisinde bulunmuşlar[10], fakat bu öneri henüz HTML5 standardında yer bulmamıştır. "Mesuliyet ekonomisi" bu *postMessage* doğrulamalarının geliştirici bırakılmasındansa tarayıcı tarafından yapılmasını önermektedir. Bu şekilde unutkanlık, bilgisizlik, dalgınlık sebebiyle geliştiricilerin zafiyet içeren kod geliştirmelerine engel olmayı hedeflemektedir. Şu anki haliyle bu mümkün görünmemektedir, fakat *postMessage* ara yüzünü kullanılarak hazırlanabilecek kütüphanelerle bu ekonomi sağlanabilir. Her durumda *postMessage* içeren çıktılar ikinci bir gözün gözden geçirme faaliyetine tabi tutulmalıdır.

2.2. Yerel Depolama/Veritabanı

İnternet için çok yeni olmayan fakat HTML5 ile standarda giren yeniliklerden bir diğeri yerel depolama mekanizmalarıdır. Standartta iki şekilde tanımlanan yerel depolama tarayıcılar tarafından anahtar-değer ikilisi yazıp okuma ve SQL veritabanı servisi sağlama şeklinde sağlanacaktır. Bu okuma/yazma ve sorgulama işlemleri sırasında tarayıcılar "Aynı Orijin Politikası"nı uygulayacak ve alan dışı veriye erişime izin vermeyecektir. HTML5 ile yerel depolama mekanizması tanımlanmadan önce de kullanıcı makinelerine veri saklamak için kullanılan metotlar aşağıdaki gibi özetlenebilir.

- **Çerez**: Yeteneği itibariyle herhangi bir veriyi kullanıcı makinesinde saklamak için kullanılabilecek çerezler, zamanla kullanıcı tanımlayıcı değerlerin saklanması için kullanılır olmuştur. Anahtar-değer ikilisi şeklinde yazılabilen ve okunabilen çerezler de "Aynı Orijin Politikası"na tabi olup içerdiği verinin önemi nedeniyle sıkı güvenlik önlemlerine de tabidir. Bu yüzden yanında başka verinin saklanması ve tutulması çok uygulanabilir bir yöntem değildir. Çerezlerin bir başka dezavantajı da bütün istek ve cevaplarla birlikte taşınıyor olmasıdır. Bu durum her istekte sunucuya gitmesi gerekmeyen veriler için gereksiz ağ kaynakları kullanımı manasına geldiğinden çerezler bu tür verileri saklamak için tercih edilebilir bir mekanizma değildir.

- **Adobe® Flash Objeleri:** İstemcide veri depolama ihtiyacına Adobe'nin 2002 yılında geliştirdiği çözümdür. Flash çerezleri olarak tanınmasına rağmen asıl amacı veri depolamaktır.

- **Google Gears:** 2007 yılında Google, açık kaynak kodlu Gears eklentisi ile tarayıcıların veri depolayabilme yeteneği kazanmasını amaçlamıştır. Gears, özetle, SQLite veritabanı ve bu veritabanına erişebilmek için gerekli bir ara yüzden oluşmaktadır.

WHATWG ve W3C veri depolama konusundaki bu çok başlılığı ortadan kaldırmak için standarda yerel depolama ve veritabanını eklemiştir. Yakın zamanda Google, Gears değil de HTML5 standardını takip edeceklerini açıklamıştır[11].

2.2.1. HTML5 Standardında Yerel Depolama

HTML5 standardında tanımlanana göre tarayıcılar JavaScript kodu aracılığıyla yerel depolama alanlarına anahtar-değer ikilileri yazabilir:

localStorage.setItem("key", value);

yazılı olan bu değerleri okuyabilirler:

localStorage.getItem("key");

veya bu değerleri silebilirler:

localStorage.removeItem("key")

Standartta yerel veritabanı olarak SQLite veritabanı belirtilmiş ve tarayıcıların bu veritabanına olan ara yüzü tanımlanmıştır. Yerel veritabanı üzerinde web uygulamaları temel SQL işlemlerinin tamamını gerçekleştirebileceklerdir. Aşağıdaki kod parçası yerel veritabanı açıp içerisinde bir tablo oluşturmaktadır.

*openDatabase('test', '1.0', 'Yerel Veritabanı', 5*1024*1024, function(db){*

db.ChangeVersion('', '1.0', function(t){

t.ExecuteSql('CREATE TABLE settings(id, name, value)');}, error);

});

2.2.2. HTML5 Yerel Depolama Zafiyetleri

Yerel depolama mekanizmaları web uygulamalarının kabiliyetini oldukça arttırırken sunucu ve istemci arasında akan trafiğin azaltılması konusunda da büyük etkisi olacaktır. Bununla birlikte yerel depolama mekanizmaları kullanılırken alınması gereken güvenlik önlemleri gözden kaçırılmamalıdır. Kullanıcı makinelerinde veri saklamak aşağıda sıralanan bir dizi güvenlik zafiyetine sebep olabilecektir:

- **Hassas Verilerin Sızması:** Kullanıcı makinelerine kaydedilebilecek herhangi bir verinin yetkisiz erişim, veri bütünlüğü, girdi geçerliliği gibi problemlerin oluşabilecektir. İstemci depolama alanları sunucunun hâkimiyeti olan alanlar olmadığından buraya yazılan veriler başkaları tarafından okunabilir, değiştirilebilir ve/veya silinebilir. Özellikle ortak kullanımdaki bilgisayarlarda bu tehdidin gerçekleşme ihtimali daha yüksektir.

- **XSS ile SQL Enjeksiyonu:** OWASP Web Zafiyet Top 10 listesinin ilk iki sırasını uzunca bir süredir işgal eden XSS ve SQL Enjeksiyonu, HTML5 standardında tanımlanan ve JavaScript ile veritabanına erişimi sağlayan ara yüz ile bir arada uygulanabilecek iki saldırı olacaktır. XSS veya herhangi bir başka şekilde istemci makinesine erişen saldırganlar burada saklanan verileri değiştirdiği durumda sunucunun haberi dahi olmadan bu veritabanını kötüye kullanabileceklerdir.

2.2.3. HTML5 Yerel Depolama Güvenliği

HTML5 standardı ile tanımlanan yerel depolama mekanizmalarının güvenlik konusundaki temel prensibi hiç kuşkusuz gizlilik üzerine olacaktır. Bu veritabanları sunucu hâkimiyeti dışında kaldıkları için hiçbir surette hassasiyet taşıyan veriler buralarda saklanmamalıdır. Bu konudaki geliştiricilerin benimseyebileceği prensip "sunucu tarafında açık bir şekilde saklanamayacak veriler, istemci tarafında hiçbir surette saklanmamalıdır". Her ne kadar tarayıcılar yerel depolama mekanizmalarında "Aynı Alan Prensibi"ne uygun hareket etseler de, bu yerel makinelerin güvenliğinin sağlanamayacağı, ortak kullanıma açık olabilecekleri gibi sebeplerden dolayı hassas verileri buralarda saklamamalıdırlar. En nihayetinde tarayıcılar alan uyumuna bakmakta, aynı alan için kullanıcıları birbirinden ayırt edemezken, kullanıcının kendisinin mi yoksa kullanıcı tarafından çalıştırılan kötü niyetli kod parçalarının mı veritabanına erişmek istediğini kontrol edemezler. Başka bir deyişle, hassasiyet içermeyen ve yetkisiz kullanıcıların da erişebildiği veriler ancak istemci makinelerinde saklanabilirler.

Yerelde depolanan verilerin bütünlüğü de tehlike altında olacağından web uygulamaları bu kaynaktan okudukları veriye; genelde hiçbir yerden okudukları verilere, hiçbir şekilde güvenmemeli, verinin bütünlüğü kullanılmadan önce mutlaka doğrulanmalıdır.

HTML5 standardında herhangi bir alanın oluşturduğu veritabanlarını birbirinden ayırt edecek özellik veritabanı ismidir. Aynı alanın farklı kullanıcıları arasında ayrım yapabilecek bu isim belirlenirken mutlaka tekil bir isim seçilmeli, bu isim tahmin edilebilir olmamalıdır. Aksi takdirde saklanan veri yetkisiz erişime kolayca izin verecek ve veri güvenliği tehlikeye girecektir.

Veritabanı erişimi güvenliği konusunda yapılan çalışmalar HTML5 yerel veritabanları için de geçerlidir. Bu veritabanı iletişimi için obje-ilişkisel eşleştirim kütüphaneleri piyasaya çıkmıştır. Bu kütüphaneler veritabanı iletişiminde kullanıcı girdilerini temizlemeli, olası enjeksiyon saldırılarına karşı veritabanını korumalıdırlar.

Kullanıcılar yerel depolama işleminden önce uyarılmalı, onayladıkları takdirde istemcilere veri kaydedilmelidir. Ayrıca, kullanıcıların farklı istemcilerden erişim gerçekleştirmeleri durumunda bu onaylama mekanizması tekrar devreye alınmalıdır.

2.3. HTML5 Web Soket

HTML5 standardı ile web dünyasına gelen bir diğer devrimsel nitelikteki yenilik de web uygulamalarının istemcilerin alt seviye kaynaklarına ulaşıp ağ iletişimi için soket açmalarını sağlayacak ara yüzün standarda eklenmesidir. Böylelikle "bağlantısız protokol" olarak tanımlanan http üzerinde çalışan web uygulamaları "bağlantılı" bir alternatife sahip olmuştur.

Bu soket ara yüzü de "Aynı Alan Prensibi" ile çalışmakta ve tarayıcılar soket açtıkları alan ile soketi açan uygulamanın alanını eşleştirmektedir. Böylelikle daha önce tarayıcılara yüklenen Adobe® Flash ve JAVA Applet gibi eklentilerle erişilen alt seviye kaynaklara JavaScript ile erişilebilecek, istemci ve sunucu arasında alternatif bir kanal açılabilecektir.

Yapısı itibariyle alanlar arası iletişim ile benzerlik gösteren web soket ara yüzü, yine üzerinde uygulanabilecek saldırı senaryoları açısından da benzerlik göstermektedir. Barth ve arkadaşları [7] bu saldırı senaryolarını uygulamış ve bulgularını standart geliştiricileriyle paylaşmışlardır. Soket ara yüzü özellikle güvenlik açısından henüz olgunlaşmamış bir yenilik olduğundan daha önceden destekledikleri halde Opera ve Firefox yeni sürümlerinden soket desteğini kaldırmışlardır.

2.3.1. HTML5 Web Soket Ara Yüzü

Standartta tanımlanan web soket ara yüzünü kullanarak bir bağlantı oluşturabilmek için:

```
var conn=new
WebSocket("ws://html5.websocket.com");
```

cümlesi kullanılabilir. Kanal güvenliği gerekli olduğu durumlarda soket adresinde *ws://* yerine *wss://* kullanılmalıdır. Daha sonra bu bağlantı objesinin açma, kapama ve mesaj alma ara yüzlerine ilgili fonksiyonlar bağlanarak soket ara yüzü kullanılabilir. Soket ara yüzü kullanarak sunucuya mesaj göndermek için de:

```
conn.postMessage("Hello World!");
```

fonksiyonu kullanılmalıdır. İstemci ile sunucu arasında bir soket açılmak istendiğinde, önce 80inci portta HTTP üzerinden bir anlaşma sağlanır, daha sonra bu bağlantı istemci tarafından soket bağlantısı olarak başka bir porta yükseltilir. Bu mekanizma bağlantının güvenlik duvarı engelini aşması için gereklidir.

2.3.2. Web Soket Zafiyetleri

Web soket ara yüzünün *postMessage* ara yüzünde bahsedilen saldırılara karşı zafiyeti bulunduğu yine Barth ve arkadaşları tarafından gösterilmiştir[7]. Web soketin *postMessage* ara yüzünden farklı olarak alt seviye kaynaklara erişiminin olması onu daha güçlü ve aynı zamanda daha tehlikeli bir hale getirmektedir. Her ne kadar tarayıcı tarafından "Aynı Alan Prensibi"ne göre çalıştırılsa da, bahsedilen senaryodaki DNS-yeniden sorgulama saldırıları ile bu kontrol aşılabilmekte ve bundan sonrası saldırganın hayal gücüne kalmaktadır. Saldırgan bu noktadan sonra, ağ üzerinde makine ve port taraması yaparak başlayacağı saldırı işlemini bulduğu bir açıklık aracılığıyla ağ üzerindeki bir makineyi ele geçirmeye kadar varabilecek saldırıları da yine bu soket ara yüzü üzerinden gerçekleştirebilmektedir. Barth aynı makalesinde soket bağlantısı için daha güvenli bir protokol önermiş ve önerisi HTML5 geliştiricileri tarafından incelemeye alınmıştır.

2.3.3. HTML5 Web Soket Güvenliği

HTML5 soket ara yüzünde gerekli olan güvenlik kontrolleri tarayıcı tarafından yapılmaktadır. Tarayıcı uygulamaların yalnızca istemci tarafından uygulama alanına soket açmasına izin vererek olası saldırıların önüne geçmektedir.

Bu kontrollere rağmen geliştiricilerin dikkat etmesi gereken hususlar bulunmaktadır. Bunlardan en önemlisi hassas verilerin soket ara yüzü üzerinde taşınacağı durumda güvenli soket ara yüzü kullanılması gerektiğidir. Bu şekilde veriler kanal üzerinde şifrelenmiş bir şekilde taşınacak ve uçtan uca güvenlik sağlanmış olacaktır.

HTML5 standardında web soket ara yüzü tanımı henüz olgunlaşmamış ve yaygın bir şekilde kullanılmaya başlanmamıştır. Firefox ve Opera bu ara yüzdeki zafiyetlerden dolayı yeni sürümlerinde soket ara yüzünden desteğini çekmiş ve standardın güvenli bir şekilde tanımlanmasını beklemeye başlamıştır.

JavaScript üzerinden soket seviyesinde istemci kaynaklarına erişim İnternet dünyası için yeni sayılabilecek bir uygulamadır. Geliştiricilere alternatif kanal ile sunucu iletişimi sağlayabilecekleri bir altyapı sunan soket ara yüzü, kullanıcıların da kullanım kalitesini arttıracağı konusunda bir şüphe bulunmamaktadır. Fakat, soket ara yüzü henüz tam manasıyla yaygınlaşmamış güvenliği açısından derinlemesine incelenememiştir. Kullanılmaya başlandıkça gerek tarayıcı gerçeklemeleri gerekse protokolün kendisi güvenlik açısından daha detaylı bir şekilde incelenebilecek ve olası zafiyetleri görülebilecektir. Güvenlik açısından belirli bir olgunluğa erişmeden soket ara yüzünün kullanılması hassas verilerle çalışan uygulamalar için pek uygulanabilir durmamaktadır. Bunun yerine önce standardın olgunlaşması, daha sonra İnternette kullanımının yaygınlaşması beklenmelidir.

2.4. Öğe Özelliklerin Kötüye Kullanımı

Web üzerinde gerçekleştirilen saldırı senaryolarının bir kısmında HTML öğelerinin özellikleri kullanılmaktadır. Örneğin CSRF olarak bilinen Alanlar Arası İstek Düzme saldırılarında URI verilen öğeler sonucu yapılan GET istekleri kullanılarak tarayıcılara kötü amaçlı istekler yaptırılabilir[12]. Bu saldırılar hali hazırda İnternet üzerinde gerçekleştirilmekte, geliştiriciler ve güvenlikçiler tarafından da yoğun bir şekilde incelenmektedir.

HTML5 standardının tanımında web dünyasına yeni giren öğeler kadar eski öğeler için yeni tanımlanan özellikler de standardı oldukça genişletmekte ve güçlendirmektedir. Fakat, bu genişletme ve güçlendirme aynı zamanda kötü niyetli saldırganlar için de yeni saldırı yüzeyleri manasına

gelmektedir. Aşağıda bu türde kötüye kullanılabilecek yeni özelliklerden birkaçı listelenmiştir:

- **formaction:** formlar üzerinde HTML öğelerinin işlem yapmasını sağlayan bu özellik XSS saldırılarına açıktır.

- **autofocus:** HTML5 ile web dünyasına giren autofocus, elemanların otomatik olarak focus almasını sağlar. onfocus veya onblur olaylarıyla birlikte kullanıldığında kullanıcı hareketi olmaksızın saldırı gerçekleştirilebilir.

- **onerror, onscroll:** Yeni tanımlanan bu olaylar ile kullanıcı farkında olmadan tarayıcıda kod çalıştırılabilir.

HTML öğelerinin özelliklerinin kötüye kullanılmasını inceleyen bu liste HTML5 ile artık daha da kabarık bir hale gelmiştir[13]. Bu listede verilen zafiyet durumlarının oluşmasına engel olmak için HTML kodlarının oluşturulmasında kullanılan kullanıcı girdileri mutlaka doğrulanmalıdır. Yapılması gereken doğrulamalar ve dikkat edilmesi gereken öğler ve/veya öğe özellikleri için HTML5 güvenlik listeleri kontrol edilebilir[13].

Bu noktada altı çizilmesi gereken bir başka husus da HTML5 özelliklerinin tarayıcıların desteklemesiyle birlikte artık uygulamaların kullanımına sunulduğu gerçeğidir. Bu uygulamalar HTML5 ile geliştirilmemiş dahi olsa tarayıcılar HTML5 öğelerini ve özelliklerini tanırlar. Bu durum geliştiricilerin ve güvenlikçilerin hali hazırda çalışan uygulamaları HTML5 kontrolleri ile birlikte test etmeleri gereksinimini doğurmuştur. Hali hazırda web uygulamaları için geliştirilen ve kullanılan test araçlarında HTML5 öğeleri ve özellikleri dikkate alınmadığı gibi, bu uygulamaların güvenlik açısından test edilmelerinde ve sıkılaştırılmalarında da bu özellikler göz önünde bulundurulmamıştır. Aynı şekilde web uygulamalarının otomatik güvenlik testlerini yapan araçlarda da bu hassasiyet eklenmemiş olabilir. Geliştiricilerin ve güvenlikçilerin bu duruma dikkat etmesi gerekmektedir. Özet olarak, HTML4 standardı için geliştirilen ve güvenli hale getirilen uygulamalar HTML5 için de güvenlidir önermesi tehlikeli ve yanlıştır. Geliştiriciler ve güvenlikçilerin web üzerinde servis ettikleri uygulamaları HTML5 öğelerini dikkate alarak tekrar test etmesi ve güvenlik hedeflerini doğrulaması gerekmektedir. Web uygulaması güvenlik testi gerçekleştiren otomatik araçlar da en kısa zamanda yeni öğeleri ve özellikleri desteklemeli, testlerini bu yeni saldırı yüzeyinde gerçekleştirmelidir.

Web uygulaması güvenliği denildiğinde es geçilemeyecek bir konu da girdi doğrulamasıdır. Girdi doğrulaması temelde hiçbir kaynaktan gelen girdiye güvenilmemesi, girdinin doğruluğunun teyit edilmesi demektir. Bu doğrulamayı web uygulamalarının dışarıya açık bütün ara yüzlerinde, yeterli ve doğru biçimde, aynı zamanda HTML5 öğelerini de hesaba katarak yapan uygulamalar güvenli olduklarını iddia edebilirler.

3. HTML5 Güvenliği

Şüphesiz HTML5 İnternet dünyasında yeni bir çığır açacak ve hem geliştiriciler için hem de kullanıcılar için vazgeçilmez uygulamalara imkân tanıyacaktır. Burada gözden kaçırılmaması gereken HTML5 standardının henüz taslak halde bulunduğu gerçeğidir. Taslak halde bulunan bir standarttan yola çıkılarak hızlı bir şekilde tarayıcılar tarafından desteklenen bu yeni özellikler bugüne kadar karşılaşılmamış, bilinmeyen zafiyetlere sebebiyet verebileceği gibi, bilinen zafiyetlerin farklı biçimlerde tekrar ortaya çıkartılmasına da sebep olabilirler.

Burada tekrar altını çizmemiz gereken bir başka nokta tarayıcıların desteklemesiyle birlikte bütün İnternet kullanıcılarının HTML5 kullanmaya başlamasıdır. Bu geçiş sırasında kullanıcının onayı alınmadığı gibi, otomatik güncellemeyle tarayıcısını güncelleyen kullanıcılar HTML5 zafiyetlerinin oluşturabileceği tehditlerin hedefi haline gelmektedir. Burada geliştiricilere önemli bir sorumluluk düşmektedir. Bugüne kadar İnternet üzerinden servis ettikleri yazılımlar HTML5 standardının tarayıcılarla desteklenmesinden sonra güvenlik zafiyeti gösterebiliriler. Nispeten yeni ve tamamlanmamış olan bu zafiyetlere karşı güvenlik testleri derinlemesine ve eksiksiz bir şekilde bir an evvel yapılmalı, yeni geliştirilen uygulamalarda da bu yazıda bir kısmı verilen güvenlik önerilerine uygun bir şekilde geliştirme yapılmalıdır.

HTML5 güvenlik testi yapmaya aday olan araçlar da var olan zafiyet ve tehdit veritabanlarını güncellemeli ve tarayıcılar tarafından desteklenen özellikler bütününü testlerine dâhil etmelidirler.

Son olarak vurgulamak istediğimiz bir diğer nokta da Firefox ve Opera'nın yeni sürümlerde zafiyet ve açıklıklara sebebiyet verebileceğinden dolayı soket ara yüzünden desteğini çekmesidir. Süregelen tarayıcı savaşlarında öne çıkma arzusunun yerine kullanıcılarının güvenliğini ön plana çıkarması bu iki tarayıcıyı güvenlik açısından diğerlerinin önüne geçirmeyi başarmıştır.

Bütün bu önlem ve kısıtlamalarla birlikte İnternet üzerinde birlikte çalışabilirliği önemli ölçüde arttıracak olan HTML5 standardının kullanımı ve yaygınlaşması desteklenmeli; kritik olmayan uygulamalar aracılığıyla standarttaki zafiyetler bir an evvel tespit edilip kapatılarak HTML5 standardı bütün geliştiricilerin kullanımına açılmalıdır.

4. Sonuçlar

HTML5 standardı henüz taslak halinde olmasına rağmen çözüm getirdiği sorunlar ve web üzerinde çalışan uygulamaların yeteneklerini genişletmesi açısından özellikle Facebook, Google, Apple gibi üreticiler tarafından çoktan benimsenmiş ve uygulamaya konmuştur. Popüler tarayıcılar da bu sürece yoğun bir şekilde destek vermekte ve standardın olgunlaşması için çaba sarf etmektedirler. Bu görünüme göre çok uzak olmayan bir zamanda HTML5 standardının yetenekleri kullanıcılar tarafından istenmeye başlayacak ve web üzerinde geliştirme yapan bütün üreticiler standardı programlarına alacaktır. Böyle bir ortamda web uygulamalarının HTML5 standardına kısa zamanda keskin bir geçiş yapacaklarını öngörmek çok da yanlış olmaz.

Bu noktada, özellikle olgun bir HTML4 ile geliştirme hayatlarına başlamış geliştiricilerin HTML5 zafiyetleri konusunda bilgi sahibi olmaları, geliştirme sırasında güvenlik gereksinimlerini de göz önünde bulundurmaları kullanıcılar için hayati önem taşımaktadır. Bu ihtiyaç da web geliştiricilerinin web güvenliği ile ilgili çalışmaları her zamankinden daha yakından ve daha çok takip etmelerini gerektirmektedir.

5. Kaynakça

[1] D.Raggett, A. Le Hors ve I. Jacobs. “HTML 4.01 Specification”. http://www.w3.org/TR/html401/, 24.12.1999 [11.06.2011]

[2] Wikipedia. “HTML5”. http://en.wikipedia.org/wiki/HTML5, 12.06.2011 [12.06.2011]

[3] W3C. “W3C Confirms May 2011 for HTML5 Last Call, Targets 2014 for HTML5 Standard”. 14.02.2011 [12.06.2011]

[4] OWASP. “Cross-site Scripting (XSS)”. https://www.owasp.org/index.php/Cross-site_Scripting_(XSS), 20.10.2010[11.06.2011]

[5] W3C. “Same-Origin Policy”. http://www.w3.org/Security/wiki/Same_Origin_Policy, 06.06.2010 [15.05.2011]

[6] Adobe. “Cross-domain Policy File Specification”. http://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html, 22.01.2010 [15.05.2011].

[7] L. Huang, E. Chen, A. Barth, E. Rescorla, ve C. Jackson. “Talking to Yourself for Fun and Profit”. 5inci “Web 2.0 Security and Privacy” Konferansı, California, US, 2011.

[8] A.Van Kesteren. “Cross Origin Resource Sharing”. 27.07.2010 [15.05.2011].

[9] A.Barth, C. Jackson, ve W.Li. “Attacks on JavaScript mahsup communication”. 3üncü “Web 2.0 Security and Privacy” Konferansı, California, US, 2009.

[10] S. Hanna, E.C.R. Shin, D. Akhawe, A. Boehm, P. Saxena ve D. Song. “The Emperor’s New API: On the (In)Secure Usage of New Client-side Primitives”. 4üncü “Web 2.0 Security and Privacy Conference”, California, US, 2010.

[11] I. Fette. “Hello HTML5”. http://gearsblog.blogspot.com/2010/02/hello-html5.html, 19.02.2010 [25.05.2011].

[12] OWASP. “Cross-site Request Forgery (CSRF)”. https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF), 09.04.2010 [11.06.2011].

[13] “HTML5 Security Cheatsheet”. http://html5sec.org/. [17.05.2011]

Mobil Ağlarda Kimlik Doğrulama Hakkında Bir İnceleme

Fatma Akgün[1], *Ercan Buluş*[2],

[1]Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
Trakya Üniversitesi, Edirne
fatmaa@trakya.edu.tr

[2]Bilgisayar Mühendisliği Bölümü
Namık Kemal Üniversitesi, Tekirdağ
ercanbulus@nku.edu.tr

Özetçe

Günümüzde yaygın olarak kullanılan haberleşme ortamlarında, çeşitli şekillerde kurulan bağlantılarda kişilerin kim olduğunun anlaşılabilmesi büyük bir problemdir. Özellikle telefon haberleşmesinde genellikle sadece ses iletildiğinden konuşulan kişinin kim olduğunu tespit edebilmek çok zordur. Birinci nesil Analog haberleşmede sayısal iletim yapılamadığından kimlik doğrulama işlemini uygulamak mümkün olmasa da sayısal haberleşme imkanı sağlayan mobil haberleşme teknolojisinde kimlik doğrulama işlemini gerçekleştirebilmekteyiz. Sahte kullanıcıları engelleyebilmek için mobil haberleşme cihazlarında cihaz açılırken kişinin kim olduğunun ve bağlanılan sistemin gerçek sistem olup olmadığının doğrulanması gerekmektedir. Karşılıklı kimlik doğrulama adı verilen bu sistem sayesinde kullanıcının mobil ağa dâhil olmasına ve güvenilir görüşmeler yapabilmesine, ayrıca mobil internet imkanı sayesinde verilerini doğru kişilere iletmesine izin verilmektedir. Fakat bazı durumlarda ise kimlik doğrulama yapılsa bile tek taraflı bir doğrulama işlemi yapıldığından haberleşmede yine güven sağlanamaz. Bu bağlantı şeklinde doğru kullanıcının sahte sistemlere bağlanmasına neden olup verilerin çalınması işlemi gerçekleşebilir. Çalışmamızda öncelikle mobil cihazlarda kullanılan kimlik doğrulama işlemleri nesillerine göre sınıflandırıp, bu sistemler üzerinde kullanılan kimlik doğrulama yöntemlerin işlem basamakları incelenildi.

1. Giriş

İlk haberleşme sistemi olan analog haberleşmede sayısal bir iletim yapılamadığından veriler üzerinde şifreleme ya da haberleşen kişiler arasında kimlik doğrulama işlemi yapılamamıştır. Fakat gelişen teknoloji ile sayısal sistemlerin ortaya çıkışı sağlanmış ve kablolu veya kablosuz sistemler üzerinde güvenlik konusunda daha hassas davranılmış ve hem verinin şifreli iletimi hem de haberleşen kişilerin karşılıklı kimlik doğruluğu üzerinde çeşitli güvenlik algoritmaları geliştirilmiştir. Bu sayede iletilen verilerin doğru kişiye ve doğru bir biçimde aktarımı sağlanmıştır. Fakat geliştirilen bu sistemlerde kullanılan güvenlik algoritmaları üzerine kötü amaçlı kişiler tarafından çeşitli saldırılar yapılarak[1], algoritmaları kırıp, verileri ele geçirmek, değiştirmek ve silmek gibi güvenliği ortadan kaldırıcı durumlar amaçlanmıştır. Bu alanda kablosuz haberleşme türü içerisinde yer alan ve son zamanlarda kullanımı yoğun bir biçimde artmış olan mobil haberleşme sistemleri de bu tür saldırılar ile karşı karşıyadır. Mobil teknolojilerin zaman ve mekân gözetmeksizin iletişim imkânı sunması ve ayrıca cep telefonlarının kullanım kolaylığı, küçülen boyutları ve insan hayatını kolaylaştıracak pek çok önemli hizmetler sunması neticesinde toplumda kullanımı her geçen gün daha da fazla artmaktadır. Bu ortamların kullanımının yaygınlaşması ile de bu ortamlara yapılan saldırı sayısında da oldukça artış görülmektedir. Çalışmamız da 2. Nesil ve 3. Nesil mobil haberleşmede kullanılan kimlik doğrulama algoritmaları ve bu algoritmaların güçlü ve zayıf yönleri anlatılacaktır.

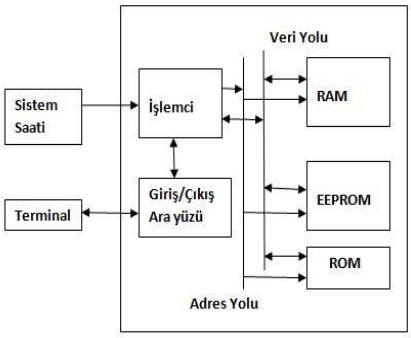
2. Kimlik Doğrulama Nedir?

Kullanıcıların uzak veya yakındaki herhangi bir sisteme giriş yapıp o sistemi kullanabilmesi ya da herhangi bir kişi ile iletişim sağlayabilmesi için kendini o sisteme veya o kişiye tanıtması gerekir. Bu olaya kimlik doğrulama (authentication) denmektedir. Kimlik doğrulama işlemi bir şeyler bilerek kimlik doğrulama örneğin; şifre, bir şeylere sahip olarak örneğin; akıllı kart ya da bazı karakteristik özellikleri kullanarak örneğin; parmak izi vs. şekillerinde yapılabilir[2]. Bazı durumlarda sadece kullanıcının kendini sisteme veya karşı taraftaki kullanıcıya tanıtması haricinde karşı taraftaki kullanıcının ve sisteminde kendini kullanıcıya tanıtması istenebilir. İşte yapılan bu işleme ise karşılıklı kimlik doğrulama denmektedir. Bu yöntemler ile güvenliğin temel ilkelerinden bütünlük ve güvenilirlik sağlanmaktadır. Dünyada artık bankacılık sistemleri, mobil haberleşme, kablosuz haberleşme, akıllı kart sistemleri, e-posta alıp-verme, çevrimiçi alışveriş, okul, hastane, özel şirketler, yurtlar vs. alanlarda kimlik doğrulama işlemi yapılmaktadır. Basit olarak bir kimlik doğrulamada en temel yöntem kullanıcının tanımlayıcısı (ID) ve şifresi ile sistemin kaynaklarına erişmesidir. Bu yöntemde sistemin kaynaklarına erişmek isteyen kullanıcı ID ve şifresini güvensiz ağ üzerinden uzak sisteme iletir. Karşı sistem üzerinde tutulan ID ve şifre tablosu aranır, her iki değerde var olan sistem değerleri ile karşılaştırılır, eşleşirse kullanıcıya sistemin kaynaklarına erişim izni verilir[2,3]. Herhangi bir algoritmadan geçirilmemiş bu değerlerin aktarımları esnasında kötü niyetli kişiler tarafından bu verilerin çalınıp, amaç dışına taşınması olayı gerçekleştirilmiştir. Bu tür sorunları ortadan kaldırmak için kimlik doğrulamada sayısal sertifikalar, imzalar, karmaşık algoritmalar ve şifreleme metotları, belirli kimlik delili, gizli anahtar kullanımı gibi karmaşık işlem gerektiren özel sistemler kullanılarak[3], kullanıcı-kullanıcı, kullanıcı-sistem veya sistem-sistem arasında bilgi hırsızlığının veya sahtekârlığın önüne geçilmek amaçlanmıştır.

3. Mobil Haberleşmede Kimlik Doğrulama?

Mobil haberleşme sistemlerinde kimlik doğrulama yapabilmek için SIM (Subscriber Identity Module) Abone Kimlik Modülü adı verilen kartlar kullanılır. SIM kart üzerinde şebeke tarafından verilen ve şebekeye giriş için kullanılan aboneyle ilgili bilgiler bulunur. SIM; IMSI(International Mobile Subscriber Identity-Uluslar arası Mobil Abone Kimliği), Kimlik Tanıma Algoritması, Kimlik Tanıma Anahtarı ve diğer bilgi ve fonksiyonları içeren güvenli bir modüldür. SIM'in temel fonksiyonu ağ ve MS'in(Mobile Station-Mobil İstasyon) kötü yönde kullanımını engellemek için abone kimlik tanımlaması yapmaktır[4]. Güvenli mikro işlem tabanlı uygulamalarda kullanılan bu modül üzerinde birçok güvenlik testleri uygulanmıştır.

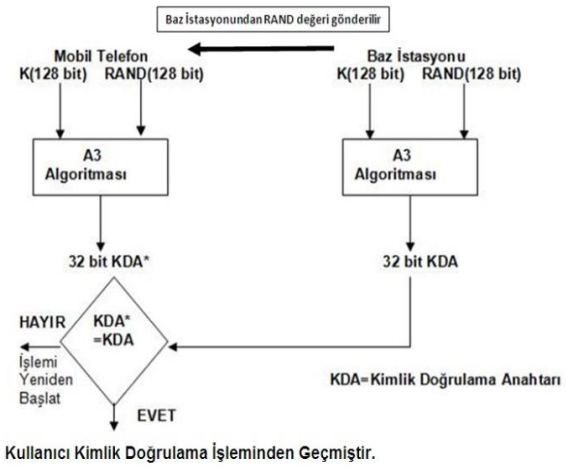
SIM modülü üzerinde RAM, ROM ve EEPROM olarak adlandırılan 3 tür bellek bulunur. RAM belleği; aktarılacak verileri depolar ve işler. CPU (İşlemci) ile çalışan bellektir. CPU, başlangıçta işletim sistemini RAM belleğe yükler. EEPROM belleği; gerçek kullanıcı verilerini ve temel dosya sistemini saklar, abone tanımlamalarını, numara bilgilerini K anahtarını, ağ ilişkili bilgileri ve cihaz tanımlamalarını içerir. Abone kimlik tanımlamaları, hava üzerinde iletilen bilgilerin güvenliği, dosya erişimleri SIM üzerinden yapılmaktadır. ROM belleği; işletim sistemi, uygulamalar ve çeşitli güvenlik algoritmalarını içerir[5]. Bunların yanında verilerin değişimini sağlayan I/O birimi vardır. Bu SIM ile ME (Mobile Equipment-Mobil Cihaz) arasındaki iletişimi sağlar. SIM üzerinde en önemli parametreler şifreleme anahtarının üretimini ve kimlik doğrulanmasını sağlayan IMSI ve K bilgileridir. Bu tür parametreler dışarıdan okunmaya karşı korunmalıdır. Bu verilere ancak özel kilit uygulanmamış kodlar iler erişilebilir. Yani ME, SIM içerisindeki EEPROM'a doğrudan ulaşamaz ancak SIM'in CPU'sundan bu bilgileri isteyebilir. Bu alana doğrudan erişim yasaklanmıştır. CPU, AuC(Authentication Center-Kimlik Doğrulama Merkezi) tarafından sağlanan RAND(rasgele) değerini kullanarak SRES(Signature Response-İmza) bilgisini üretir[6].



Şekil 1: SIM Blok Diyagramı

3.1 İkinci Nesil GSM Haberleşme Sistemi'nde Kimlik Doğrulama

GSM Avrupa'da kullanılan ikinci nesil mobil haberleşme sistemidir. Cep telefonumuzu açtığımız zaman, şebeke, bağlanmak isteyen telefonu önce güvenlik aşamasından geçirir. Bu esnada IMEI (International Mobile Equipment Identity-Uluslararası Mobil Abone Kimliği) numarası ve IMSI numarası kullanıcıdan sisteme gider. Sistem aldığı IMSI numarasını veritabanında sorular ve buradan bu SIM için özel anahtar değer K ifadesini alıp, birde kendi ürettiği RAND değerini A3 (Kimlik Doğrulama algoritması)'e uygulayarak kimlik doğrulama anahtarını üretir[7]. Aynı zamanda bu işlemleri yaparken ürettiği RAND değerini de kullanıcıya göndererek onunda bu işlemleri gerçekleştirmesini bekler. Kullanıcı sistemden gelen bu RAND değerini ve SIM içerisinde bulunan K anahtar değerini alarak yine SIM kart içerisinde bulunan A3 algoritmasına uygular ve elde ettiği sonucu sisteme gönderir. Sistem gelen anahtar değeri ile kendi elde ettiği anahtar değerini karşılaştırır. Doğrulama testi yapıldıktan sonra şebeke, telefonu kendisine kaydeder ve bağlı olduğu MSC(Mobile Switching Center-Mobil Anahtarlama Merkezi) kayıt altında tutulur[3].



Şekil 2: A3 Doğrulama Algoritması

A3 kimlik doğrulama algoritması tek yönlü bir HASH algoritmasıdır. Tek-yönlü HASH algoritması, tek yönlü çalışan bir özet fonksiyonudur. Girdi değerinden özet değerini hesaplamak kolaydır ancak aynı özet değerini veren girdi değerini üretmek zordur. İyi bir tek-yönlü özet fonksiyonu, iki girdi değerinden aynı özet değerinin üretilmesinin zor olduğu fonksiyondur[8]. Tek yönlü özet fonksiyonlarında geri dönüş olamaz, özetten gerçek değer türetilemez. Giriş değerinde yapılan bir bitlik değişim bile özet üzerinde büyük bir değişime neden olabilir. GSM haberleşmesinde kullanılan A3 algoritması güvenilir olmasına rağmen, sistem üzerinde tek taraflı bir kimlik doğrulaması yapıldığından yani baz istasyonunun kullanıcıyı sorgulaması fakat kullanıcının baz istasyonunu sorgulamaması neticesinde konuşmaların dinlenmesi, verilerin değiştirilmesi, e-posta, web, veritabanı sunucularına saldırılarda bulunulması gibi sakıncalı durumlar teşkil edilmektedir[9,10,13]. Bu olumsuz sonuçlar üçüncü nesil haberleşme sistemlerinde karşılıklı kimlik doğrulama yapılmasıyla ortadan kaldırılmıştır.

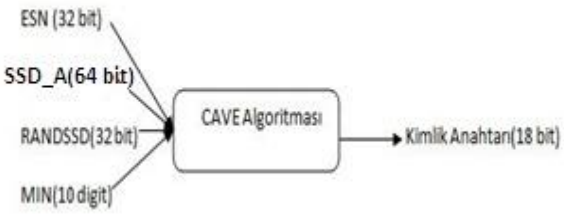
3.2 İkinci Nesil CDMA Haberleşme Sistemi'nde Kimlik Doğrulama

CDMA sistemi Amerika'da kullanılan ikinci nesil haberleşme sistemidir. CDMA ağındaki başlıca güvenlik durumları özel anahtar olan "A_key" ve Elektronik Seri Numarası (ESN) bağlıdır. A_key hem mobil hem de AC (Authentication Center-Kimlik Doğrulama Merkezi) içinde saklıdır. A_key hiçbir zaman hava ara yüzünden aktarılmaz veya sistemler arasında gönderilmez. En yüksek seviyede her iki sistemde bu ana anahtar değere sahiptir. Ana anahtar değeri; alt anahtarların üretimi ve kimlik doğrulama için kullanılır.

Bu değer 64 bit gizli anahtardır ve
1-) Kimlik Doğrulama
2-) Ses Gizliliği
3-) Mesaj şifreleme için kullanılır.

Bu değerleri üretebilmek için sistem üzerinde CAVE (Cellular Authentication and Voice Encryption- Hücresel Kimlik Doğrulama ve Ses Şifreleme) algoritması uygulanır. CAVE; kimlik tanıma, anahtar elde etme, gizlilik ve veri koruma için kullanılan basit türde bir 128 bitlik, 4 veya 8 döngüde işlem yapan bir HASH fonksiyonudur. CAVE, mobil aboneleri sahtekâr kopyalama işlemlerinden korumak için hedef alınan bir algoritmadır[11,12].

CDMA Sisteminde yapılan ilk işlem, ana anahtar değerinden işlem yapılacak diğer anahtarları bulmaktır. CDMA'de kimlik imzası ve oturum anahtarları üretmek için kullanılan en yüksek seviyedeki anahtar değer 64 bitlik A_key değeridir. Bu değer ile 128 bitlik "Shared Secret Data" üretilir. Bu değerin ilk 64 biti SSD_A ve son 64 biti SSD_B olarak ifade edilir. İkinci işlem elde edilen bu 64 bitlik SSD_A değerinden, 18 bitlik Kimlik imzası üretmektir. Bunun için gerekli olan giriş değerleri ve çıkış değerleri aşağıda gösterildiği gibidir;



Şekil 3. Kimlik İmzası Oluşumu

Fakat CDMA sisteminde de kimlik doğrulama işleminde bazı olumsuz durumlar vardır. Örneğin; kimlik doğrulama anahtarını oluşturmak için kullanılan A_key değerinin GSM' de 128 bit olmasına rağmen burada 64 bit olması, ayrıca elde edilen kimlik doğrulama anahtarının GSM' de 32 bit olmasına rağmen bu sistemde 18 bit olması kimlik doğrulama işleminde zayıflık oluşturmaktadır. Bunun yanı sıra yine GSM' de olduğu gibi kimlik doğrulama işleminin tek taraflı olması yani kullanıcının kimlik doğrulamadan geçirilmesi fakat baz istasyonun kimlik doğrulamadan geçirilmemesi durumunda sahte baz istasyonlarının konuşmaları dinleyebilmesi veya değiştirebilmesi durumları yaşanabilir. Tüm bunlara ek olarak hem kimlik doğrulama anahtarı hem de şifreleme anahtarının oluşumunda aynı algoritmanın yani CAVE algoritmasının kullanımı güvenlik eksikliği sorunları arasında sayılabilir[14]. Tüm bu durumları aşabilmek için üçüncü nesil haberleşme sistemlerinde güvenlik konusunda daha hassas davranılmıştır.

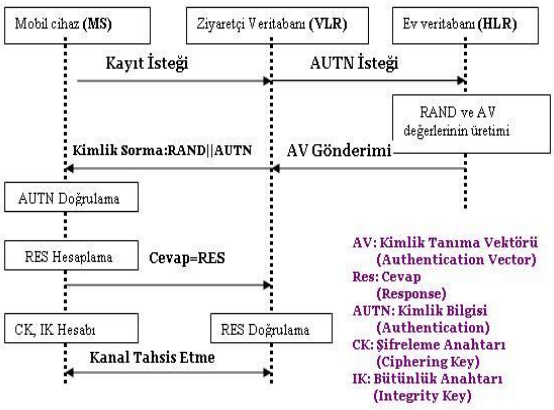
3.3 Üçüncü Nesil UMTS Haberleşme Sistemi'nde Kimlik Doğrulama

UMTS (Universal Mobile Telecommunication System-Uluslar arası Mobil İletişim Sistemi) sistemi Avrupa'da kullanılan üçüncü nesil mobil haberleşme sistemidir. Bu haberleşme sistemi 128 bit uzunluklu şifreleme anahtarı ve karşılıklı kimlik doğrulaması gibi işlemlerle daha güçlü bir şifreleme algoritmasına sahip olmuştur. UMTS, AKA (Authentication and Key Agreement Protocol-Kimlik Doğrulama ve Anahtar Anlaşma Protokolü) kullanarak ağ erişim güvenliği sağlar. Karşılıklı kimlik doğrulama, kullanıcının SIM kartı ve sistem arasında yapılmaktadır. UMTS AKA, ayrıca güvenilirlik ve bütünlük için oturum anahtarlarının üretiminden de sorumludur.

AKA işlemi 3 adımda gerçekleşir.
İlki bazı bilgilerin, sorgu-cevap şeklinde aktarılmasıdır. Kimlik tanımlama işlemini başlatmak üzere öncelikle MS, SIM içerisinde yer alan bazı özel değerleri (IMSI, IMEI) servis ağına gönderir. Kimlik tanımlama işleminde HLR (Home Location Register-Ev Ziyaretçi Ağı) ve AUC (Authentication Center-Kimlik Doğrulama Merkezi) başlıca rol oynar.

İkinci adım, kimlik doğrulama merkezi kendisine gelen özel değere (IMSI) bakarak veritabanından bu kullanıcıya ait anahtar değerini alır (K-128 bit), rastgele bir sayı üretip (RAND) bunu da alarak kimlik doğrulama algoritmasından (AES-MILENAGE)[15] geçirir ve hem bu algoritmadan elde ettiği sonucu (AV-Authentication Vector- Kimlik Doğrulama Değer Dizisi) ve hem de rastgele ürettiği değeri baz istasyonu kontrolcüsüne gönderir.

Üçüncü adımında, baz istasyonu kontrolcüsü, kullanıcı-ağ arasında karşılıklı kimlik tanımlamayı gerçekleştirmek üzere kendisine gelen (AV) değeri içerisinden $kimlik_{baz}$(AUTH) değerini ve rastgele(RAND) sayı değerleri SIM'e gönderir. SIM kendisine gelen rastgele değeri ve kendisinde bulunan özel anahtar değerini (K) kimlik doğrulama algoritmasından (AES-MILENAGE) geçirir ve kimlik anahtarı (K_{baz}) üretir ve bu anahtarı baz istasyonu kontrolcüsünden gelen değer ile karşılaştırır eğer her iki değerde eşit ise SIM ağı kimlik denetiminden geçirmiş olur, daha sonra SIM, yeni bir kimlik değeri hesaplayarak(RES) bunu baz istasyonuna gönderir. Baz istasyonu da kendinde bulunan K_{sim} (RES) değeri bu değeri karşılaştırır ve aynı ise baz istasyonu kontrolcüsü SIM'i doğrulamış olur ve her iki birim arasında güvenilir bir şekilde karşılıklı görüşme yapılabileceği kararına varılır. Şekilde görüldüğü gibi UMTS ve CDMA2000 benzer AKA işlemine sahiptir. 2G ağlarda, kullanıcı ağı kimlik denetiminden geçirmez sadece ağ kullanıcıyı kimlik denetiminden geçirir. Bu sebepten kullanıcının ağı reddetme şansı yoktur ve bu durum sahte baz istasyonlarının kurulup, verinin çalınması, değiştirilmesi veya silinmesi gibi durumlara yol açabilir, fakat UMTS ve CDMA2000 içerisinde karşılıklı kimlik doğrulaması işlemi yapıldığından bu tür durumlarla karşılaşmak mümkün değildir.



Şekil 4. AKA: UMTS ve CDMA2000 İçerisinde Kimlik Tanıma İşlemi

USIM ve AUC, içerisinde gerçekleşen AKA işleminde (f0-f5) kriptografik fonksiyonlar kullanılır. UMTS, AKA işlemini gerçekleştirmek için MILENAGE algoritmasını kullanır. MILENAGE, simetrik blok şifreleme olan RIJNDAEL algoritması üzerine inşa edilmiştir. Ev ağından (HE), Ziyaretçi ağına (VLR) ağına gönderilen AV, bir bilgi kümesidir. Bu değer, RAND, XRES, CK, IK ve AUTN gibi kimlik bilgilerine sahiptir. AKA prosedürü içinde yer alan farklı fonksiyonlar ve USIM/AUC içerisinde bulunan 128 bitlik master K anahtarı, kimlik tanımlama bilgilerini üretmek için kullanılır[19].

RAND=f_0(Internal State) **MAC=f_1**(K,SQN||RAND||AMF)
XRES=f_2(K,RAND) **CK=f_3**(K,RAND)
IK=f_4(K,RAND) **AK=f_5**(K,RAND)
AUTN=SQN[XOR]AK||AMF||MAC

Fn	Amacı	Algoritma
f0	Rasgele sayı üretmek	MILENAGE
f1	Ağ kimlik tanıma fonksiyonu	MILENAGE
f1*	Resenkrazyonu sağlayan mesaj kimlik tanıma fonksiyonu	MILENAGE
f2	Kullanıcı sorgu-cevap kimlik tanıma fonksiyonu	MILENAGE
f3	Şifreleme anahtarı elde etme fonksiyonu	MILENAGE
f4	Bütünlük anahtarı elde etme fonksiyonu	MILENAGE
f5	Normal işlem için anonymity anahtarı elde etme fonksiyonu	MILENAGE
f5*	Resenkrazyon Anonymity anahtar elde etme fonksiyonu	MILENAGE

Tablo 1. AKA İçerisinde Yer Alan Fonksiyonlar ve Amaçları[17]

AUTN içindeki SQN numarası sürekli güncellenerek against replay attack'larından korunmayı sağlar. AMF bilgi alanıdır. AK (Anonymity Key) SQN'in serilerini gözlemleyerek, kimlik tanıma izini saklamak için SQN ile XOR'lanır. USIM, RAND, AUTN ve f_1,f_2,f_3,f_4,f_5 ile ilk SQN değerini hesaplar[16]. UMTS içindeki güvenilirlik sistem sinyalinin ve dataların korunmasını sağlarken, bütünlük koruma sadece sistem sinyalinin korunmasından sorumludur.

3.4 Üçüncü Nesil CDMA2000 Haberleşme Sistemi'nde Kimlik Doğrulama

CDMA2000 (Code Division Multiple Access - Kod Bölmeli Çoklu Erişim) Amerika'da kullanılan üçüncü nesil mobil haberleşme sistemidir. CDMA2000 mimarisi, IMT-2000 (International Mobile Telecommunication 2000- Uluslar arası Mobil İletişim 2000)'den elde edilir ve 3GPP2 (3 Generation Partnership Project 2- Üçüncü Nesil Ortaklık Projesi 2) tarafından belirlenmiştir. Bu sistem önceki 2G/2.5G'yi temel alır. İçerisinde kullanılan AKA prosedürü de, UMTS AKA prosedürünün benzeridir. CDMA2000 sisteminde kimlik doğrulama işleminde en önemli durum UIM(User Identity Module) ve AC (Authentication Center) içerisinde ilk etapta bulunacak olan K başlangıç anahtarının oluşturulmasıdır ve bu anahtar değerin oluşumu çeşitli şekillerde olabilir[18]. Bazı durumlarda eğer SIM kart taşınabiliyor ise (GSM, CDMA ve UMTS sistemlerinde de bu şekildedir) K değeri USIM içerisine gömülür, eğer USIM kart taşınamaz ise sadece telefona özgü ise bu durumda K değeri telefon içerisinde var olan hafızaya gömülür. K değerinin önemi büyüktür çünkü bu değer sayesinde AKA algoritması içerisinde mobil ve servis ağı arasında oturum anahtarları oluşturulur ve veriler güvenilir bir şekilde gönderilir. CDMA2000 sisteminde UMTS'e göre bazı yeni kriptografik fonksiyonlar eklenmiştir. F11 ve UMAC gibi. F11, AV içerisinde yer alan UIM Kimlik Anahtarı (UAK-USIM Authentication Key) üretmek için kullanılır. UAK kullanılarak sistem roque shell saldırılarından korunur. UMAC veya MAC fonksiyonları ise sinyal verisinin bütünlüğünü korumak için kullanılır. UMAC fonksiyonu, IK (Integrity Key-Bütünlük Anahtarı) ve UAK değerlerinin her ikisine de bağlıdır. Ama bazı zamanlar sadece IK değerine bağlı kalabilir. UAK'ın kullanımı opsiyoneldir. UMAC, sadece UIM içerisinde hesaplanabilir hava ara yüzü ile iletilmez. UMAC'ın kullanımı etkili bir tekrarlı kimlik tanımlama işlemi sağlar. AKA algoritmasında, ek bazı kriptografik fonksiyonlar da kullanılabilir. SHA-1, cdma2000 içerisinde bazı durumlarda kullanılan tek yönlü bir çekirdek fonksiyondur. Kullanıcı kimlik tanımlaması, anahtar elde edilmesi ve mesaj kimlik tanımlaması gibi durumlar için kullanılırken bazı durumlarda da, bu işlemler için CDMA2000, SHA-1 Core Compression fonksiyonu nu kullanır[18]. CDMA2000 sisteminde UMTS sisteminde olduğu gibi kullanıcı ve servis ağı arasında gizlilik ve bütünlük koruma değerleri hat üzerinden direk gönderilmez. Bu duruma çözüm olarak SS7 protokolünü veya IPSec tüneli sayesinde veri aktarımı sağlanır ve bu güvenilir tünel oluşumları ile 3. Şahısların veriye erişimi engellenir.

4. Mobil Teknolojiler Arasında Kimlik Doğrulama İşleminin Karşılaştırılması

Mobil sistemlerin gelişimi ile kimlik doğrulama ve verilerin şifreli iletimi konularında önemli gelişmeler sağlanmıştır. 2G sistemler olan GSM ve CDMA sistemlerinde kimlik doğrulamanın tek taraflı yapılması, yani sadece kullanıcının denetlenmesi fakat baz istasyonunun denetlenmemesi sonucu verilerin yanlış kişilerin eline geçmesi, sahte baz istasyonlarının kurulup gerçek kullanıcının hattından görüşmeler yapılıp faturanın gerçek kullanıcıya yansıması gibi çeşitli saldırılara maruz kalınmıştır. Bunun yanı sıra kimlik doğrulama algoritması sonucu elde edilen kimlik anahtar değer uzunluğunun yeterli güvenliği sağlayacak biçimde olmaması ve bu sebepten dolayı yapılan kriptanaliz işlemleri sonucu anahtar değerin zorluk oluşturmadan kolayca elde edilmesi nedeniyle ve bu sistemler üzerinde verinin iletiminde şifreleme işleminin sadece kullanıcı ve baz istasyonu arasında olması, yani baz istasyonundan sonra verinin, kimlik doğrulama merkezine iletiminde herhangi bir şifreleme işleminin olmaması sonucu bu sistemleri kullanmada çeşitli güvenlik açıkları ortaya çıkmıştır. Tüm bu eksikleri gidermek üzere geliştirilen 3G UMTS ve 3G CDMA2000 sistemleri üzerinde hem karşılıklı kimlik doğrulama yapılabilmesi hem de elde edilen kimlik doğrulama anahtarının boyunun yeterli uzunlukta olması ve tüm bunlara ek olarak kullanıcıdan başlayıp kimlik doğrulama merkezine kadar verilerin tamamen şifreli iletimi sonucu 2G sistemlerinden 3G sistemlerine geçişe büyük sebep olunmuştur. Bu sayede doğru kişilerle görüşülmesi, araya 3. kişilerin girip konuşmaları dinleyememesi, verilerin yetkisiz kişilerce ele geçirilmesi, silinmesi, değiştirilmesi veya gerçek kullanıcının hattına girip görüşmeler yapılıp faturalamanın yine gerçek kullanıcıya yansıması gibi durumlarının önüne geçilmesi amaçlanmıştır.

5. Sonuçlar

Günümüzde Mobil haberleşmenin sağladığı imkânlar arasında istenildiği zaman veya istenildiği yerden hem sesli, hem görüntülü konuşma yapabilme imkânı, internete sorunsuzca erişip e-posta alıp-verme, haber okuma, araştırma yapma, ders kaydı yapma, ders notu elde etme, sınav sonucu öğrenme, banka işlemleri yapabilme, e-alışveriş yapabilme vs. durumlarını sayabiliriz. Fakat teknolojinin sağlamış olduğu bu kolaylıkların yanında tehlikelere de maruz kalması kaçınılmaz olmuştur. Bu sebeple sistemler üzerinde güvenlik konusunda detaylı çalışmalar yapılmıştır ve halen de yapılmaktadır. Yaptığımız araştırmalar sonucu mobil haberleşmenin temeli olan 2G sistemlerinde bu hususlarda bazı açıklar olmasına rağmen 3G sistemler üzerinde bu açıkların giderildiği görülmüştür.

REFERANSLAR

[1] SAĞIROĞLU, S., MOHAMMMED, M., "Mobil Ortamlar Üzerine Yapılan Saldırılar Üzerinde Bir İnceleme", TUBAV, Yıl: 2009, Cilt:2, Sayı:2, Sayfa:138-147.

[2] ÖZKOÇ, E., "Akıllı Kart Tabanlı Uzaktan Kimlik Doğrulama Sistemi Tasarımı", Yüksek lisans Tezi, Gebze İleri teknoloji Enstitüsü, 2008.

[3] ALAZEIB, A., "An Ontology for Generic Wireless Authentication", Thesis, Stuttgart, 07.October.2005.

[4] VEDDER , K., "Smart Cards", Chairman ETSI TC SCP, Group Senior VP, Giesecke & Devrient, 2nd ETSI Security Workshop, 1997.

[5] REDL, S. M., WEBER, M. K., OLIPHANT, M. W.," GSM and Personel Communaticon Handbook", Artech House, Boston LONDON,1998.

[6] Martin SAUTER," Communications Systems for the Mobile Information Society", Nortel Networks, Germany,2006.

[7] ERGÜLER, İ., KARAHİSAR, A., ANARIM, E., "GSM İletişim Sistemindeki Zayıflıklar ve Olasıl Saldırılar", SAVTEK 2004, 24-25 Haziran, ODTU, Ankara.

[8] BUDAK, B., " Güvenli Özet Algoritması", Yükseklisans tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Temmuz 2010.

[9] MEYER, U., WETZEL, S., "On The Impact of GSM Encryption and Man-In-The-Middle Attacks On The Security of Interoperating GSM/UMTS Networks", 2004 IEEE.

[10] Bulus E., "Designing attacks for SMTP servers", International Journal of Computer Systems Science and Engineering 26-1, Jan 2011, pages: 43-48.

[11] ROSE, G., "Authentication and Security in Mobile Phones", QUALCOMM Australia.

[12] BALANI, A., "Authentication and Encryption in CDMA Systems", LG Soft India Private Limited Mumbai-India.

[13] BOCAN, V., CRETU, V., "Threats and Countermeasures in GSM Networks", Journal of Networks, Vol. 1, No. 6, 2006.

[14] CHEN, J. C., ZHANG, T., "IP-Based Next-Generation Wireless Networks, Chapter 5: Security", 2004.

[15] "Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication 197, November 26, 2001

[16] NYBERG, K., "Cryptographic Algorithms for UMTS", European Congress on Computational Methods in Applied Sciences and Engineering, ECCOMAS 2004

[17] KQIEN, G., TELENOR R&D and AGDER UNIVERSITY COLLEGE, "An Introduction to Access Security in UMTS", IEEE Wireless Communications, 2004.

[18] ROSE, G., KQIEN, G., TELENOR R&D and AGDER UNIVERSITY COLLEGE, "Access Security in CDMA2000, Including a Comparison with UMTS Access Security", IEEE Wireless Communications, 2004.

[19] ALTUN, M., "Yeni Nesil Kablosuz Mobil Ağlar İçin Bir Sanal USIM Uygulaması", Yükseklisans Tezi, Ege Üniversitesi Fen Bilimleri Enstitüsü, 2009.

Kablosuz Geçici Ağlarda Yönlendirme Saldırılarının Analizi ve Önlenmesi

İbrahim Zağlı[1] Güray Yılmaz[2] Coşkun Sönmez[3]

[1,2]Bilgisayar Mühendisliği Bölümü, Hava Harp Okulu, İstanbul
[3]Bilgisayar Mühendisliği Bölümü, Yıldız Teknik Üniversitesi, İstanbul

[1]e-posta: zagli@hho.edu.tr [2] e-posta: gyilmaz@hho.edu.tr
[3] e-posta: acsonmez@yildiz.edu.tr

Özetçe

Hareketli Geçici Ağlar, düğümler arası bağlantıların çok zorlu bir iletişim ortamı oluşturacak kadar değişken ve çoğunlukla tutarsız olduğu, kendiliğinden ortaya çıkan (erişim noktası v.b. olmadan) kablosuz ağlardır. Bu nedenle, her düğüm komşularının ötesindeki düğümlerle haberleşebilmek için diğer düğümlere muhtaçtır ve diğerlerinin iletişimini desteklemek için bir yönlendirici gibi hareket etmek zorundadır. Ağ içerisindeki bir düğüm belirgin bir biçimde arızalı olması veya ağ kaynaklarını sadece kendisinin kullanmak istemesi ya da daha da kötüsü belirli bir düğüm veya düğüm grubunun iletişimini engellemeye çalışması sonucu protokol kurallarının gerektirdiğinden farklı hareket edebilir. Hareketli Geçici Ağlar üzerinde yönlendirme işlemini gerçekleştirmeye çalışan protokoller için kritik problem sahalarından birisi yönlendirme ihlallerinin ayırt edilmesi ve olumsuz etkilerinin azaltılmasıdır. Bunun yapılabilmesi ve ağ üzerinde adil ve etkin kaynak kullanımının sağlanabilmesi için ihlal modelleri hakkında yeterli bilgiye sahip olunması gerekir. Bu çalışma kapsamında, literatürde üzerinde çalışılan ihlal yöntemleri sebep oldukları sonuçlar açısından analiz edilerek temel savunma yöntemleri tasarlanmıştır.

1. Giriş

Yakın gelecek için en umut vadeden sayısal iletişim ortamı olması nedeniyle, özellikle son 10 yılda Hareketli Geçici Ağlar (HGA) üzerinde bir çok araştırmacı tarafından çok yönlü araştırmalar yapılmaktadır [1,2,3]. Hareketli Geçici Ağlar, düğümler arası bağlantıların çok zorlu bir iletişim ortamı oluşturacak kadar değişken ve çoğunlukla tutarsız olduğu, kendiliğinden ortaya çıkan (erişim noktası v.b. olmadan) kablosuz ağlardır [1].

Herhangi bir merkezi yönetim mekanizmasının yokluğunda, HGA bünyesinde, her düğüm komşularının ötesindeki düğümlerle haberleşebilmek için diğer düğümlere muhtaçtır ve diğerlerinin iletişimini desteklemek için bir yönlendirici gibi hareket etmek zorundadır. Bu sebeplerden dolayı, HGA araştırmalarında yoğun olarak çalışılan temel konulardan biri de yönlendirme protokolleri olmuştur [4,5,6].

Veri paketlerini herhangi bir düğümden (kaynak) bir diğer düğüme (hedef) aktarmak için ihtiyaç duyulacak ara düğümlerin tespit edilmesi olarak tanımlanabilecek olan temel HGA yönlendirme probleminin üstesinden gelmek üzere araştırmacılar tarafından çok çeşitli ve bazıları yoğun şekilde kabul görmüş (AODV, TORA, vb.) önerilerde bulunulmuştur [8]. Veri paketlerinin takip edecekleri yolun tespit edilmesi işlemine yol tespiti adı verilir. Yol keşfi ve yol seçimi olarak iki bölüme de ayrılabilecek olan yol tespiti işlemi gerek herhangi bir ihtiyaç ortaya çıkmadan önce (proaktif, pro-active), gerekse ihtiyaç ortaya çıktığı anda (on-demand) gerçekleştirilebilir [16]. Her iki durumda da etkili ve sağlıklı bir iletişim ortamının oluşabilmesi için HGA'yı oluşturan düğümlerin yüksek seviyede eş güdüm içerisinde olmaları çok önemlidir.

Son dönemde gelişen çoklu ortam uygulamalarının yaygınlaşması ile HGA üzerinde bu uygulamaların ihtiyaç duydukları kalite kısıtlarının karşılanabilmesi için yönlendirme protokolleri seviyesinde özel önlemler alınmasının gerekliliği ortaya çıkmıştır [1,6]. Bunu en temel nedeni, hareketliliğin sonucu zaten oldukça yetersiz, değişken olan ağ kaynaklarının içerisinden belirli kısıtlara uygun olanların seçilmeye çalışılmasının zorluğudur. Bütün bunlara ilave olarak yönlendirmenin gerçekleştirilmesi için gereken eşgüdüm unsuru bu şartlar altında çok daha kritik bir hal almaktadır. Bu alanda bir çok bilimsel çalışma yapılmış olsa da henüz uluslararası standart olarak kabul görmüş mevcut bir çalışma bulunmamaktadır [5].

Ağ içerisindeki bir düğümün belirgin bir biçimde arızalı olması veya ağ kaynaklarını sadece kendinin kullanmak istemesi ya da daha da kötüsü belirli bir düğüm veya düğüm grubunun iletişimini engellemeye çalışması sonucu protokol kurallarının gerektirdiğinden farklı hareket ettiği duruma *yönlendirme ihlali* adı verilir.

Kalite kısıtlı olsun ya da olmasın HGA üzerinde yönlendirme işlemini gerçekleştirmeye çalışan protokoller için kritik problem sahalarından biri yönlendirme ihlallerinin ayırt edilmesi ve olumsuz etkilerinin azaltılması konusudur. Bunun yapılabilmesi ve ağ üzerinde adil ve etkin kaynak kullanımının sağlanabilmesi için ihlal modelleri hakkında yeterli bilgiye sahip olunması gerekir. Yönlendirme ihlallerinin bazı ortak noktaları olmasına rağmen, uygulamada olan yönlendirme protokolü kuralları değişiklik gösterebileceğinden alınacak önlemlerin de protokol bazında değerlendirilmesi gerekmektedir.

Son dönemde, *telaş saldırıları* [18], *solucan deliği saldırıları* [19] ve *sybil saldırıları* [17] gibi belirli ihlal modellerine odaklı çeşitli önerilerde bulunulmuştur. Bunlara ilave olarak ağ üzerinde güven düzeyi bilgisine dayalı bir yapı oluşturmaya yönelik çözüm yöntemleri de önerilmiştir [4,5,6].

Önerilen yöntemlerin büyük çoğunluğu kurallara uyan düğümlerin menzilleri içerisindeki süregelen iletişimi dinlemelerine yönelik önlemler içermektedirler

[7,14,15,16]. İletişimin dinlenmesi aynı zamanda değerlendirilmesi anlamına gelmektedir. Ayrıca, bu değerlendirme sonucunda etraftaki düğümler için karar verilen bir güven seviyesi bilgisi diğer düğümler ile paylaşılarak, bütün düğümlerin hareket tarzı hakkında fikir edinilmekte ve bu bilgiye dayanarak düğümlerin iletişim ağından faydalanma seviyelerine karar verilmektedir [9]. Bu yaklaşım, en temel anlamda, kurallara uyan düğümler için sürekli fazladan işlem maliyetine sebep olmaktadır.

Bu çalışma kapsamında, ikinci bölümde daha önceki çalışmalarda belirlenmiş olan saldırı türleri analiz edilmiş, üçüncü bölümde ihlal modellerinin temel özellikleri, zayıflıkları ve doğurdukları sonuçlar incelenmiştir. Takiben dördüncü bölümde, bu çalışmaların ışığında belirlenen anahtar özelliklere karşı beş temel savunma modeli tasarımları açıklanmıştır.

2. Saldırı Türlerinin Analizi

Yönlendirme protokollerinin büyük çoğunluğunda yürütülen işlemleri 3 ana aşamaya ayırmak mümkündür [1];

- Yol keşfi ve seçimi
- Veri paketi iletimi
- Yol bakımı

Yol keşfi ve seçimi aşamasında, kaynak düğümden hedef düğüme ulaşmak için, veri paketlerinin sırasıyla iletileceği ara düğümler tespit edilmeye çalışılır. Bu aşama ağ içerisindeki yüksek katılımlı işbirliğinin başlaması gereken aşamadır. Genellikle "RREQ" adı verilen nispeten çok küçük boyutlu bir yol istek paketinin ağ içerisinde yayınlanması yoluyla başlar. Bazı protokollerde "RREQ" paketi hedef düğüme ulaştığında bazılarında ise "RREQ" yayınına cevap olarak yayınlanan "RREP" isimli cevap paketlerinin kaynağa ulaşmasıyla sona erer. Toplanan bilgi kullanılarak hedef ya da kaynak düğüm tarafından veri paketlerinin izleyeceği yola karar verilir [10,12,13]. Özellikle değişikliğe aşırı hassas olan kalite kısıtlı iletişimde kullanılan yönlendirme protokollerinde yol seçimi işlemi daha sonraki aşama içerisine aktarılabilmektedir [1].

Veri paketlerinin iletimi aşaması, yol keşfinin başarılı şekilde tamamlanmasını müteakip başlar. İletişimin esasen gerçekleştiği aşama bu aşamadır. Önceki aşamada kesin olarak belirlenmiş olan ya da iletim sırasında belirlenmesi için gerekli bilgilerin toplanmış olduğu yol kullanılarak veri paketleri hedef düğüme ulaştırılır.

Üçüncü aşama, HGA mevcut olduğu sürece tekrarlanan bir aşamadır. Bu aşamada, ağ içerisinde iletişim devam ederken değişen durumlara hızlı şekilde reaksiyon göstererek yönlendirme işleminin arzu edilen şekilde devam etmesine olanak sağlamaya çalışılır. Değişen bağlantı durumlarının ve komşuluk bilgilerinin etraftaki diğer düğümlere özel bir bilgi paketi yardımıyla rapor edilmesi ve alınan bilgi paketlerinin gerektirdiği hareket tarzının yerine getirilmesi şeklinde çalışır [1].

Yönlendirme protokolü ihlalleri bahsi geçen aşamalardan herhangi birisinde olabileceği gibi birden fazla aşamaya yayılmış birleşik bir saldırı şeklinde de gerçekleşebilir.

Belirli bir düğüm ya da düğüm grubu tarafından yönlendirme protokolü kurallarının ihlal edilmeye çalışılmasının sebepleri;

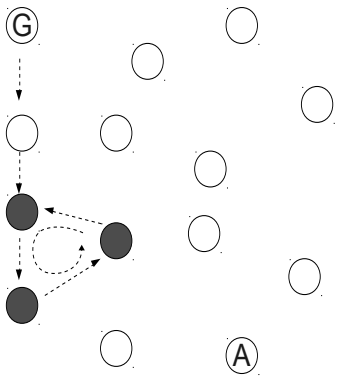
- Ağın belirli bir bölgesindeki iletişimi engellemek,
- Belirli bir düğümün iletişimini engellemek,
- Ağ kaynaklarının kendisine tahsisini sağlamak
- Arıza durumları

olarak sıralanabilir [13]. Bu amaçlara ulaşmak için saldırgan düğüm (veya düğüm grubu) tarafından gerçekleştirilebilecek farklı ihlal modelleri konu alınarak bir çok çalışma yapılmış ve yapılmaktadır [17,18,19]. Bu bağlamda en çok kullanılan ihlal modelleri ortak ve ayrılan noktalarının bulunması amacıyla analiz edilmişlerdir.

2.1. Yönlendirme çemberi

Yönlendirme çemberi (loop), sahte yönlendirme paketleri göndererek veri paketlerinin belirli sayıda düğüm arasında döngüye girmesini sağlamak yoluyla enerji ve bant genişliğini tüketmeyi amaçlayan ihlal türüdür. Saldırgan düğüm yol keşfi aşamasında normal şekilde davranabileceği gibi kendi üzerinden geçen yolun seçilmesini sağlamaya yönelik çok cazip cevaplar da verebilir.

Sonraki aşamada, Şekil 1'de gösterildiği gibi, saldırgan düğüme iletilmek üzere ulaşan veri paketleri eğer saldırgan düğüm yalnız ise yol keşfi aşamasına katılmayan bir düğüme gönderilebilir ya da varsa diğer saldırgan düğümler yardımıyla belirli bir grup düğüm arasında dolaşması sağlanabilir. Her iki durumda da dışarıdan gözlendiğinde söz konusu saldırgan düğümün gelen veri paketlerini ilettiği görülecektir. İhlalin anlaşılması için gözleyen düğüm tarafından her paketin hangi düğüme iletilmesi gerektiğinin bilinmesine ihtiyaç vardır. Böyle bir bilginin bütün düğümler tarafından kaydedilmesine çalışmak iletişimle doğrudan ilgili olmayan düğümlerin çok fazla gereksiz işlem gücü ve bellek harcaması anlamına geleceği değerlendirilmelidir. Literatürde kabul görmüş halleriyle birçok HGA yönlendirme protokolü bu saldırıya açıktır [25]. Yol keşfine katılmayan düğümlere veri paketi iletilmesi durumunda paketi alan düğüm saldırgan değil ise durumun rapor edilerek saldırgan düğümün iletişimin dışında tutulmasını sağlamak mümkündür ve tek saldırgan olduğu durumda basit ve etkili bir yöntem olacaktır. Birbirlerine komşu olan bir grup saldırgan düğüm kullanıldığında savunulması oldukça zor, çok etkili bir saldırı olarak kalacaktır.



Şekil 1: Yönlendirme çemberi saldırısı.

2.2. Yönlendirme kara deliği

Yönlendirme kara deliği (blackhole), saldırgan düğüme ulaşan bütün paketlerin göz ardı edildiği ihlal biçimidir. Amacı; HGA üzerinde iletişimin engellenmesi olabileceği gibi, kaynakların başkaları tarafından kullanılmasını engellemek de olabilir. Bazen bir düğüm istem dışı hatalı çalıştığında ortaya çıkabilir. Örneğin, ayarları yanlış yapılmış bir güvenlik duvarı uygulaması, gelen bütün paketlerin göz ardı edilmesine sebep olabilir. Her iki durumda da hızla tespit edilip bertaraf edilmediği takdirde süregelen iletişimler açısından ciddi sonuçlar doğuracaktır [11,20].

Yol keşfi aşamasında yayınlanan paketler de dâhil olmak üzere gelen bütün paketleri göz ardı etmesi halinde yol keşfine katılmadığı için, saldırgan düğüme veri paketi iletilmeyecektir. Bu durum ilk bakışta güvenli gibi görünse de özellikle düğüm yoğunluğunun az olduğu ağ ortamlarında ağın belirli bölgelerine erişimi güçleştirebilecek ve bölümlenmeye sebep olabilecektir. Bu tür ihlallerin asıl tehlikeli oldukları durum, bilinçli olarak sadece veri paketlerinin göz ardı edildiği, diğer protokol paketlerine tamamen normal davranıldığı durumdur. Yol keşfi ve yol bakımı amacıyla yayınlanan paketlere normal cevaplar veren bir saldırgan düğüm, kendisine yönlendirilmek üzere gönderilen veri paketlerini göz ardı ederek iletişimi engelleyecektir. Genellikle geriye raporlama yapmayacağı ya da olumlu raporlar göndereceği için tespit edilmesi güçtür [28].

Yol keşfine katıldığı durumlarda, yol seçimi aşamasını ara düğümlere dağıtan yönlendirme protokolleri [1] üzerinde bile etkili olabileceğinden bu durumu tespit eden bir mekanizmanın kurulmasına ihtiyaç olabileceği değerlendirilmektedir.

2.3. Yönlendirme gider deliği

Yönlendirme gider deliği (sinkhole), saldırgan düğümün bütün yönlendirmeyi üzerine alacak şekilde kontrol paketleri yayınlayarak kendisine ulaşan veri paketlerinin silindiği ya da içeriğinin değiştirildiği saldırı biçimidir [25]. Kara delik saldırılarından farklı olarak paketleri üzerine çekmek için yol keşfi aşamasına müdahale etmektedir. Literatürde ki birçok çalışmada kara delik saldırılarıyla girişimli şekilde ele alınmışlardır. Ayrıca ileride bahsedilecek olan gri delik saldırılarına da çok benzemektedirler.

Veri paketlerinin göz ardı edilmesi, protokolün ağ üzerinde çalışmasını engelleyecektir. Çünkü yol üzerinde saldırgan düğümden sonra yer alan düğümlerin olup biten ile ilgili herhangi bir bilgileri olmayacaktır. Daha da kötüsü, özellikle UDP iletişiminde, kaynak düğüm ile saldırgan düğüm arasında yer alan düğümlere de herhangi bir problem rapor edilmediği için, iletişimin sorunsuz devam ettiği varsayılacaktır. TCP iletişim kendi standardında bulunan ACK uygulaması sayesinde en azından iletişimin normal olmadığı bilgisini edinecektir. Yönlendirme protokolü seviyesinde, kaynak ve hedef düğüm arasında ve/veya ara düğümler arasında iletişim süresince gerçekleşen periyodik bir raporlama sisteminin bu tür bir saldırıyı tespit (ve önleme) açısından etkili olabileceği değerlendirilmektedir.

2.4. Zıt bölgeye yönlendirme

Saldırgan düğüme ulaşan veri paketlerinin hedef düğümün olmadığı bölgeye doğru yönlendirilmesi yoluyla iletişimi engellemeyi amaçlayan ihlal biçimidir. Düğümlerin fiziksel yerleşimleriyle ilgili genel olarak bilgi sahibi olunmasını gerektirir [21]. Ayrıca uyarlamalı yönlendirme kullanan protokollerde yol keşfi aşamasına katılmamış, yani yol isteğine cevap vermemiş düğümlere ulaşan veri paketleri genellikle göz ardı edilmektedir [1]. Ağa yeni katılmış düğümlerin doğrudan iletişime katkı sağlamasının istendiği durumlarda, ilk defa karşılaşılan iletişimler yeni bir yol keşfinin başlamasına sebep olabilir. Böyle bir durumda, bahsi geçen ihlal şekli hem gereksiz kontrol paketi yayınlanmasına hem de iletişimin gereksiz olarak ağı meşgul etmesine sebep olur. Bunun yanında, ara düğümlere ulaşan ilgisiz veri paketleri ağ üzerinde yanlış bir şeylerin olduğunun işaretçisi olarak kullanılıp tedbir alınması için harekete geçilmesini sağlayabilirler.

2.5. Gri delik

Gri delik (grayhole) saldırısı, saldırgan düğümün sadece belirli paketleri göz ardı ettiği diğerlerine ise normal usullerde davrandığı ihlal biçimidir [22]. Örneğin, sadece yönlendirme paketlerini geçirip diğerlerini silmek, ya da belirli hedeflere giden veri paketlerini silmek diğerlerini normal olarak işlemek gibi. Bu saldırı türünün, tespit edilmesi ve kaçınılması en zor saldırı türü olduğu değerlendirilmektedir. Genellikle tespit edilmesi için teknik bilgi kadar -herhangi bir düğümün hedef olması için sebeplerin analiz edilmesi gibi- düşünsel bilginin de kullanılması gerekebilir. Bu durum çoğunlukla ve doğal olarak saldırı tespitinde insan etkileşimine olan ihtiyacı gündeme getirmektedir.

Çalışmamız, IP iletişimi ağ katmanı içerisinde kaldığı için, kullanıcı etkileşimini içeren çözümler kapsam dışında kalmaktadır. Bu yüzden muhtemel saldırı sebeplerini göz ardı ederek, gerçekleşen iletişimin analizi yolu ile saldırının tespit edilmeye çalışılması gerektiği varsayılmıştır.

Saldırgan düğümün davranış şekli, daha çok, ağ üzerinde tutarsız, tamamen rastlantısal iletişim problemleri varmış gibi algılanacak şekilde sonuçlar doğuracaktır.

Birçok yönlendirme protokolü ağ üzerinde herhangi bir problem oluştuğunda mevcut imkanları maksimum seviyede kullanarak problemli bölgenin etrafından dolaşmaya çalışacak şekilde tasarlanmıştır [1,6,12,25]. Ancak bu sürecin çalışabilmesi için genellikle problemin oluştuğu düğümün cevap vermeyi kesmesi ya da problemi bir adım gerisindeki düğüme rapor edebilmesi gerekmektedir.

Bahse konu saldırı biçimlerinde ise iki durum da söz konusu değildir. Bir adım gerideki düğüm açısından iletişim gayet normal olarak devam etmektedir. Saldırgan düğümün bir adım ilerisindeki düğüm açısından ise herhangi bir iletişim olmadığı için her şey normaldir. Bu durumda sadece saldırgan düğüm problemin farkındadır ve onunda bu durumu rapor etmek gibi bir niyeti olmayacağı açıktır. İlk akla gelen iki seçenekten birisi, sonraki düğüm seçiminde rastlantısallığı devreye alarak belirli oranda paketin saldırgan düğüme doğru gitmemesini garanti altına almak olabilir ki, bu durum şans faktörünü ön plana çıkaracağından yeterli olmayacaktır. Diğer seçenek ise, iletişimin "sonraki düğüm" olarak seçilmeyen düğümler tarafından sessizce kontrol edilmesi olabilir. Buna benzer çözümler Kara Delik saldırılarına karşı teklif edilmiştir [2,24].

2.6. En iyi yolu seçmeme

En iyi yolu seçmeme (detour), saldırgan düğümün, kendisine gelen veri paketlerini göndereceği ara düğümü seçerken rapor edilmiş en uygun yolu seçmek yerine daha kötü olduğu rapor edilmiş yolu seçerek, kurallara kısmen uyarken diğer yandan iletişimi kötü yönde etkilemeyi amaçlayan saldırı biçimidir. Genellikle belirli bir bölgedeki ağ kaynaklarının diğer iletişimler tarafından kullanılmasını engellemek ya da hedef aldığı bir düğüme doğru olan iletişimi engellemek amacıyla gerçekleştirilir. Bu saldırı türünün tespit edilebilmesi için saldırgan düğümün yaptığı tercihlerin komşu düğümler tarafından değerlendirilmesinin etkin bir yöntem olabileceği değerlendirilmektedir [26].

Saldırgan düğüm kendisine gelen her veri paketini sonraki düğüme ileteceği için, dışarıdan bakıldığında son derece normal hareket ettiği gözlemlenir. Ancak en kötü yolu seçmesinden dolayı, en iyi ihtimalle gereksiz yeni bir yol keşfinin başlamasına sebep olur ya da en kötü durumda veri paketinin hedefe ulaşamayıp kendisinden sonraki bir noktada kaybedilmesine sebep olur. Bu özelliği nedeniyle de tespit edilmesi oldukça zorlaşmaktadır. Tedbir olarak, yol keşfi aşamasında aynı seviyede bulunan düğümlerin yol isteklerine verilen duyabildikleri cevapları analiz ederek, daha sonra bu düğümler tarafından yapılan duyabildikleri tercihleri verdikleri cevaplara göre değerlendirip derecelendirerek, gerçek problem noktasını tespit edilmesi sağlanabilir. Bu tespit doğru olarak yapılabilirse uygun bir raporlama yöntemiyle çevre düğümler tarafından saldırgan düğüm iletişimden soyutlanabilir.

2.7. Bölümleme

Bölümleme (partitioning), sahte yönlendirme paketleri yayınlamak yoluyla mevcut ağ yapısını parçalara ayırarak belli bir bölgenin diğer düğümlerle iletişimi engellemeye çalışan ihlal biçimidir [13]. Bu saldırı türü genellikle kaynak veya hedef düğüm tarafından yol tayini yapılan yönlendirme protokollerinde etkili olmaktadır. Uyarlamalı yönlendirme protokollerinde etkili olabilmesi için öncelikle yanlış yol isteği cevapları yayınlamak yoluyla yönlendirmeyi kendi üstüne çekmek daha sonra gelen veri paketlerini geri yansıtarak bölümlemeyi gerçekleştirmeye ihtiyaç duyar. Bu durumda dahi uzun süreli etkili olabilmesinin mümkün olmadığı değerlendirilmektedir. Özellikle geri besleme yöntemleri kullanılarak yapılan tercihlerin doğruluğunun sınandığı durumlarda kısa sürede tespit edilebilecek bir saldırı türü olduğu değerlendirilmektedir.

Saldırgan düğüm, yönlendirme protokolü kuralları içinde hareket edeceği varsayımıyla düşünüldüğünde, etkili olmak için özellikle belirli bir gölgeden gelen bütün isteklere çok cazip cevaplar verecektir [23]. Belirli bölgelerden gelen veri paketlerini diğer bölgeye geçirmeyecek şekilde hareket edecektir. Uyarlamalı yönlendirme protokollerinde iletişim üzerinde uzun süre etkili olamayacaktır, çünkü, bu tür protokoller [1] belirli bir düğümde oluşabilecek ani problemlere karşı en hızlı şekilde cevap verecek biçimde tasarlanmıştır. Bu sebepten dolayı söz konusu düğüm hızla iletişim güzergâhının dışına itilerek etkisiz konumda kalacaktır. Eğer protokol kurallarına uymayarak doğrudan paketlerin silinmesi şeklinde hareket edilecek olursa bu durumda da "Sinkhole" sadırı tipine karşı alınması gereken önlemlerin etkili olacağı değerlendirilmektedir.

2.8. Sanal düğüm ekleyerek üzerinden geçen yolu uzun gösterme

Saldırgan düğümün, yol keşfi sırasında sahte düğümler ekleyerek kendi üzerinden geçen yolların gerçekte olduğundan daha uzun görünmelerini sağlamaya çalıştığı saldırı biçimidir. Uyarlamalı yönlendirme protokollerinde yol keşfi sırasında cevap paketlerinin değiştirilmesi yoluyla saldırgan düğümün kendisi üzerinde veri paketi iletilmesini engellemeye çalışması şeklinde uygulanır [25]. Veri iletiminin tamamı üzerinde

büyük bir etkisi olmasa da, ağ kaynaklarının kullanılmasını kısıtladığı için istenmeyen bir durumdur. En ideal durum ağ üzerindeki düğümler tarafından sağlanan imkânların ağ üzerinde gerçekleşen bütün iletişim tarafından etkin şekilde kullanılması olduğu için herhangi bir düğümün buna benzer bir davranış içine girmesi istenmeyen bir durumdur. Yol keşfi aşamasında; İstek ve/veya cevap paketlerinde bulunan sıra numaralarının değiştirilmesi ya da kalite kısıtlı yönlendirme söz konusu kısıt değerinin bilinçi olarak kötü hesaplanması yoluyla aldatıcı bilgi sağlanması, veri iletim aşamasında ise; tamamen normal hareket ederek gizli kalmaya çalışması şeklinde gerçekleşir.

Öncelikle, yönlendirme protokolü istek ve cevap paketlerindeki sıra numaraları gerektiği şekilde gerçekleşmediğinde bu paketleri göz ardı etmek üzere tasarlanmalıdır. Bu sayede sıra numaralarının gerektiğinden farklı atanması o düğümü iletişim güzergahı dışında bırakmaktan başka etki yaratmayacaktır. Saldırgan düğümün devre dışı bırakılması zaten istenen durum olduğundan dolayı bu yöntemle amaca ualaşılacağı değerlendirilmektedir. Yine de bu gibi durumlara karşılık ağ üzerinde "ne kadar verirsen o kadar alırsın" prensibine dayanan bir öncelik mekanizmasının kurulmasının bu gibi saldırılara karşı caydırıcı etkisi olabileceği değerlendirilmektedir.

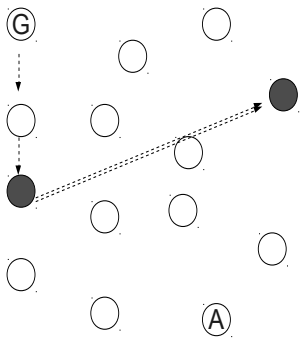
2.9. Diğer düğümleri karalama

Gözlemci düğüme ya da komşu düğümlere belirli bir düğüm hakkında yanlış bilgiler vererek, o düğümün haksız yere saldırgan olarak tanımlanmasına sebep olmaya çalışan saldırı biçimidir. Bu saldırı türü ağ üzerinde bilinen bir saldırı tespit sistemi var olduğunda kullanılabilen bir türdür. Eğer kullanılan saldırı tespit sistemi ağ üzerindeki diğer düğümlerin komşu düğümler hakkında edindiği tecrübelere dayanıyor ise, bu durumda bu saldırı türü tehlikeli olabilmektedir [23]. Bahsi geçen türde saldırı tespit sistemleri kullanan HGA'larda, kötü niyetli düğümlerin, tespit sistemini yanlış yönlendirebilecekleri gerçeği göz önünde bulundurulmadır. Bu tür hareketler aslında bir yönlendirme protokolü ihlali değildir. Saldırı tespit sistemlerinin kendisinin ihlal edilmesidir. Ancak eğer söz konusu olan yönlendirme protokollerinin ihlallere karşı korunması ise, geliştirilen yönteme karşı uygulanabilecek saldırıların da göz önünde bulundurulması gerekir. Bu ihlal türü bu amaçla inceleme kapsamına alınmıştır. Az düğüm tarafından sağlanan raporların güvenirliliğinin düşük kabul edilmesinin gerekliliğini göz önüne çıkarmaktadır.

2.10. Solucan deliği

Solucan deliği (wormhole), birbirinden uzakta konuşlanmış iki saldırgan düğümün aralarında oluşturdukları özel bir iletişim yolu ile (VPN benzeri) birine gelen veri paketlerinin doğrudan diğerine aktarılması yoluyla yönlendirmenin bozulmaya çalışıldığı saldırı biçimidir (Şekil 2) [19]. Ağ üzerindeki diğer düğümler tarafından iki normal düğüm arasındaki normal bir iletişim olarak algılanacağı için tespit edilmesi oldukça zor bir saldırı türüdür. Ancak iki ayrı konumdaki iki ayrı düğüm tarafından kendine özgü kuralları olan bir iletişim gerektirdiğinden gerçekleştirilmesi de aynı oranda güç olan bir saldırı biçimi olduğu değerlendirilmektedir. Ayrıca, ilk saldırgan düğümün komşuları açısından incelendiğinde kara delik saldırılarına çok benzer şekilde iletilen paketlerin aktarılmadığına yönelik belirtiler vereceği için, aynı grup içinde ele alınmalarının uygun olacağı değerlendirilmektedir. Yönlendirme istek ve/veya cevap paketlerinin de solucan deliği üzerinden aktarılması durumunda uyarlamalı yönlendirme kullanan protokoller çok uzak noktalarda düşük sıra numaralı istek paketlerinin yayınlanmasına sebep olabilir. Bu durum çok sayıda gereksiz istek ve cevap paketinin ağ içerisinde tekrarlanarak yayınlanması anlamına gelecektir.

Solucan deliği üzerinden aktarılan veri paketleri ilk düğüm üzerinde kaybolmuş gibi algılanacaktır. Yol keşfi aşamasında istek ve cevap paketleri aktarılmaz ise, veri paketleri B noktasına komşu düğümler tarafından yabancı trafik olarak algılanıp göz ardı edilerek silinecektir. Bu durum aslında "kara delik" saldırılarına benzemektedir [11]. "Kara Delik" saldırılarına yönelik alınan önlemlerin büyük ölçüde bu tür saldırılara karşı da etkili olacağı, ayrıca, çevre düğümler tarafından gözleme dayalı saldırı tespit sistemleri "solucan deliği" iletişimini tespit edebilecek şekilde tasarlanabileceği değerlendirilmektedir.



Şekil 2: Solucan deliği saldırısı.

2.11. Telaş saldırıları

Sadece ilk gelen yönlendirme isteğine cevap verilen ve diğerlerinin dikkate alınmadığı protokollerde, herhangi bir ara işlem yapmadan gelen istek paketlerini hızla yayınlayarak diğer düğümlerin başkasından gelen istekleri göz ardı etmelerini sağlamaya çalışan saldırı biçimidir 2.11. (hızlı "RREQ" yayını). Başarılı olduğu taktirde bütün trafiği kendi üzerine toplamış olacağından, diğer saldırı türlerine geçiş aşamasında kullanılabilir [25]. Ayrıca, bütün isteklere karşılanma

durumunu incelemeden olumlu cevap verdiği için, ilave işlem yapmasa da iletişimi olumsuz yönde etkileyeceği çok açıktır. Bu sebeple istek ve cevap mekanizmasının ve yol seçimi işleminin bu tür saldırıları bertaraf edecek şekilde ele alınması zorunluluk haline gelmektedir. Basit olarak ilk gelen cevaba işlem yapılsa bile gelen diğer cevapların kaydedilerek alternatif durumlarda kullanılmasını sağlamak şeklinde tedbir alınabilir. Doğrudan hedefmiş ya da hedefe komşuymuş gibi hızlı cevaplar.

Doğrudan komşu olan düğümlere başlatılan iletişimlerde yol keşfinin kullanılmaması bu gibi saldırıların komşu düğümler tarafından etkili olmasının önüne geçilmesi açısından önemli olduğu değerlendirilmektedir. Ancak, ilk kuşak komşulardan uzakta olan saldırganlar için ilave tedbirlerin alınmasının gerekliliği aşikârdır. Bu yüzden, verilen cevapların tutarlılığının diğer komşu düğümler tarafından da değerlendirildiği, çoğul katılımlı bir yol keşfi tasarım çalışmasının gerekli olabileceği değerlendirilmektedir. Ayrıca, sahte cazip cevap paketleri kaynak düğüm tarafından iletişimin hemen başlatılmasına ve saldırgan düğüm tarafından paketlerin göz ardı edilerek iletişimin engellenmesine sebep verebilir. Bu açıdan yaklaşıldığında kara delik saldırıları ile büyük benzerlik göstermektedir.

2.12. Denizanası saldırıları

Kara delik saldırılarında olduğu gibi, saldırgan düğümün gelen veri paketlerini değişken şekilde gereğinden fazla bekleterek göndermesi yoluyla uçtan uca veri iletim süresini uzatmayı amaçlayan saldırı biçimidir. Özellikle TUQR [1] benzeri kalite kısıtlı yönlendirme (KKY) kullanan protokoller üzerinde ciddi etkileri olabilecek türden saldırılardır. Yol keşfi ve yol bakımı aşamalarında tamamen kuralla uygun davranırken, veri paketlerinin iletimi aşamasında kendisine ulaşan veri paketlerini -örneğin kuyruklama algoritmasını değiştirmek yoluyla- gerekenden uzun süre bekletip daha sonra yönlendirerek paket iletimini geciktirmeyi amaçlarlar. Başarılı olduklarında, özellikle çoklu ortam uygulamalarının aksamasına sebebiyet verirler. Ağ üzerinde oluşacak sorunları taklit eder şekilde davrandıkları için tespit edilmeleri oldukça zor ancak aynı zamanda ağ sorunlarına verilene tepkilere maruz kalacakları için bertaraf edilmeleri de aynı oranda kolay olabilecek saldırılar oldukları değerlendirilmektedir [26].

Bu tür saldırıları tespit etmek ve karşı koymak için yapılabilecek en pratik çözüm, yine, çok noktalı harici kontrole dayanan derecelendirme sistemi ile bu tür düğümlerin kuyruk algoritmalarını algılamaya çalışarak karar verecek bir sistem geliştirmek olarak değerlendirilmektedir.

2.13. Kaynakları tüketen saldırılar

Normalden fazla sayıda kontrol paketleri yayınlamak ya da rastgele hedef düğümlere veri paketleri göndermeye çalışarak ağ üzerindeki düğümlerin kontrol paketleri yayınlanmasına sebep olmak yoluyla ağ üzerindeki kontrol paket iletişimini arttırarak normal iletişimin engellenmesine çalışan saldırı biçimidir. Uyarlamalı protokollerin aynı hedefe ulaşmaya çalışan iletişime ilerleyen aşamalarda bütün ağı meşgul etmeden cevap geliştirebileceği düşünüldüğünde bu tür protokollere karşı fazla etkili olamayacak bir saldırı türü olduğu, ancak yönlendirme tablolarında gereksiz yere büyüme yaratacağı için yine de olumsuz etkilerinin olacağı değerlendirilmektedir [21].

Bu tür saldırıların uyarlamalı yönlendirme protokollerini etkileyebilmesi için saldırgan düğümün belirli bir düğüme sürekli olarak iletişim kurması gerekmektedir. Aksi halde, veri iletimi olmadan yol keşfi yapmaya çalışması ilk seferinde etkili olsa da daha sonraki denemelerde yönlendirme tabloları üzerinden cevap verileceği için etkili olamayacaktır. Ancak başka bir düğümle eş güdümlü olarak düzenlenen saldırılarda iletişimin içeriğinin incelenmesi mümkün olamayacağı için çözüm bulunması oldukça zordur. Bu sebeple alınabilecek en mantıklı tedbir olarak ağ kaynaklarına kota uygulanması düşünülebilir. Şöyle ki; herhangi bir düğüm ilk kuşak komşularından uzaktaki herhangi bir düğümle iletişim için belirli bir süre içinde belirli bir oranda bant genişliği veya iletişim zamanı kullanabilir. Belirlenen eşik değer aşıldığında ya iletişim durdurulur ya da tahsis edilen kaynaklar en aza indirilerek (örn: kuyruk önceliği düşürülerek) muhtemel bir saldırının etkili olma oranı düşürülebilir.

3. İhlal Modelleri

Önceki bölümde analiz edilen ihlal türleri sonuçları açısından incelenerek, saldırgan düğümlerin yönlendirme protokollerinin hangi aşamalarında ne tür ihlaller gerçekleştirerek iletişimi ne şekilde etkiledikleri tespit edilmeye çalışılmıştır. İnceleme sonuçları Tablo 1'de özetlenmiştir.

Buna göre, yönlendirme protokolü ihlallerinin doğurduğu sonuçların algılanmasına ve bu sonuçların düzeltilmesine yönelik tedbirler alınmasının zaman içerisinde geliştirilecek yeni ihlal şekillerinin tespit edilmesine ve önlenmesinde de etkili olabileceği değerlendirilmektedir.

Tablo 1: İhlal şekilleri sınıflandırması

Yönlendirme Aşaması	İhlal Şekli	Sonuçları
Yol keşfi	Hızlı, doğru olmayan cevaplar	İletişimin aksaması ve gereksiz ilave yol keşfi faaliyetleri
	İstek ve/veya cevap paketinin iletilmemesi	İletişimin engellenmesi, kaynakların etkin kullanılamamas ı
Veri Paketi İletimi	İlgisiz rastgele veri paketleri gönderimi	Gereksiz yere tetiklenen yol keşfine yönelik kontrol paketi yayılımı
	Veri paketlerinin yanlış yöne iletilmesi	
	Veri paketlerinin düzenli veya düzensiz şekilde silinmesi	İletişimin kesilmesi, geri raporlanamaya n iletişim sorunları
Yol keşfi / Veri Paketi İletimi	Belirli bir iletişime özel olarak ilgili paketlerin düzenli veya düzensiz şekilde silinmesi	Hedefte bulunan iletişimin aksaması veya tamamen engellenmesi

Problem bu açıdan incelendiğinde, yol keşfi aşamasında saldırgan düğümlerin kullanabilecekleri iki ihlal şekli tespit edilebilmiştir. Birincisi doğru olmayan cevapları normal düğümlere göre çok hızlı oluşturmaları ve yayınlamaları, diğer ise belirli bir tip ya da bütün kontrol paketlerini hiç iletmemek biçiminde gerçekleşmektedir. Bir diğer aşama olan veri iletimi aşaması ise en etkili saldırıların gerçekleştiği aşamadır. Bu aşamada, saldırgan düğümlerin gerçekleştirdikleri ihlaller sonucunda ortaya çıkan temel durum veri paketinin olması gereken yol üzerinden seyahat etmemesidir. Bu aşamada gerçekleştirilen saldırılar genellikle ağ üzerindeki iletişim problemleriyle benzer belirtiler oluşturur. Oluşan durum iletişim problemlerinden ayırt edilebilmelidir. Bunların dışında bazı saldırı türlerinin iki aşamayı da birlikte kullanarak hareketlerindeki tutarsızlıkları gizlemeyi başarabilmektedir. Bu nedenle, ağ üzerinde yönlendirme faaliyetlerinin topyekûn ele alınarak değerlendirilmesi gerekmektedir.

4. Savunma Modelleri

Önceki bölümde analiz edilen saldırı yöntemlerinin ortak noktalarının incelenmesi sonucunda yönlendirme protokollerinde uygulanabilecek ihlallerin büyük çoğunluğunun engellenmesi için alınması gereken önlemlerin beş ana gruba ayrılabileceği değerlendirilmiştir. Buna göre;

4.1. İlgisiz veri paketi engelleme sistemi

Bölüm 2.1, 2.4, ve 2.10'da incelenen ihlal türlerinde karşılaşıldığı gibi, yol keşfi ve yol seçimi aşamalarından geçmemiş bağlantılara ait veri paketleri ile olumsuz şekilde sistemin etkilenmeye çalışan saldırılara karşı direnç gösterebilmek için bahsi geçen türde bir veri paketi alan düğüm bu durumu hemen bir kontrol paketi yardımıyla diğer düğümlere rapor etmelidir.

Bunu yapabilmek için yol keşfi aşamasında tekrarlı gelen yol istek paketlerini göz ardı etmeden önce gönderen düğüm bilgisini kaydederek, ileride kendisine ulaşan veri paketlerine ilişkin yol keşfine katılmamış olan düğümleri ayırt etmekte kullanabilir.

4.2. Sınırlandırılmış paket takip sistemi

Özellikle uyarlamalı yönlendirme protokolleri, HGA üzerinde oluşabilecek yerleşim değişimleri ve iletişim problemlerinin ortaya çıkardığı sorunlara karşı direnebilmek ve iletişimin devamlılığını sağlayabilmek için bu gibi durumları yol üzerinde geriye doğru raporlayarak düzeltici işlem uygulama prensibini göre tasarlanmışlardır. Kalite kısıtlı iletişimde, paketlerin yeniden gönderimini engellemek ve mümkün olduğunda diğer imkânları kullanarak ilgili paketi hedef düğüme ulaştırabilmek önemlidir. Herhangi bir ağ sorunu olmadığı halde veri paketlerinin kaybedilmesine yol açan yönlendirme ihlallerinin karşısında daha hassastırlar.

İster kalite kısıtlı olsun ister olmasın iletişimin daha etkin yapılabilmesi için, HGA üzerinde tasarlanmış yönlendirme protokollerinin bir düğümden diğerine iletilen veri paketinin hedefe ulaşana dek yol üzerindeki üçüncü bir düğüme iletildiğinden emin olmasını sağlayacak bir sisteme ihtiyaç duyar.

Kablosuz iletişimin doğası gereği bir düğüm alıcı menzili içerisindeki düğümlerin iletişimlerini dinleyebilir. Bu özellik kullanılarak bir düğüm aktarmış olduğu veri paketinin yol üzerindeki düğüm tarafından aktarılıp aktarılmadığını, hangi düğüme ve ne kadar süre sonra iletildiğini tespit edebilir. Bu bilgi sayesinde aktardığı veri paketinin akıbeti ve sonraki düğüm olarak

seçtiği komşusunun davranış özellikleri hakkında bilgi edinebilir. Bu bilgi Bölüm 4.5'de açıklanacak olan raporlama sistemine benzer bir sistem yardımıyla söz konusu düğümün komşularına aktarılabilir. Bu sayede istenmeyen şekilde davranış gösteren düğümler hızla ağ üzerindeki iletişim ortamından soyutlanarak olumsuz etkilerinden azaltılabilir.

Normal ağ protokollerinde, üst katmanlara ya da diğer düğümlere iletilmek üzere düğümün kendisine yönelmemiş paketlerle ilgili herhangi bir bilgi yönlendirme katmanına ulaşmayacaktır. Bu nedenle, bu sistemin uygulanabilmesi için, yönlendirme protokollerinin çalıştığı ağ katmanından daha alt katmanları da içerisine alan bir çalışma yapılmasının gerektiği değerlendirilmektedir.

4.3. Çapraz kontrol sistemi

Yukarıda bahsi geçen, sınırlandırılmış paket takip sistemine benzer özellikler taşısa da, Çapraz Kontrol Sisteminin daha geniş kapsamlı bir görev alanı bulunmaktadır. Temel hedef, yol keşfi ve seçimi aşamasında, yol üzerinde hedefe kendisinden daha yakın olan düğümlerin verdikleri cevapları kaydederek, daha sonra iletişimin gerçekleştiği esnada bütün iletişimlere ait hareket modellerini takip edip, normal dışı ve şüpheli görünen davranışların rapor edilmesidir.

Bu yaklaşıma benzer şekilde önerilmiş sistemler bulunmaktadır. Temel dezavantajı, bütün iletişimi takip etmeye çalışacağından dolayı işlem gücü ve bellek ihtiyacının yanında güç tüketimini de diğer çözümlere nazaran arttıracak olmasıdır.

4.4. Uyarlamalı yük dengeleme protokolü

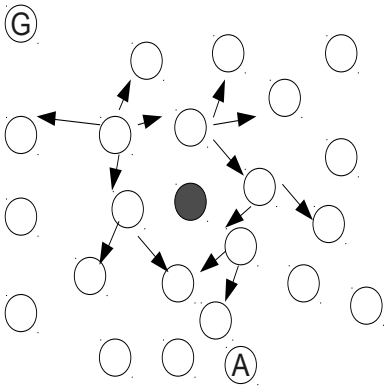
HGA kapsamındaki kaynakların tüketilmesine ya da iletişimin engellenmesine yönelik olarak, protokol kurallarına tamamen uygun davranırken yoğun bir şekilde paket ileten saldırılara karşı düğümler üzerindeki kuyruk algoritmasının uyarlamalı bir şekilde yeniden düzenlenmesi yoluyla iletişim kısıtlamasına gidilebileceği değerlendirilmektedir. Bu uygulama aynı zamanda ağ üzerindeki kaynakların adil dağılımını sağlama görevini de yerine getirebilir. Kalite kısıtlı yönlendirmenin kullanıldığı ortamlarda yük dengelemesi yaparken kalite kısıtına ilişkin düzenlemelerin göz önünde bulundurulmasına ihtiyaç vardır.

Her normal işleyen düğüm üzerinde, kendi üzerinden geçen veri paketlerinin iletişim bazında yoğunluğu hesaplanarak belirli bir eşik değer üzerine çıkan iletişimler için önceliğin düşürülmesi şeklinde tasarlanmıştır. Bu tasarım ağ üzerindeki sıkışmalara tepki veren diğer çözümlerle birleştiğinde, mevcut kaynaklarla mümkün olan en etkin iletişimin sağlandığı bir ortamın oluşturulmasına büyük katkı sağlayacaktır.

4.5. Kısıtlı yayılımlı iletişim raporlama sistemi

HGA üzerinde yönlendirme protokollerinin tasarlanmasında en kritik bilgi, iletilen veri paketinin sonraki düğüm tarafından başka bir düğüme doğru şekilde iletilip iletilmediği bilgisidir. Bu bilginin sağlanması birçok ihlal davranışını sonuçları açısında açığa çıkaracak ve doğru tasarlanmış bir tepki sistemi ile etkin şekilde bertaraf edilmesinin yolunu açacaktır.

Her ara düğüm, süre gelen iletişim içerisinde, belirli aralıklarla veya herhangi bir tetikleme mekanizmasının harekete geçirmesi sonucunda iletişimde bulunduğu komşu düğümleri hakkında o düğümü çevreleyen komşuları aracılığıyla bilgi toplaması prensibine dayanır. Bu sistemin belirli aralıklarla tekrarlanmak üzere tasarlanmasının ağ iletişimindeki problemlere karşı da ilave hassasiyet geliştirilmesi açısından uygun olacağı değerlendirilmektedir.



Şekil 3: Kısıtlı yayılım gösterimi

Tasarlanmaya çalışılan bu tip raporlama sistemlerinin temel problemi, yayınlan raporlamanın ilgisiz düğümler tarafından alınması ve ayrıca gerektiğinden fazla yayılmasından dolayı ağ üzerinde kontrol paketi yükünü arttırmasıdır. Bu problemin aşılabilmesi için, sorgulamada kullanılacak olan kontrol paketlerinin sadece hedefteki düğümü sarmalayan komşu düğümleri arasında yayılmasını sağlayacak bir sistem tasarlanmalıdır [27].

Bu sistem, kontrol paketlerine konulacak bir sayacın paketin iletildiği düğümler tarafından eksiltilmesi ile sağlanabilir. Sadece sıfırdan büyük sayaç değerine sahip olan paketlerin iletildiği bir ortamda örneğin başlangıç değeri 3 olan bir sayaç sayesinde, raporlama ve sorgu paketlerinin sadece istenilen bölgede yayılması sağlanmış olacaktır (Şekil 3). Özellikle düğüm sayısının oldukça fazla ve düğümlerin iletişim menzillerinin düşük olduğu ortamlarda, diğer iletişimlerin etkilenmesini engellemek açısından etkili olacağı değerlendirilmektedir.

5. Sonuç

HGA üzerinde yönlendirme protokollerinin temel problemlerinden birisi olan ihlallerin incelenmesi ve sınıflandırılması, genel anlamda ihlallerin anlaşılması ve etkin çözümler geliştirilebilmesi için gereklidir. Bu amaçla, bu çalışma kapsamında, bugüne dek çalışılmış ve incelenmiş olan ihlal türlerinden öne çıkanlar detaylı şekilde analiz edilmiştir.

Gerçekleştirilen analiz çalışmasının ardından, incelenen saldırı yöntemlerinin doğurduğu sonuçlar sınıflandırılmaya çalışılmış, elde edilen sınıflandırma sonrası saldırıların ortak olarak etkiledikleri protokol işlev ve aşamaları tespit edilmiş, bu aşamalarda söz konusu sonuçların oluştuğunu tespit edip düzeltici işlem yapmaya yönelik prensipler ortaya konulmuştur.

Belirlenen prensipleri yansıtacak şekilde 5 ayrı savunma modeli tasarlanmıştır. Bu modeller yardımıyla literatürde yaygın olarak çalışılan saldırı türlerinin ve ihlal şekillerinin tespit edilip önlenebileceği öngörülmektedir.

Bu çalışmada elde edilen savunma modelleri sonraki aşamalarda, belirgin protokollere savunma sistemleri tasarlayabilmek için kullanılması amaçlanmıştır.

6. Kaynakça

[1] Zagli, I. ve Song, M., ``TUQR: A Topology Unaware QoS Routing Protocol for MANETs", Proceedings of the 5th WSEAS International Conference on Telecommunications and Informatics, Istanbul, Turkey, May 27-29, 2006 (pp 207-212) .

[2] Badis, H. ve Al Agha, K. 2004 “An efficient QOLSR extension protocol for QoS in ad hoc networks”, Vehicular Technology Conference, 2004, (pp2650 – 2653).

[3] K.-C. Wang ve P. Ramanathan 2003 “End-to-end delay assurances in multi-hop wireless local area networks”, in Proc. IEEE GLOBECOM, 2962–2966.

[4] Jiang S., He D. ve Rao J., “A Prediction-Based Link Availability Estimation for Routing Metrics in MANETs” IEEE/ACM Transactions on Networking, Vol. 13, No. 6, 2005 , (pp1302 - 1312)

[5] Lian J., Li L. ve Zhu X., “A Multi-Constraint QoS Routing Protocol with Route-Request Selection Based on Mobile Predicting in MANET ” International Conference on Computational Intelligence and Security Workshops , 2007, (pp342 – 345).

[6] Walrand J., “Implementation of QoS Routing for Manets ”, SmartNets report, 2007.

[7] Schweitzer C. M., Carvalho T. C. ve Ruggiero W., “A Distributed Mechanism for Trust Propagation and Consolidation in Ad Hoc Networks ”, ICOIN 2006, (pp156 – 165).

[8] E. M. Royer and C. K. Toh, “A review of current routing protocols for ad hoc mobile wireless networks”, IEEE Personal Communications Magazine, vol. 6, no. 2, 1999, (pp. 46–55).

[9] Yang H., Shu J., Meng X. ve Lu S., “SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks ”, IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, 2006 , (pp261 – 273).

[10] Buchegger S., Boudec J.Y.L., “Self-Policing Mobile Ad Hoc Networks by Reputation Systems ”, IEEE Communications Magazine , 2005, (pp101 – 107).

[11] Luo J., Fan M., Ye D., “Black Hole Attack Prevention Based on Authentication Mechanism”, IEEE ICCS, 2008, (pp173 – 177).

[12] Kamhoua C.A., Pissinou N., Miller J. ve Makki S.K., “Mitigating Routing Misbehavior in Multi-hop Networks Using Evolutionary Game Theory ”, IEEE Globecom 2010 Workshop on Advances in Communications and Networks , 2010, (pp1957 – 1962).

[13] Nath R., Sehgal P. K., Sethi A. K., “Effect of Routing Misbehavior in Mobile Ad Hoc Network ”, IEEE 2nd International Advance Computing Conference , 2010, (pp218 – 222).

[14] Boodnah J., Poslad S., “A Trust Framework for Peer-to-Peer Interaction in Ad Hoc Networks ”, Computation World , 2009, (pp707 – 712).

[15] Liu Z., Joy A. W. ve Thompson R. A. , “A Dynamic Trust Model for Mobile Ad Hoc Networks ”, Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS’04), 2004.

[16] Karri G.R., Khilar P.M., “Routing Misbehavior Detection and Reaction in MANETs ”, 5th International Conference on Industrial and Information Systems, ICIIS 2010 , (pp80 – 85).

[17] Newsome J., Shi E., Song D. ve Perrig A., “The Sybil Attack in Sensor Networks: Analysis & Defenses ”, PSN’04, 2004 .

[18] Hu Y., Perrig A. ve Johnson D. B., “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols”, WiSe 2003.

[19] Hu Y., Perrig A. ve Johnson D. B., “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks ”, Rice University Department of Computer Science Technical Report TR01-384 , 2002.

[20] Zhang X.Y., Sekiya Y. ve Wakahara Y., “Proposal of a Method to Detect Black Hole Attack in MANET ”, ISADS '09 International Symposium on Autonomous Decentralized Systems, 2009, (pp1-6).

[21] Hu Y.C., Perrig A., Johnson D.B., “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks ”, Journal Wireless Networks archive Volume 11 Issue 1-2, 2005, (pp21 – 38).

[22] Ngai E.C.H., Liu J. ve Lyu M.R., “On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks ”, IEEE ICC, 2006 , (pp3383 – 3389).

[23] Sharma S. ve Singh M., “Defending Wireless Ad Hoc Network from Single and Cooperative Black Holes ”, First International Conference on Emerging Trends in Engineering and Technology , 2008, (pp134 – 139).

[24] Umuhoza D., Agbinya J.I. ve Omlin C.W., “Estimation of Trust Metrics for MANET Using QoS Parameter and Source Routing Algorithms ”, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications , 2007, (pp80 – 85).

[25] Nguyen H.L. ve Nguyen U.Y., “Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks ”, Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL’06) , 2006, pp(149 – 154).

[26] Aad I., Hubaux J.P., ve Knightly E.W., “Denial of Service Resilience in Ad Hoc Networks ”, ACM Mobicom, 2004.

[27] Dokuker S., Erten Y.M., Acar C.E., “Performance analysis of ad-hoc networks under black hole attacks ”, SoutheastCon, 2007. Proceedings. IEEE, (pp148 – 153).

[28] Tamilselvan T., Sankaranarayanan V., “”Prevention of Blackhole Attack in MANET ”, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) , 2007, (pp21 – 26).

SNMPv3 İLE GÜVENLİ AĞ TOPOLOJİ KEŞFİ

Musa BALTA[1] **İbrahim ÖZÇELİK**[2]

[1,2] Bilgisayar Mühendisliği Bölümü

Bilgisayar ve Bilişim Bilimleri Fakültesi

Sakarya Üniversitesi Esentepe Kampüsü 54187 Serdivan / SAKARYA

[1]e-posta: mbalta@sakarya.edu.tr [2]e-posta: ozcelik@sakarya.edu.tr

Anahtar kelimeler: Topoloji Keşfi, Snmpv3

ABSTRACT

This paper's aim is to discover an enterprise network which is created in a virtual enviroment with SNMPv3. An algorithm that is used previously in academic researchs, is redesigned for our topology according to security criterias. Thus, data can collected securely from SNMP devices in network without any data theft.

1.Giriş

Günümüzde kurumsal ağlar, gerek artan kullanıcı sayıları gerekse üzerlerinde çalışan uygulamaların fazlalığı yüzünden daha kompleks ve daha büyük yapılar haline gelmiştirler [1-4]. Büyüyen bu kurumsal ağlardan daha efektif ve verimli bir şekilde yararlanabilmek için en üst düzeyde yönetim ve bakım anlamına gelen ağ yönetim kavramı ortaya çıkmıştır. Ağ yönetimi sistemleri kendi içlerinde güvenlik, topoloji çıkartma, izleme, kontrol, koordinasyon ve planlama gibi birçok özellik barındırırlar. Bu özelliklerin efektif ve verimli bir şekilde kullanılabilmesi için öncelikle kurumsal ağın topoloji keşfinin ve cihazlar arasındaki bağlantıların iyi tespit edilmesi gerekir ki oluşturulacak olan ağ yönetim sistemi, yapılan bu topoloji keşfinin sonuçlarına göre en iyi şekilde tasarlanabilir.

Ağ topolojisi keşfi alanında kullanılan bir çok teknik vardır ve bu alanda bir çok akademik çalışma yapılmıştır. Ağ topolojisi keşfetmede ping, trace-route, DNS (Domain Name System-Alan Adı Sistemi) ve SNMP (Simple Network Management Protocol-Basit Ağ Yönetim Protokolü) gibi birçok teknik vardır [1-4]. Fakat bunlardan sadece SNMP diğerlerine oranla daha iyi ağ performansı sağlar ve sahadaki cihazların kendi aralarındaki bağlantılardan, cihaz tipine kadar tüm ağ bilgisini güvenli ve eksiksiz bir şekilde çekebilir.

Bu bildiride, SNMP' nin güvenlik versiyonu olan SNMPv3 kullanılarak oluşturulan algoritma sayesinde, sanal ortam üzerinde modellenen kurumsal bir ağ alt yapısının topoloji keşfi yapılacaktır. Önerilen algoritma sanal ortam üzerinde çalışacağı için gerçek ortamdan daha kısa sürede icra edilecektir.

2.SNMP (Basit Ağ Yönetim Protokolü)

SNMP, bir çok ağın yönetilmesinde kullanılan basit bir ağ yönetim protokolüdür. Genel itibariyle SNMP 3 yapıdan oluşur; ajan yazılımı (agent), SNMP-sunucusu (SNMP-server) ve bir de SNMP motorunun olduğu ağ yönetim sistemidir. SNMP'nin çalışma mekanizması istek gönderme ve isteğe cevap alma şeklindedir ve bunun için taşıma katmanında UDP protokolünü kullanır [5]. SNMP sayesinde bir cihazdan bilgi alınabileceği gibi, cihazdaki bilgi değiştirilebilir ve cihaza yeni bir yapılandırma uygulanabilir. Örneğin cihaz baştan başlatılabilir, cihaza bir yapılandırma dosyası gönderilebilir ya da cihazdan alınabilir.

SNMP cihazdan veri çekeceği zaman daha önceden tanımlanmış olan bazı değerleri kullanarak bu işlemi gerçekleştirir. Bu değerlere yönetim bilgi tabanı (MIB, Management Information Base) değerleri denir ve rakamlarla ifade edilir. Örneğin 1.3.6.1.2.1.1.5.0 değişkeni cihazın sistem adına denk gelmektedir [6,7].Bu yönetim bilgi tabanı değerlerinde ulaşılmak istenen değeri tutan

değişkenlere ise de nesne tanımlayıcısı (OID, Object Identifier) denir. Yönetim bilgi tabanı ve nesne tanımlayıcıların değerleri [8] nolu kaynaklarda bulunmaktadır.

SNMP, ağ güvenliğini sağlarken bazı kriterler kullanır. Bunlardan en önemlileri [8] :

- Kimlik doğrulama: Veri bütünlüğünü sağlar ve verinin kaynağını doğrular.
- Topluluk ismi: Yönetilen cihazlar ve SNMP arasında mesaj iletimi esnasında kullanılan doğrulama parametresidir.
- Şifreleme: SNMP paketlerini şifreler.
- Gizlilik: Ağdaki SNMP paketlerinin içeriğinin gizli tutulması.
- Güvenlik seviyesi: Her SNMP paketi üzerinde kullanılan şifreleme algoritmalarıdır. HMAC MD5, AES veya SHA kullanılır.
- Veri bütünlüğü: Bir mesaj paketi içinde parçalara bölünmemiş veri durumudur.
- SNMP kullanıcısı: SNMP yönetici işlemlerini yapan kullanıcıdır. Ağ yönetim sisteminden gelen SNMP mesajlarına göre ağın durumuyla ilgili değişiklik yapabilir.
- Güvenlik modeli: SNMP ajanı tarafından kullanılan güvenlik stratejisidir. Üç tanedir: SNMPv1, SNMPv2c, SNMPv3.

Bu güvenlik kriterlerini tüm SNMP versiyonları desteklemez. SNMP versiyonlarının güvenlik bazlı karşılaştırmalı tablosu aşağıda verilmiştir.

Tablo 1: SNMP güvenlik modelleri ve seviyeleri [8]

Model	Seviye	Kimlik Doğrulama	Şifreleme
v1	noAuthNo Priv	Topluluk ismi	Yok
v2c	noAuthNo Priv	Topluluk ismi	Yok
v3	noAuthNo Priv	Kullanıcı adı	Yok
v3	authNoPriv	MD5,veya SHA	Yok
v3	authPriv	MD5, veya SHA	DES

SNMPv3, yukarıdaki tabloda görülebileceği gibi güvenlik düzeylerinin hepsini destekleyebildiği için verilerin iletimi esnasında kullanılan şifreleme algoritmaları ile SNMP sorgularının daha güvenli bir şekilde kullanılmasını sağlamaktadır. Böylelikle SNMP paketleri de şifrelenmiş şekilde gideceği için ağ güvenliği sağlanmış olacaktır.

3.Ağ topolojisi keşfi uygulaması

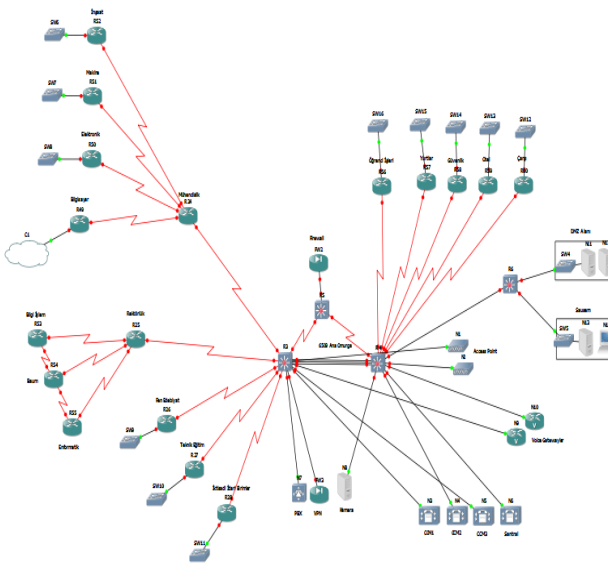
Ağ topoloji keşfi, birçok akademik çalışmaya konu olan geniş ve kapsamlı bir alandır [1-4]. Piyasada gerek ticari gerekse akademik birçok ağ topoloji keşfi yapan uygulamalar mevcuttur [9-10]. Yapılan bu çalışmaların çoğu gerçek ortamlar üzerinde yapılmaktadır. Uygulamamızda ana referans alınan çalışma [1] numaralı çalışmadır. Bu çalışmada da gerçek ortamda SNMPv2c ile sorgulama yapılarak topoloji keşfi yapılmaktadır. Bizim çalışmamızda ise kurumsal bir ağın topolojisi sanal ortamda oluşturularak güvenli bir ortam sunan SNMPv3 ile topoloji keşfi gerçeklenecektir.

Bu amaçla bir sonraki bölümde ilk önce modelleme ortamı ile alakalı bilgi, daha sonrasında ise topoloji keşfinde kullanılacak algoritma hakkında bilgi verilecektir.

3.1 Modelleme ortamı

Ağ topolojisinin modellenebilmesi için bir ağ modelleme simülatörü olan GNS3 (Graphical Network Simulator) programı kullanılmıştır. Cisco cihazlarını birebir gerçekleyebilen bir simülatör olduğu için GNS3 seçilmiştir [11]. Uygulama kodunun çalıştırılabilmesi için de VMWARE Workstation sanallaştırma programı üzerinde sanal makine oluşturulup gerekli bağlantılar yapılarak topolojiye ilave edilmiştir [12].

Sanal ortam üzerinde oluşturulan ağ yapısı (Şekil 1), 2 adet ana omurga Cisco 6509 anahtar cihazı etrafında modellenmektedir. Bunlardan birine, bir kurumsal ağın dış servislerini kurum dışı bir ağa (özellikle internete) açan ve ek bir güvenlik katmanı gibi çalışan sivil bölge (DMZ, Demilitarized Zone) alanı, kurum içi ve kurum dışı ağlara güvenli bir şekilde bağlanabilmeyi sağlayan sistem olan sanal özel ağ (VPN, Virtual Private Network) sunucuları, kurum içi iletişimi sağlayan çağrı yöneticileri (call manager) ve erişim noktaları (access point) bağlanmakta, diğer omurga anahtar cihazına ise kurumsal ağın akademik ve idari birimleri bağlanmaktadır.



Şekil 1: Örnek kurumsal bir ağ yapısı

GNS3 programında gerekli konfigürasyonlar (SNMP aktivasyonu, yönlendirici konfigürasyonları, Vlan (Virtual Local Area Network-Sanal Yerel Alan Ağı) konfigürasyonları, vb.) yapıldıktan sonra kurumsal bir ağ yapısının modellenmesi tamamlanır. Uygulama kodunun ve algoritmanın çalışacağı kısım ise VMWARE Workstation programında oluşturulmuş ve Şekil 1'de verilen topolojiye bulut olarak eklenmiştir.

3.2 Önerilen Algoritma

Önerilen bu algoritma, oluşturulan topoloji üzerindeki cihaz tiplerinden, cihazlar arasındaki bağlantıya kadar birçok konuyu ele almaktadır.

Algoritmayı yürütmeye başlamadan önce ağdaki tüm cihazların SNMP konfigürasyonlarının yapılması gerekir. Verilerin güvenli bir şekilde cihazdan okunabilmesi için SNMPv3 kullanılır. Cihaz üzerinde SNMPv3 aktif edilirken aşağıdaki sıra izlenir [5,8]:

- Grup oluşturulur: Tablo 1'deki güvenlik modeli (v3) ve güvenlik düzeyi seçilir. Aşağıdaki komut satırında aynı bölgedeki cihazlar için grup1 isimli grup oluşturmuş olup, güvenlik düzeyi v3 seçilerek bu gruba sadece "read" özelliği atanmıştır.

  snmp-server group grup1 v3 priv read grup1_oku

- Kullanıcı oluşturulur: Gruba eklenecek kullanıcılar güvenlik esaslarına göre oluşturulur. Burada oluşturulan güvenlik kriterleri için kullanıcı doğrulaması için "md5" algoritması, şifreleme için ise de "aes" algoritması kullanılmıştır.

  snmp-server user kullanıcı1 grup1 v3 encrypted auth md5 cisco priv aes 256

- Özellikler atanır: Oluşturulan gruplara "read, write ve notify" özellikleri atanır. Çalışmamız sadece topoloji keşfetme amacında olduğu için "read" komutu kullanılmıştır.

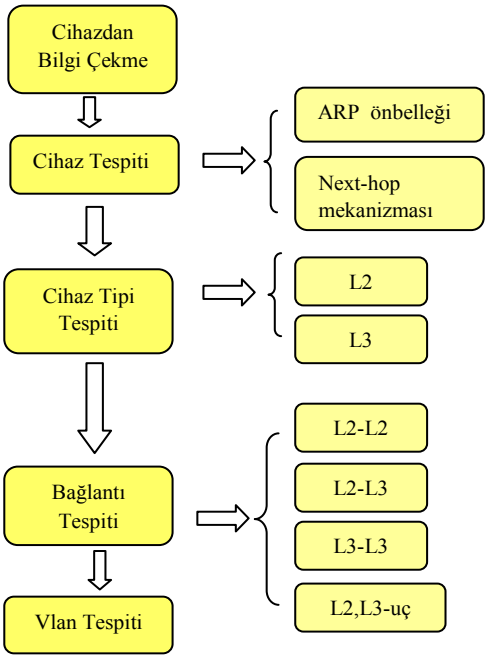
  snmp-server view izle system included

- VPN kullanıcıları için gerekli ayarlamalar yapılır. Oluşturulan gruplara "context ve match" parametreleri kullanılarak bir içerik tanımlanmalıdır.

Gerekli ayarlamalar yapıldıktan sonra algoritma çalıştırılmaya hazırdır. Daha öncede ifade edildiği gibi SNMP protokolü istek gönderme ve isteğe cevap şeklinde çalışır [4]. Cihazın sistem bilgisi, üzerindeki yönlendirme tablosu, mac adres tablosu, cihaz üzerinden geçen paket sayısı gibi cihazla ilgili tüm bilgiler MIB denen değerlerle ifade edilir. Yani cihazdan ilgili veri çekileceği zaman o veriyle alakalı olan MIB değeri sorgunun sonuna eklenir.

Algoritma da, cihazlardan dönen bu SNMP MIB değerlerine göre oluşturulmuş ve algoritmanın her aşamasında yapılan işleme göre MIB değerleri kullanılmıştır.

Uygulama için önerilen algoritma aşağıda verilmiştir. Bu algoritma, GNS3 modelleme programının anahtar cihazlar (switch) ve mantıksal topolojilerdeki bazı özellikleri desteklememesinden dolayı, [1] numaralı çalışmada önerilen algoritmanın özelleştirilmiş halidir:



Şekil 2: Önerilen Algoritma

Algoritmanın adımları:

- **Cihazdan bilgi çekme**: Sanal ortam üzerinde ağ topolojisi oluşturulduktan sonra cihazlar üzerinde konfigürasyon yapılır, daha sonra bu cihazlara SNMP sorgusu gönderilerek bilgi çekilir.

- **Cihaz tespiti**: ARP önbellek kayıtları ve Next-hop mekanizması kullanılarak, cihazlar üzerinden "ipNetToMediaNetAddress" ve "ipRouteNextHop" değerleri çekilir [13,14].

- **Cihaz tipi tespiti**: Cihazdan çekilen "sysServices" değerine göre cihazın L2 veya L3 cihaz olduğuna karar verilir.

- **Bağlantı tespiti**: Cihazlardan dönen ip ve mac adres eşleştirmeleri sonucunda aradaki bağlantının L2 bağlantı veya L3 bağlantı olduğuna karar verilir.

- **Vlan tespiti**: Cihazlardan dönen "Cisco-VTP-MIB" değeri kullanılarak vlan numarası ve ismi tespit edilir [15].

3.3 Uygulama geliştirme ortamları

Uygulama java programlama diliyle yazılmaktadır. Veritabanı olarak MySql kullanılmaktadır. SNMP kütüphanesi için Advent Net Java API'leri kullanılmaktadır [16]. Topoloji keşfinden sonra topoloji çıktısının grafiksel olarak görüntülenebilmesi için Java'nın grafik kütüphanelerinden JGraphT kullanılmaktadır [17].

Sonraki çalışma olarak, sanal ortam üzerinde oluşturulan kurumsal ağın içersinde kaç adet L2, L3 cihazın olduğu, bu cihazlar arasında hangi bağlantı türlerinin olduğu, oluşturulan Vlan (Sanal yerel ağ) isimleri ve numaraları belirlenip, topolojinin grafiksel olarak şeması çıkarılacaktır.

4.Sonuçlar

Bu çalışmada kurumsal bir ağ yapısının topoloji keşfinde gerçek bir ortam üzerinde çalışmak yerine fiziksel ortamdaki sıkıntılarla karşılaşmamak için sanal bir ortam üzerinde bir çalışma yapılmıştır. Sanal ortam için GNS3 ve VMWARE programları kullanılmış, bu programlar üzerinde gerekli konfigürasyonlar yapılmış ve güvenli bir ortam sunan SNMPv3 kullanılarak örnek bir kurumsal ağ yapısı oluşturulmuştur. Topoloji keşfi için daha önceden yapılan birçok akademik ve ticari uygulamada kullanılan teknikler göz önüne alınarak bir algoritma önerilmiştir. Bu algoritmanın uygulama geliştirme ortamları başlığı altında verilen araçlarla gerçeklenmesi sonraki çalışma olarak hedeflenmiştir. Bu hedefin gerçeklenmesi ile önerilen algoritmanın farklı topolojiler üzerinde çalıştırılmasına ve çıkan sonuçlara bağlı olarak topolojiler arasında performans testleri yapılmasına da imkan tanıyacağı sonuç olarak öngörülmüştür.

5. Teşekkür

Bu çalışma SAÜ Bilimsel Araştırma Projeleri Komisyonu tarafından desteklenmiştir. (Proje no: 2011-50-01-072)

6. Kaynakça

1.Pandey S. , Choi M. , Won Y. ,Hong J. , SNMP-based enterprise IP network topology discovery,In International Journal of Network Management 2011; Volume 21, Issue 3, May 2011, Pages: 169–184

2. Siamwalla R, Sharma R, Keshav S. *Discovering internet topology*. Technical report, Cornell University, May 1999.

3. Breitbart Y, Garofalakis M, Jai B, Martin C, Rastogi R, Silberschatz A. Topology discovery in heterogeneous IP networks:the NetInventory system. *IEEE/ACM Transactions on Networking* 2004; **12**(3): 401–414.

4. Lowekamp B, O'Hallaron DR, Gross TR. Topology discovery for large Ethernet networks. In *ACM SIGCOMM*, San Diego, CA, August 2001; 237–248.

5.http://www.dell.com/content/topics/global.aspx/power/en/ps2q03_maah?c=us&1=en&cs=555 [Ziyaret Tarihi: 25.07.2011]

6. JIZONG LI, WEB-based Network Monitoring Using SNMP, CGI and CORBA, in University of Manitoba, August 1999, 6:10-14:22.

7. E. MELLQUIST, SNMP++: An Object-Oriented Approach to Developing Network Management Applications, Prentice Hall PTR, 1997; 5:10:20-28

8.http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html [Ziyaret Tarihi: 15.07.2011]

9. http://nmap.org/book/man.html [Ziyaret Tarihi: 16.07.2011]

10.http://www.paessler.com/manuals/prtg8/quick_start_guide.htm [Ziyaret Tarihi: 16.07.2011]

11.http://www.gns3.net/documentation [Ziyaret Tarihi: 25.06.2011]

12. http://www.vmware.com/support/pubs/[Ziyaret Tarihi: 25.06.2011]

13. Cisco. SNMP community string indexing. http://www.cisco.com/en/US/tech/tk648/tk362/techn

ologies_tech_note09186a00801576ff.shtml [Ziyaret Tarihi: 27.07.2011].

14. Bierman A, Jones K. Physical topology MIB. *IETF RFC-2922*, September 2000.

15.CISCO-VTP-MIB http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00801576ff.shtml [Ziyaret Tarihi: 05.07.2011].

16. AdventNet. AdventNet SNMP API. http://snmp.adventnet.com/[Ziyaret Tarihi: 01.07.2011].

17. JGraphT. Implementation and source code. http://jgrapht.sourceforge.net[ZiyaretTarihi:02.07.2011]

İnternet Bankacılığında Akıllı SMS İçin Üç Yollu El Sıkışma

Onur Gök[1] H.Engin Demiray[2]

[1,2]Bilgisayar Mühendisliği Bölümü, Kocaeli Üniversitesi, Kocaeli
[1]e-posta: ogok@kocaeli.edu.tr [2] e-posta: hedemiray@kocaeli.edu.tr

Özetçe

İletişim ve bilişim sektöründeki hızlı gelişim ve zamanın en değerli olduğu gerçeği, bankaların da bu gelişime ayak uydurma çabaları ve müşterilerine daha hızlı ve kaliteli hizmet vermeleri için İnternet bankacılığı önemli alternatif yol olmuştur. Bu alternatif bankacılık hizmeti sayesinde, banka müşterileri zaman ve mekandan bağımsız tüm bankacılık hizmetlerini gerçekleştirmeleri hem müşteri hem banka açısından büyük kolaylıklar sağlamıştır. Bu kolaylıklarla beraber, internet altyapısının getirdiği bazı güvenlik riskleri de mevcuttur. Bu risklerden bir tanesi de banka müşterisinin kimlik doğrulamasıdır. Kimlik doğrulama işlemleri için, bankalar internet bankacılığı sistemleri kapsamında günümüze kadar farklı metotlar uygulanmıştır. Bu metotlardan bazıları sadece müşterinin belirlediği şifreler, müşteriye verilen rast gele şifre üreten anahtarlar, cep telefonuna gelen şifreler olmuştur.Günümüzde en yaygın olarak kullanılan metot iki kademeli kimlik doğrulamasıdır. Birinci adımda kullanıcının belirlediği şifre, ikinci adımda bankanın müşterinin cep telefonuna gönderdiği SMS onay şifresinin kullanılarak internet bankacılığı sistemine girilmesi şeklindedir. Bu yöntemde SMS onay şifresinin müşteriye veya üçüncü kişilere ulaşıp ulaşmadığı konusunda bir kontrol yapılmamaktadır. Bu sebeple güvenlik açığı ortaya çıkmaktadır. Bu çalışmamızda bu güvenlik zafiyetini ortadan kaldırmak için bir onay mekanizması yöntemi önerilmiştir. Önerilen çalışmada, bilgisayar ağlarında bağlantı kurmak için kullanılan 3 yollu el sıkışma benzetimi yapılmıştır.

1. Giriş

Türkiye'de faaliyet gösteren bankaların birçoğu müşterilerine internet üzerinden de hizmet vermektedir. Günümüzde İnternet Bankacılığı; bankalar, ve müşterileri açısından önemli bir yer tutmakta olup, işlemlerin hızlı bir şekilde sonuçlandırılması ve maliyetler açısından her iki tarafa da fayda sağlamaktadır. Türkiye Bankalar Birliği üyesi olan ve İnternet Bankacılığı hizmeti veren 25 bankadan alınan bilgilere göre; Aralık 2008 itibariyle internet bankacılığı yapmak üzere sistemde kayıtlı olan ve en az bir kez sisteme giriş yapmış toplam müşteri sayısı 12.580.671'dir.

Internet Bankacılığı, işlem maliyetinin düşüklüğü, kolaylığı, ürün çeşitliliği, hızlı bilgi değişimi gibi avantajlarıyla hem bankalar hem de tüketiciler için en cazip dağıtım kanalı olarak dikkat çekmekte ve bütün dünyada hızla yayılmaktadır [1].

İlk İnternet Bankacılık hizmeti 1997 tarihinde verilmeye başlanmıştır. Oldukça yeni olan bu dağıtım kanalında ilk yıllarda kayıtlı dolandırıcılık işlemi azdı. İnternet bankacılığının büyük bir hızla yaygınlaşması ile beraber, tüm dünyada olduğu gibi, ülkemizde de internet üzerinden yapılan dolandırıcılık girişimlerinde artış gözlemlenmektedir. Son dönemde, bu konudaki yasal boşluklar internet bilgi hırsızları (hacker) tarafından fark edilmiş kötü niyetli girişimler ve saldırılar başlamıştır. İnternet bankacılığı dolandırıcılık eylemlerindeki ortak kurgu; müşterinin özel bilgilerinin, kullanıcı bilgisayarından çeşitli yöntemlerle çalınması ve bu bilgilerin kullanılarak müşteri adına internet üzerinde işlem yapılmasıdır .

Kimlik hırsızlığı (identity theft), bir başkasına ait kişisel bilgilerin yetkisiz olarak kullanılması suretiyle işlenen dolandırıcılık yöntemidir [2].

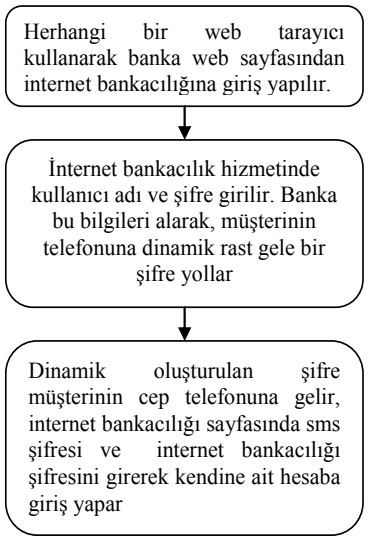
Kimlik hırsızlığında dolandırıcıların en çok kullandığı yöntemler şöyle sıralanabilir:

Tuş kaydediciler (keylogger),
Ekran kaydediciler (Screenlogger)
Oltalama (Phishing)
Casus yazılım (Spyware)
Sosyal mühendislik.

Kimlik hırsızlığı yöntemlerine bakıldığı zaman, bu yöntemlerin genellikle kullanıcının tedbirsiz ve dikkatsizliklerinden kaynaklandığı görülmektedir. İnternetteki tehlikelerden haberi olmayan bir kullanıcı, internet bankacılığında geleceğin mağdurlarından biri olarak görülebilir[3].

Bir banka müşterisinin, internet bankacılığı sistemini kullanabilmesi için, banka sisteminin müşteri kimliğini doğrulaması gerekmektedir. Bu doğrulama, sadece bankanın ve müşterinin bildiği bilgilerin sorgulanması ile olmaktadır. Müşterinin bilgisayarından girdiği kişisel bilgiler banka sisteminde saklı kişisel bilgilerle karşılaştırılıp, yetkili müşteri tarafından yapılıp yapılmadığı sistem tarafından kontrol edilerek girişe izin verilmektedir. İnternet bankacılığı işlemlerinde kişisel bilgilerin doğrulanmasında, güvenliğin sağlanması için geliştirilen teknikler arasında, güvenlik ihtiyacına göre parola, şifre, para çıkışlarında ikinci bir işlem şifresi, ortak belirlenen cep telefonlarına Mesaj, Akıllı SMS, IP Kısıtlaması, Tek Kullanımlık Şifre, Akıllı Anahtar, Elektronik İmza gibi tekniklerden bir kaçı uygulanabildiği gibi, güvenlik ihtiyacına göre bunların kombinasyonundan oluşan kademeli bir anlayışı da uygulandığı görülmüştür.

Günümüzde kullanılan kişisel bilgilerin doğrulanmasında kullanılan yöntemlerinden birisi de akıllı SMS'dir. Bu yöntemde müşteri bankanın internet hizmetini kullanmak istediğinde, bankanın web sayfasından sisteme giriş yapmak için kullanıcı adı (hesap numarası da olabilir) ve internet şifresini kullanmakta, bu şifre ile giriş yaptıktan sonra cep telefonuna bankanın ürettiği rast gele dinamik bir şifre gelmektedir. Belli bir zaman aralığında bu şifreyi web sayfasında kullanarak internet bankacılığı sistemine giriş yapılabilmektedir.



Şekil 1: Uygulanan internet bankacılığı adımları

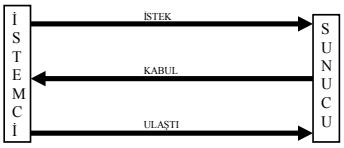
Şekil 1'de internet bankacılığı sisteminde, akıllı SMS kullanımının amacı, müşterilerin web sayfasına girmek için kullandıkları statik şifre ve kullanıcı adının 3. kişiler tarafından internet ağı üzerinden keylogger, screenlogger, truva atı, phishing gibi yöntemleri ile ele geçirilme ihtimaline vardır. Bu durumu engellemek için internet bankacılığı

sistemlerinde Akıllı SMS yüksek oranda bir çözüm olmuştur. Yukarıda bahsedilen internet ağı kullanılarak yapılan kimlik hırsızlıklarını etkisiz hale getirmek için, internet bankacılığı sistemine girmek isteyen müşteriye farklı bir alt yapı olan GSM kullanılarak dinamik bir şifre gönderilmektedir. Bu sayede kimlik hırsızlarının bu bilgiye ulaşmaları engellenerek, sadece cep telefonuna giden SMS şifresini bilen müşterinin internet bankacılığı sistemine girmesi sağlanır.

Günümüzde bu güvenlik mekanizmasına rağmen, kimlik hırsızlığı ile ilgili farklı metotlar yapıldığı görülmüştür. Müşterinin kimlik bilgileri ve telefon numarası elde edilerek, GSM kartı bloke edildiği, akıllı SMS'lerini, kopyalanan aynı telefon numarasına sahip başka bir telefona yönlendirildiği ve bu sayede internet bankacılığı şifresi ve akıllı SMS şifresi ile müşterilerin hesaplarına girilip boşaltıldığı tespitleri yapılmıştır. Gönderilen akıllı SMS'in müşteriye ulaştığı bilgisi böyle bir açığı engelleyecektir. Bankanın gönderdiği SMS'in istekte bulunan müşteri tarafından alındığı bilgisini bankaya iletmesi durumunda yukarıdaki anlatılan durum için bir çözüm olacaktır. Bu çözüm, bilgisayar ağlarında iki üç bilgisayar arasında iletişime geçmeden önce bağlantı kurmak için kullandığı üç yollu el sıkışma mantığına benzemektedir. Müşteri ilk olarak internet bankacılık sistemine girerek 1. yolu oluşturacak, banka müşteriye SMS ile dinamik şifre göndererek 2. yolu oluşturacak, müşteri dinamik şifreyi kendisinin aldığını bankaya SMS ile ileterek 3. yol oluşmuş olacaktır.

2. Üç Yollu El Sıkışma ve Uygulamaya Benzetimi

İnternet ağlarında iki uç bilgisayarın birbiri ile haberleşmesi için tanımlanmış protokol olan TCP'de, bilgisayarlar haberleşmeye başlamadan önce birbirleri ile bağlantı kurmak için Tomlinson[4] tarafından önerilen 3 yollu el sıkışma mantığını kullanır[5]. Bu mantığa göre, bağlantı kurmak isteyen istemci , bağlantı kurulmak istenen sunucuya İSTEK mesajı gönderir ve belli süre bekler. Sunucu eğer müsaitse istemciye KABUL mesajını iletir. Sunucu KABUL mesajının istemciye gittiğini öğrenmek için belli bir süre istemciden KABUL mesajının ulaştığına dair ULAŞTI mesajı bekler , ULAŞTI mesajı bu süre içerisinde sunucuya ulaşırsa her iki bilgisayar bağlantı kurma işlemi yaparlar.



Şekil 2: İnternet ağlarında TCP bağlantı kurma

İnternet bankacılığı için kullanılan Akıllı SMS yönteminde, müşterinin SMS'i aldığına dair bankaya cep telefonu üzerinden göndereceği ULAŞTI mesajı tam bir bağlantı kurulmasını sağlayacaktır. Fakat burada ULAŞTI mesajının içeriği önem kazanacaktır. Bu mesajın içeriği, müşteriyi tanımlaması gerekecektir. Bu nedenle, mesaj içeriği 3. kişilerin eline geçemeyecek sadece banka ve müşteri tarafından bilinen statik veya dinamik, donanımsal veya yazılımsal bir bilgi olması gerekecektir. Mesaj içeriğinin nasıl olması gerektiği ile ilgili birden fazla çözüm yolu olabilir. Bu çözüm yolları şu şekilde sıralanabilir:

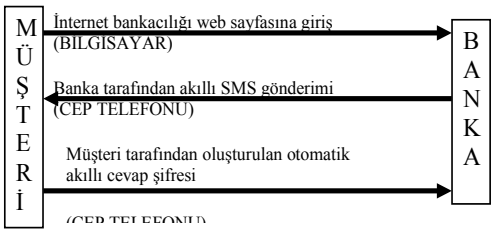
- Donanımsal bilgi: cep telefonu IMEI numarası
- Müşteri bazlı bilgi: Müşterinin bankadan elden aldığı veya banka kartı ile ATM'den alabileceği akıllı cevap şifresi
- Yazılımsal bilgi: Bankanın üreteceği , cep telefonlarına yüklenebilecek bir yazılım olacaktır. IMEI numarası, akıllı cevap şifresi (sadece müşterinin bildiği) oluşan 2 anahtarlı kriptolanmış bilgi.

5070 sayılı Elektronik İmza Kanunu'nda yer alan şekliyle elektronik imza; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar.

Elektronik imza kavramı çok genel bir tanım olup kişilerin elle atmış olduğu imzaların tarayıcıdan geçirilmiş hali olan sayısallaştırılmış imzaları, kişilerin göz retinası, parmak izi ya da ses gibi biyolojik özelliklerinin kaydedilerek kullanıldığı biyometrik önlemleri içeren elektronik imzaları veya bilginin bütünlüğünü ve tarafların kimliklerinin doğruluğunu sağlayan sayısal imzaları içermektedir. Sayısal imza, imzalanan metine göre farklılık gösterir ve içeriğin matematiksel fonksiyonlardan geçirilerek eşsiz olduğu düşünülen bir değer bulunması sureti ile elde edilir. Yani kişilerin, elle atılan imzada olduğu şekilde tek imzası yoktur; bunun yerine imzalamada kullanılan anahtarları vardır. 5070 sayılı Elektronik İmza Kanunu'nda ve bu metinde geçen "elektronik imza" kavramı sayısal imzayı işaret etmektedir.

Uluslararası Mobil Cihaz Kodu (IMEI: International Mobile Equipment Identity): Her bir GSM telefon cihazına üretim aşamasında IMEI numarası yüklenmektedir. IMEI numarası her bir cihazın kimlik numarası olup tek ve benzersizdir.

Günümüzde internet bankacılığı işlemlerinde E-imza, cep telefonlarına gönderilen akıllı mesaj olarak kullanılmaktadır. Tek ve benzersiz olan IMEI numarası bir E-imza uygulaması olarak kullanılması temelinde üç yollu el sıkışma mantığı ile müşteri ve banka arasında bağlantı kurmak daha güvenilir bir yol olacağı düşünülmektedir.



ŞEKİL 3. İnternet bankacılığında üç yollu el sıkışma

Müşteri, herhangi bir bilgisayardan bankasının internet bankacılığı sistemine giriş yapmak istediğinde, web sayfası üzerinden müşteri numarası ve parola kullanarak bağlantı isteğinde bulunur. Bağlantı isteği bankanın sisteminde yorumlanır. Banka müşterinin kayıtlı olduğu cep telefonuna akıllı SMS ile bir şifre gönderir. Kimlik doğrulama işlemi için, müşteriden cevabı cep telefonu üzerinden bekler. Müşterinin mesajı aldığına dair donanımsal, yazılımsal veya müşterinin girdiği alındı şifresini GSM üzerinden Sms yoluyla göndermesi ile internet bankacılığı sisteminde oturum açmak için izin alır. Bankanın sistemine giden alındı mesajı ile birlikte, müşteri internet bankacılığına girmek için parola ve akıllı SMS şifresini sistemde girerek, oturum açabilir.

Cep telefonun tek ve benzersiz olan fiziksel adresi(IMEI) sayısal imza olarak kullanılarak, kimlik hırsızlığının azaltılması sağlanacaktır. Bunun yanında bankaların internet bankacılığı sistemine müşterilerin cep telefonu IMEI numaralarını kayıt edilmeleri gerekmektedir. Bu hem bankalara hem müşteriye ek bir yük getirmesi dezavantaj olarak görülebilir. Bunun yanında müşterinin de sms olarak alındı cevabı göndermesi müşteriyi uğraştırması veya zamanını alması bir dezavantaj olarak görülebilir fakat gelişen bilişim sistemi ile birlikte cep telefonu üzerinde geliştirilebilecek uygulamalarla bu yük azaltılabilir. Sayısal imza için ek bir donanım için maliyet de düşünülürse, cep telefonlarının sayısal imza için kullanılması sadece bankacılık işlemleri için değil, internet ortamında sayısal imza gerektiren diğer tüm uygulamalar için de bir anahtar olması mantıklı bir seçim olabilir.

3. Sonuçlar

Ocak 2010 tarihinden itibaren BDDK tarafından zorunlu hale getirilen elektronik imza, internet bankacılığı hizmetlerinde, cep telefonlarının dolaylı olarak elektronik imza gibi kullanılması gibi durumu ortaya çıkarmıştır. Bankalar ve GSM firmaları birbirlerinden farklı kurumlardır ve hizmet yönleri farklı olduğu için, internet bankacılığında güvenlik için cep telefonu kullanılmasında bazı boşluklar ortaya çıkmaktadır. Akıllı SMS, internet bankacılığı dolandırıcılıkları için büyük oranda çare olmuş fakat kullandığı GSM hizmetlerindeki farklılıklardan kaynaklanan (sim kart kopyalama gibi) açık meydana gelebilmektedir. Yaptığımız çalışmada bu açığın kapatılması için bir öneri yapılmıştır.

Müşterinin bankaya gönderdiği Akıllı SMS ulaştı mesajının temelinde, tek ve benzersiz olarak kullanılan IMEI numarası vardır. IMEI numarasının sayısal imza olarak kullanılması sadece banka işlemleri için değil, elektronik ortamda tüm diğer işlemler için bir sayısal imza olarak kullanılması tercih edilebilecek bir metot olarak düşünülmüştür.

Cep telefonları internet bankacılığı işlemleri için bir bakış açısıyla donanımsal anahtarımız olmuştur. Önümüzdeki yıllarda, bu anahtarın sadece internet bankacılığı gibi güvenlik isteyen mekanizmalar için değil, tüm internet işlemleri içinde bir nevi Elektronik imza gibi kullanılması için IMEI numarası, parmak izi tarayıcı gibi, TC kimlik numarası gibi bilgiler donanım üzerine yazılımsal olarak gömülerek , uygulama çeşitliliği artırılabilir.

4. Kaynakça

[1] Usta, R., "Tüketicilerin Internet Bankacılığını Kullanmama Nedenleri Üzerine Bir Araştırma", Doğuş Üniversitesi Dergisi, 6 (2) 2005, 279-290 (2005).

[2] Kocamaz, C., "Kimlik Hırsızlığına Karşı Web Tarayıcıların Kullanımı Kimlik Hırsızlığı", www.sayisaldelil.net, Erişim Tarihi:02/10/2009 (2009).

[3] Ayvaz Reis, Z., Gülseçen, Z., Bayrakdar, B., "Güvenli Internet Bankacılığı Eğitim Sistemi :GIBES, Akademik Bilişim Konferansı, 2010

[4] Raymond S. Tomlinson, "Selecting Sequence Numbers," INWG Protocol Note 2, IFIP Working Group 6.1, August 1974. Also in Proceedings of the ACM SIGCOMM/SIGOPS Interprocess Communications Workshop, (Santa Monica, CA, March 24–25, 1975), and ACM Operating Systems Review, Volume 9, Number 3, July 1975, Association for Computer Machinery, New York, 1975.

[5] Kurose, J.F. & Ross, K.W. (2010). Computer Networking, 5th ed. Boston, MA: Pearson Education, Inc.

Şifreli İnternet Trafiğinin Gerçek Zamanlı Sınıflandırılması

Cihangir Beşiktaş[1] Hacı Ali Mantar[2]

[1,2]Bilgisayar Mühendisliği Bölümü, Gebze Yüksek Teknoloji Enstitüsü, Kocaeli
[1]TÜBİTAK BİLGEM, Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi, Kocaeli
[1]e-posta: cihangirbesiktas@uekae.tubitak.gov.tr [2] e-posta: hamantar@bilmuh.gyte.edu.tr

Özetçe

İnternet trafik akışlarının uygulama veya protokol bazında sınıflandırılması ağ izleme, hizmet kalitesi, nüfuz tespiti, ağ güvenliği, trend analizi vb. alanlarda etkin bir şekilde kullanılmaktadır. Son zamanlarda bazı P2P uygulamalarının dinamik port numaraları, maskeleme teknikleri kullanmaları port bazlı tespit sistemlerinin yetersiz kalmasına neden olmuştur. Bu engellere alternatif olarak geliştirilen yük bazlı tespit sistemleri ise uygulamaların güvenlik ve takip edilmeme amacıyla şifreleme mekanizmalarına gitmesi ve uygulama katmanında imza arama işlemlerinin çok maliyetli olması nedeniyle yerini makine öğrenmesi ve istatistiki verilere dayanan yaklaşımlara bırakmıştır.
Bu çalışma gerçek zamanlı olarak şifreli internet trafiğini de tespit edebilen makine öğrenmesi tabanlı bir yöntemi ele almaktadır. Bu yöntemde öğrenme aşamasında trafik akışlarının ilk bir kaç paketinin paket boyutlarından uygulamalara özgü paket boyutları vektörü ve normalize edilmiş standart sapma vektörü karakteristikleri çıkartılmaktadır. Yeni bir akışın sınıflandırması ise her bir uygulamanın karakteristiği ile yapılan ağırlıklı kosinüs benzerliği hesabına göre yapılmaktadır. Deneysel sonuçlar önerilen yöntemin yüksek bir başarıma sahip olduğunu göstermektedir.

1. Giriş

Gerçek zamanlı internet trafik sınıflandırması internet servis sağlayıcılarına nüfuz tespiti ile güvenlikte, hizmet kalitesi ile ağın performanslı kullanılmasında, trend analizlerinde, protokol bazlı filtreleme ile farklı kategorilerde internet hizmet peketlerinin oluşturulmasında fayda sağlamaktadır. Ayrıca hükümetlerin koyduğu yükümlülükler çerçevesinde IP veri trafiğinin yasal olarak izlenmesinde de etkin bir rol oynamaktadır.
İnternet trafik sınıflandırılması ile aynı kaynak IP, port, hedef IP, port ve iletim protokolüne (TCP, UDP) sahip olan paketlerin oluşturduğu ağ akışlarının hangi uygulamaya veya protokole ait olduğu tespit edilir. En basit anlamda bu işlem ağ akışlarının IANA tarafından belirlenen protokollerin klasik TCP veya UDP port numaralarına [1] bakılarak gerçekleştirilir. Fakat bazı uygulamaların dinamik port numaraları kullanmaları, bazı uygulamaların da güvenlik duvarlarını aşmak için http, ftp gibi servislerin genelde internete açık olan klasik port numaralarını kullanması port bazlı yaklaşımları yetersiz kılmıştır. Moore ve Papagiannaki [2] port bazlı yaklaşımların %70 başarım sağladığını tespit etmişlerdir.
Port bazlı yaklaşımların yetersiz oluşu araştırma dünyasını yük bazlı yaklaşımlara yöneltmiştir [3, 4].
Yük bazlı yaklaşımlarda ağ akışlarındaki paketlerin uygulama katmanlarına bakılarak derinlemesine paket incelemesi yapılır. Paketlerin yüklerinde belirli imzalar aranarak ağ akışının hangi protokole ait olduğu tespit edilmeye çalışılır. Yük bazlı yaklaşımların ise aşağıda belirtilen sıkıntıları vardır:

- Kendine özgü yapıya sahip olan veya kaliteli dokümantasyona sahip olmayan protokoller için ileri seviyede tersine mühendislik çalışması gerektirmektedir.
- Şifreleme kullanan protokollerin tespit edilmesi mümkün değildir.
- Periyodik olarak protokollerin imzalarının güncellenmesi gerekmektedir.
- Paketler üzerinde yapılan imza arama işlemleri CPU ve bellek kaynaklarını yoğun bir şekilde tüketmektedir.

Yük bazlı yaklaşımların yukarıda listelenen problemlerinden dolayı CPU ve bellek kaynaklarını daha az tüketen ve şifreli trafiğin tespit edilmesine de olanak sağlayan makine öğrenmesi tabanlı istatistiki yaklaşımlar üzerine son zamanlarda birçok çalışma yapılmaktadır. Makine öğrenmesi tabanlı yaklaşımların uygulamaları bir kaç adımdan oluşmaktadır. Önce ağ akışlarının ayırt edilmesini sağlayan özellikler çıkartılır. Bu özellikler maksimum, minimum paket uzunlukları, paket uzunluklarının ortası, ortalaması, standart sapması, paketler arası süreler gibi ağ akışlarına ait davranışlardır. Daha sonra ise öğrenme aşamasına geçilir. Bu aşamada her bir uygulama veya protokol için seçilen özellikler cinsinden bir karakteristik belirlenir. Son olarak ise yeni gelen bir ağ akışının hangi uygulamaya veya protokole ait olduğunu öğrenilen karakteristiklerle karşılaştırma yaparak tespit eden sınıflandırma algoritması uygulanır.
Bu çalışma makine öğrenmesi metodolojisini kullanarak IP trafiğinin gerçek zamanlı olarak sınıflandırılması üzerine yoğunlaşmıştır. Önerilen yaklaşım ağ akışlarının ilk bir kaç paketinin paket uzunlukları ve normalize edilmiş standart sapmaları üzerinde kosinüs benzerliği hesaplaması ile sınıflandırma yapmaktadır.
Bu bildirinin kalan kısmı şu bölümlerden oluşmaktadır. Bölüm 2 makine öğrenmesi tabanlı IP trafik sınıflandırması ile ilgili yapılan çalışmalara yer vermektedir. Bölüm 3 yaklaşımımızın metodolojisini anlatmakta, bölüm 4 yaklaşımımızın deneysel sonuçlarını içermektedir. Bölüm 5 ve 6 da ise gelecek çalışmalar ve sonuçlar anlatılmıştır.

2. Benzer Çalışmalar

Makine öğrenmesi tabanlı IP trafik sınıflandırması çalışmaları metodolojileri açısından üçe ayrılmaktadırlar:

- Güdümlü sınıflandırma
- Güdümsüz sınıflandırma
- Karma sınıflandırma

Güdümlü sınıflandırmada öğrenme aşamasında kullanılan veri

kümesindeki her bir verinin hangi uygulamaya ait olduğu önceden etiketlenir ve bu etiketlere göre karakteristikler çıkartılır. Dolayısıyla öğrenme aşamasındaki veri kümesinin port ve/veya yük bazlı trafik tespiti yapan yazılımlar aracılığı ile veya manuel olarak önceden etiketlenmesi gerekmektedir.
Güdümsüz sınıflandırmada ise veri kümesindeki veriler önceden etiketli değildir ve bu verilerden benzer karakteristiklere sahip olanlar gruplanır. Bu gruplar üzerinde daha sonradan etiketleme işlemi yapılır.
Karma sınıflandırma çalışmaları ise hem güdümlü hem de güdümsüz sınıflandırma yaklaşımlarını birlikte kullanırlar.
Makine öğrenmesi tabanlı IP trafik sınıflandırması çalışmalarının ilk örneklerinden biri McGregor ve diğerlerinin [5] 2004 yılında Beklenti Maksimizasyonu algoritmasını kullanarak gerçekleştirdikleri yaklaşımdır. Bu yaklaşım güdümsüz sınıflandırma yaparak HTTP, FTP, SMTP, IMAP, NTP ve DNS protokollerini tespit etmeye çalışmıştır.
Güdümsüz sınıflandırma çalışmalarına örnek olarak Zander ve diğerlerinin [6] Beklenti Maksimizasyonu algoritmasını kullanan Bayesian sınıflandırıcısı, Bernaille ve diğerlerinin [7] basit K-Means algoritması üzerine yaptıkları çalışma, Erman ve diğerlerinin [8] öklit uzaklığı ve K-Means algoritmasını kullanarak yaptıkları çalışma gösterilebilir.
Güdümlü sınıflandırma çalışmalarında ise Saf Bayes, Saf Bayes Çekirdek Tahmini, Bayesian Ağlar, C4.5 Karar Ağaçları, k-En Yakın Komşular, Sinir Ağları ve Destek Vektör Makineleri genelde tercih edilen algoritmalar olmuştur.
Roughan ve diğerleri [9] NN, LDA ve QDA algoritmaları üzerine yaptıkları çalışmada paket uzunluklarının ortası, varyansı, kök orta karesi, ağ akışlarının süresi, toplam boyutu, toplam paketleri, bağlantıların TCP pencere boyutu, bant genişliği dağılımı gibi özellikleri kullanmışlardır.
Moore ve Zuev [10] ise ağ akışlarına ait 248 özelliği Saf Bayes algoritmasını kullanan sınıflandırıcılarını eğitmek için kullanmışlardır. Bu algoritma ile %65 akış keskinliği yakalamışlardır. Daha sonra [11] de çalışmaları genişletilerek %90 üzerinde akış keskinliği yakalanan Bayesian Sinir Ağı yaklaşımı önerilmiştir.
[9, 10, 11] deki çalışmalar ağ akışlarına ait bir çok özelliği kullandıkları için gerçek zamanda sınıflandırma özellikleri yoktur. Gerçek zamanda sınıflandırma çalışmalarından biri Crotti ve diğerlerinin [12] ağ akışlarının ilk paket uzunlukları, paketler arası geçen süreler ve paket erişim sıralarını kullanarak %91 ağ akış keskinliği yakaladıkları Basit İstatistiksel Protokol Parmakizi metodu olmuştur. Çalışmalarında değişkenlik gösteren RTT, MTU değerlerinin neden oldukları gürültüleri azaltmak için protokol maskesi ve normalizasyon teknikleri kullanmışlardır.
Vektör uzay modelini kullanarak IP trafik sınıflandırması ise Chung ve diğerleri [13] tarafından yapılmıştır. Çalışmalarında özellik olarak paketlerin yüklerinde geçen kelimelerin (16 bitlik sayı) sıklıklarından oluşan yük vektörlerini kullanmışlardır. Paketlerin yüklerini incelediklerinden çalışmaları şifreli trafiğin tespitini sağlayamamaktadır.
Bu çalışmada ise ağ akışlarının ilk bir kaç paketinin uzunlukları ve normalize edilmiş standart sapmaları vektör uzay modelinde özellik olarak kullanılmıştır. İlk bir kaç paketin uygulamaların müzakere fazını oluşturması ve paketlerin yüklerine bakılmaması şifreli trafiğin gerçek zamanda tespit edilmesini sağlayan etkenler olduğu düşünülmektedir.

3. Metodoloji

Bu bölüm IP trafik sınıflandırma yöntemimizi açıklamaktadır. Vektör uzay modeli, uygulamaların paket uzunlukları ile standart sapma vektörlerinin çıkarılması ve bu vektörleri kullanarak gerçeklenen kosinüs benzerliği bu bölümün alt başlıklarında anlatılmaktadır.

3.1. Vektör uzay modeli

Vektör uzay modeli doküman sınıflandırmada kullanılan ve metin dokümanlarını cebirsel olarak temsil eden vektörlerden oluşan bir modeldir. Bu modellemede her bir doküman, barındırdığı metinlerin sıklıklarına göre bir vektöre sahip olur. Dokümanlar sahip oldukları vektörler ile yapılan benzerlik hesapları ile sınıflandırılırlar. Bu modelleme IP trafik sınıflandırmasına da uygulanabilir. Bunun için ağ üzerinden geçen aynı uygulamaya ait akışlar bir doküman gibi ele alınıp ona ait bir vektör oluşturulur. Dokümanları temsil eden metinlerin sıklıkları yerine ise akışların paket uzunlukları ve bu paket uzunluklarının normalize edilmiş standart sapmaları kullanılabilir.

3.2. Ağırlıklı Kosinüs Benzerliği

IP trafik sınıflandırmasında yeni bir ağ akışının protokolü ağırlıklı kosinüs benzerliği ile tespit edilmektedir.
Kosinüs benzerliği iki vektör arasındaki açının kosinüsünün hesaplanmasına dayanır. Vektörler arası açı ne kadar az ise kosinüs değeri de 1' e o kadar yakındır. Dolayısıyla iki vektör birbirine ne kadar benzer ise kosinüs değeri de 1'e o kadar yakındır. Kosinüs benzerliğinin matematiksel tanımlaması aşağıdaki gibidir.
v, w iki vektör, *a* bu vektörlere ait ağırlıklandırma vektörü ve *n* vektörlerin eleman sayısı olsun. Bu durumda *a* ağırlık vektörünü kullanarak *v* ve *w* vektörleri arasındaki ağırlıklı kosinüs benzerliği hesabı 1. denklemdeki gibidir.

$$AKB(v,w) = \frac{\sum_{i=1}^{n} a_i v_i w_i}{\sqrt{\sum_{i=1}^{n} a_i (v_i)^2 * \sum_{i=1}^{n} a_i (w_i)^2}} \qquad (1)$$

3.3. Çevrimdışı Öğrenme

IP trafiğinden geçen aynı uygulamaya ait akışların vektör uzay modeli kullanılarak karakteristiklerinin çıkartılması makine öğrenmesi tabanlı yaklaşımımızın öğrenme kısmını oluşturmaktadır. Öğrenme aşaması çevrimdışı olarak önceden toplanmış öğrenme veri kümesi ile yapılmaktadır. Bu işlem aşağıdaki aşamalardan oluşur:
1. Veri kümesi üzerindeki her bir ağ akışı port ve yük bazlı sınıflandırıcı ile ya da manuel olarak incelenir ve hangi uygulamaya ait olduğu tespit edilir. Her bir akışın gelen ve giden yönde ilk bir kaç paketinin paket uzunlukları kayıt altına alınır. Bu adımın sonunda her bir uygulama için o uygulamaya ait örneklerin gelen ve giden yönde ilk bir kaç paketine ait paket uzunlukları elde edilmiş olunur.
2. Daha sonra ise her bir uygulama için sahip olduğu örneklerin gelen ve giden yönde ilk bir kaç paketine ait paket uzunluklarının ortalaması alınarak gelen ve giden paket

uzunlukları vektörü, paket uzunluklarının standart sapması hesaplanarak da gelen ve giden standart sapma vektörü hesaplanır. Standart sapma vektörü de normalizasyondan geçirilerek normalize edilmiş standart sapma vektörü elde edilir.

Öğrenme aşamasının akış şeması Şekil 1'de verilmiştir.

Öğrenme aşamasında her bir uygulama için çıkartılan paket uzunlukları ve normize edilmiş standart sapma vektörlerinin matematiksel tanımlamaları aşağıdaki gibidir.

A uygulamasına ait örneklerin *S* kümesinde olduğunu varsayalım. *k* adet örnek içeren *S* kümesindeki herbir örnek ise *n* uzunluğundaki v_i vektörü olsun. Bu durumda *A* uygulamasının paket uzunlukları vektörü 2. denklem ile, standart sapma vektörü 3. denklem ile, normalize edilmiş standart sapma vektörü ise 4. denklem ile hesaplanır.

$$PktUzVek(A) =< a_1, a_2, ..., a_n >$$

$$a_i = \frac{\sum_{i=1}^{k} v_i}{k} \quad (2)$$

$$StdSapVek\ (A) =< s_1, s_2, \ldots, s_n >$$

$$s_i = \sqrt{\frac{\sum_{i=1}^{k} (v_i - a_i)^2}{k}} \quad (3)$$

$$NormStdSapVek(A) =< ns_1, ns_2, \ldots, ns_n >$$

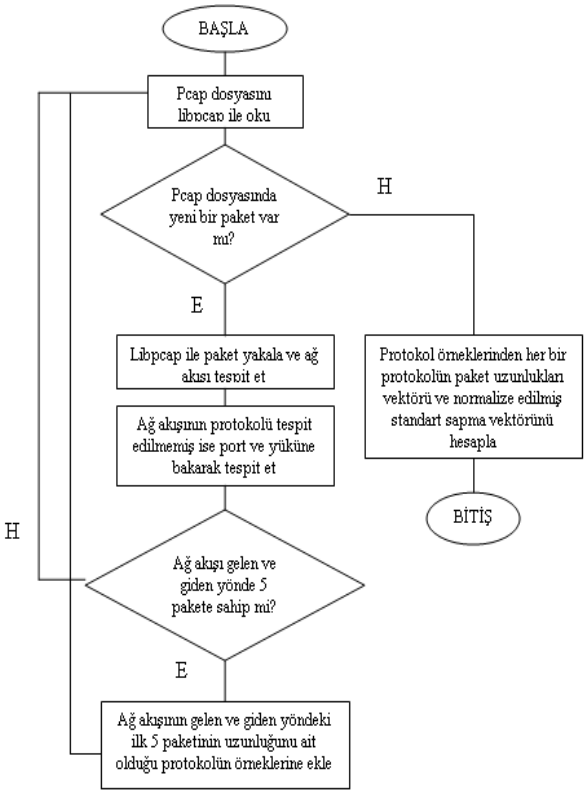
$$ns_i = \frac{1}{1 + s_i} \quad (4)$$

3.4. Çevrimiçi Sınıflandırma

Her bir uygulamaya ait karakteristikler çıkartıldıktan sonra yeni bir ağ akışının hangi uygulamaya ait olduğunu tespit etme makine öğrenmesi tabanlı yaklaşımımızın sınıflandırma aşamasını oluşturmaktadır. Bu aşama gerçek zamanda çevrimiçi olarak yapılmaktadır ve aşağıdaki adımlar ile gerçeklenmektedir:

1. Ağ üzerinde yeni bir akış tespit edilir.
2. Bu akışa ait ilk bir kaç paketin paket uzunlukları ile öğrenme aşamasında çıkartılan diğer uygulamaların paket uzunlukları vektörü ve normalize edilmiş standart sapma vektörü arasında ağırlıklı kosinüs benzerliği hesabı yapılır. Normalize edilmiş standart sapma vektörü kosinüs benzerliği hesaplamasında ağırlık olarak kullanılarak, öğrenme paket uzunluğu değişkenlik gösteren vektör elemanlarının benzerlik hesabında daha az etki yapması hedeflenmiştir.
3. Yapılan hesaplama sonucu kosinüs benzerliği en yüksek olan uygulama tespit edilen ağ akışına atanır. Böylece sınıflandırma aşaması tamamlanmış olur.

Algoritma Şekil 2'de verilmiştir.



Şekil 1: Öğrenme akış şeması

```
Yeni bir ağ akışı (X akışı) tespit et

Eğer ağ akışı gelen ve giden yönde 5 pakete ulaşmış ise
    Ağ akışının gelen ve giden paket uzunlukları vektörünü oluştur
    for karşılaştırma yapılacak her bir protokol (Proto(i)) için do
        Sonuç = Kosinus_Benzerliği (X, Proto(i))
        Eğer Sonuç > Maksimum ve Sonuç > Eşik Değeri ise
            Maksimum = Sonuç
            Proto X = Proto(i)

Kosinus_Benzerliği(X, Proto)
    Sonuç = 0, kare_X = 0, kare_Proto = 0
    for gelen ve giden paket uzunlukları vektörlerinin her bir elemanı (el(j)) için do
        sonuç += X_PktUz_el(j) * Proto_PktUz_el(j) * Proto_NStd_el(j)
        kare_X += X_PktUz_el(j) * X_PktUz_el(j) * Proto_NStd_el(j)
        kare_Proto += Proto_PktUz_el(j) * Proto_PktUz_el(j) * Proto_NStd_el(j)
    sonuç = sonuç / (kök(kare_X) * kök(kare_Y))
    return sonuç
```

Şekil 2: Trafik sınıflandırma algoritması

4. Deneysel Sonuçlar

4.1. Test Ortamı

Çalışma 64 bit FreeBSD 8.2 sistemi üzerinde test edilmiştir. C programlama dili ile geliştirilen ve libpcap paket toplama kütüphanesini kullanan test uygulaması hem ağ kartı üzerinden hem de pcap dosyaları aracılığı ile paket toplayabilmekte, öğrenme ve sınıflandırma işlemlerini yapabilmektedir.

Test için Naval Bilgisayar Bilimleri Bölümünün DEEP (Digital Evaluation and Exploitation) çalışma grubunun 2009

Kasım ve Aralık aylarında kayıt ettiği paket izleri [14] veri kümesi olarak kullanılmıştır. Bu paket izleri üzerinde port ve yük tabanlı olarak yapılan incelemede HTTP, HTTPS, SMTP ve FTP protokollerine ait 6485 ağ akışı tespit edilmiştir.

4.2. Performans Metrikleri

Trafik sınıflandırma yaklaşımlarının keskinliklerini karşılaştırmada kullanılan temel performans metrikleri şunlardır:

- *Yanlış Negatif* (YN): Üzerinde çalışılan uygulamaya ait olup yanlış tespit edilen ağ akışlarının yüzdesi.
- *Doğru Pozitif* (DP): Üzerinde çalışılan uygulamaya ait olup doğru tespit edilen ağ akışlarının yüzdesi (100 - YN).
- *Yanlış Pozitif* (YP): Üzerinde çalışılan uygulamaya ait olmayıp üzerinde çalışılan uygulama olarak tespit edilen ağ akışlarının yüzdesi.
- *Doğru Negatif* (DN): Üzerinde çalışılan uygulamaya ait olmayıp üzerinde çalışılan uygulama olarak tespit edilmeyen ağ akışlarının yüzdesi.

Bu çalışmada her bir uygulama için YN, DP, YP ve DN yüzdeleri hesaplanarak performans değerlendirmesi yapılmıştır.

4.3. Test Sonuçları ve Değerlendirme

Veri kümesi kullanılarak gerçeklenen öğrenme aşamasında hesaplanan HTTP, HTTPS, SMTP ve FTP protokollerinin karakteristiklerini oluşturan paket uzunlukları ve normalize edilmiş standart sapma vektörleri Tablo 1, Tablo 2, Tablo 3 ve Tablo 4' de verilmiştir.

Tablo 1: HTTP protokolü vektörleri

Vektör	Paket 1	Paket 2	Paket 3	Paket 4	Paket 5
Giden Paket Uzunlukları Vektörü	563.34	553.54	556.39	513.86	544.56
Giden Normalize Edilmiş Standart Sapma Vektörü	0.0023	0.0022	0.0022	0.0024	0.0022
Gelen Paket Uzunlukları Vektörü	740.98	621.57	759.85	613.45	724.14
Gelen Normalize Edilmiş Standart Sapma Vektörü	0.0027	0.0029	0.0025	0.0028	0.0025

Tablo 2: HTTPS protokolü vektörleri

Vektör	Paket 1	Paket 2	Paket 3	Paket 4	Paket 5
Giden Paket Uzunlukları Vektörü	1319.0	1276.5	1117.6	367.37	89.98
Giden Normalize Edilmiş Standart Sapma Vektörü	0.0041	0.0029	0.0021	0.006	0.0059
Gelen Paket Uzunlukları Vektörü	319.94	180.48	600.27	1128.2	991.56
Gelen Normalize Edilmiş Standart Sapma Vektörü	0.002	0.032	0.0023	0.0024	0.0018

Tablo 3: SMTP protokolü vektörleri

Vektör	Paket 1	Paket 2	Paket 3	Paket 4	Paket 5
Giden Paket Uzunlukları Vektörü	25	162.69	27.36	674.67	46.35
Giden Normalize Edilmiş Standart Sapma Vektörü	1	0.0435	0.1408	0.0029	0.0835
Gelen Paket Uzunlukları Vektörü	14.75	14.22	90.11	251.34	124.39
Gelen Normalize Edilmiş Standart Sapma Vektörü	0.2224	0.0891	0.0291	0.008	0.0041

Tablo 4: FTP protokolü vektörleri

Vektör	Paket 1	Paket 2	Paket 3	Paket 4	Paket 5
Giden Paket Uzunlukları Vektörü	64.51	64.77	51.77	27.62	26.85
Giden Normalize Edilmiş Standart Sapma Vektörü	0.0215	0.0972	0.0282	0.084	0.078
Gelen Paket Uzunlukları Vektörü	15.98	16.91	20.36	17.76	12.66
Gelen Normalize Edilmiş Standart Sapma Vektörü	0.7445	0.5202	0.0533	0.0411	0.0799

[15] de ilk 4 veya 5 paketin uygulamaların karakteristiklerinin ayırt edilmesinde daha belirleyici olduğunun tespit edilmesi üzerine testlerde ilk 5 pakete ait bilgiler kullanılmıştır.
Normalize edilmiş standart sapma vektörünün sınıflandırma performansına etkisini görmek amacıyla iki ayrı kosinüs benzerliği hesabı yapılmıştır. Bunlardan biri sadece paket uzunlukları vektörünü kullanmakta, diğeri ise normalize edilmiş standart sapma vektörünü benzerlik hesabında ağırlık olarak kullanmaktadır. Bu iki benzerlik hesabına ait sonuçlar Tablo 5 ve Tablo 6'da verilmiştir.

Tablo 5: Sadece paket uzunlukları vektörü ile kosinüs benzerliği sonuçları

	YN	DP	YP	DN
HTTP	%20.99	%79.01	%1.01	%98.99
HTTPS	%29.44	%70.56	%1.04	%98.96
SMTP	%21.22	%78.78	%0.083	%99.92
FTP	%14.24	%85.76	%8.5	%91.5

Tablo 6: Normalize edilmiş standart sapma ve paket uzunlukları vektörü ile kosinüs benzerliği sonuçları

	YN	DP	YP	DN
HTTP	%13.72	%86.28	%0.27	%99.73
HTTPS	%10.55	%89.45	%7.71	%92.29
SMTP	%5.00	%95.00	%0.00	%100.0
FTP	%8.84	%91.16	%9.75	%90.25

Benzerlik sonuçlarından normalize edilmiş standart sapma vektörünün DP değerini ortalama %12 arttırdığı görülmektedir. Ayrıca şifreli yüke sahip olan HTTPS protokolünde %19 gibi yüksek bir keskinlik artışı görülmesi ile yaklaşımımızın şifreli internet trafiğini de başarılı bir şekilde tespit edeceği düşünülmektedir.
SMTP protokolünün YP oranının sıfır olması karakteristiğinin diğer protokollerin karakteristiğine uzak olmasından kaynaklanmaktadır. Ayrıca HTTP ve HTTPS protokollerinin yanlış tespit edilen ağ akışlarının genelde FTP olarak tespit edildiği görülmektedir. Bu da HTTP ve HTTPS ile FTP ağ akışları arasında ortak bir karakteristikte ağ akışlarının bulunduğunu göstermektedir. Bunun sebebi ise HTTP ve HTTPS protokollerinin normalleştirilmiş standart sapma vektörlerindeki değerlerin düşük olmasıdır. Çünkü normalleştirilmiş standart sapma vektörlerindeki değerlerin düşük olması standart sapma değerlerinin yüksek olduğunu göstermektedir. Standart sapma değerleri ne kadar yüksek ise ağ akışlarının birbirlerine benzerlikleri de o kadar uzaktır.

5. Gelecek Çalışmalar

Çalışma aşamasındaki bazı kısıtlar gelecek çalışmalar için yol gösterici olmaktadır.
Bu kısıtlar öğrenme aşamasında çok önemli payı olan port ve yük bazlı sınıflandırıcımızın tespit edebildiği uygulama veya protokollerin sayısının, test verisinde bulunan ağ akışlarının ve protokollerinin sayısının az olmasıdır.
Daha fazla uygulama ve protokol desteğine sahip port ve yük bazlı sınıflandırıcı ve her protokol için bolca ağ akışına sahip test verisi yaklaşımımızın daha geniş çapta değerlendirilmesini sağlayacaktır.
Ayrıca şifreli protokoller için manuel olarak hazırlanacak test verileri yaklaşımımızın şifreli trafiğin tespit edilmesindeki başarısını belirlemede daha etkin bir rol oynayacaktır.

6. Sonuç

Bu çalışmanın sonuçları göstermektedir ki internet trafik sınıflandırmasında ağ akışlarının gelen ve giden yönde ilk bir kaç paketinin paket boyutları vektörleri ve bu vektörler üzerinde yapılan kosinüs benzerliği hesabı yüksek bir başarım sağlamaktadır. Yani ağ akışlarının paket boyutları vektörü protokollerin tespitinde ayırt edici özellik göstermektedir.
Protokollerin normalize edilmiş standart sapma vektörlerinin kosinüs benzerliği hesabında ağırlık olarak kullanılması ise trafik sınıflandırma performansını arttırmıştır.
Ayrıca yaklaşımımızın paket yüklerine bakmadan şifreli internet trafiğini yüksek bir başarım ile tespit edebileceği HTTPS trafiğinin tespitinde gösterdiği yüksek başarım yüzdesinden öngörülmektedir.

7. Kaynakça

[1] IANA, Internet Assigned Numbers Authority, http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml
[2] A. Moore ve K. Papagiannaki, “Toward the accurate identification of network applications”, *Proc. Passive and Active Measurement Workshop (PAM2005)*, Boston, MA, USA, Mart/Nisan 2005
[3] P.-C. Lin, Y.-D. Lin, T.-H. Lee, ve Y.-C. Lai. “Using string matching for deep packet inspection”, *IEEE Computer Practices*, 41(4):23–28, Nisan 2008.
[4] S. Sen, O. Spatscheck, ve D. Wang, “Accurate, scalable in network identification of P2P traffic using application signatures”, *WWW2004*, New York, NY, USA, Mayıs 2004.
[5] A. McGregor, M. Hall, P. Lorier, ve J. Brunskill, “Flow clustering using machine learning techniques”, *Proc. Passive and Active Measurement Workshop (PAM2004)*, Antibes Juan-les-Pins, Fransa, Nisan 2004
[6] S. Zander, T. Nguyen, ve G. Armitage, “Automated traffic classification and application identification using machine learning”, *IEEE 30th Conference on Local Computer Networks (LCN 2005)*, Avustralya, Kasım 2005.
[7] L. Bernaille, R. Teixeira, I. Akodkenou, A. Soule, ve K. Salamatian, “Traffic classification on the fly”, *ACM Special Interest Group on Data Communication (SIGCOMM) Computer Communication Review*, vol. 36, no. 2, 2006.
[8] J. Erman, A. Mahanti, M. Arlitt, ve C. Williamson, “Identifying and discriminating between web and peer-to-peer traffic in the network core”, *WWW ’07: Proceedings of the 16th international conference on World Wide Web*. Banff, Alberta, Canada: ACM Press, Mayıs 2007, sayfa 883–892.
[9] M. Roughan, S. Sen, O. Spatscheck, ve N. Duffield, “Class-of-service mapping for QoS: A statistical signature-based approach to IP traffic classification”, *Proceedings of ACM/SIGCOMM Internet Measurement Conference (IMC) 2004*, Taormina, Sicily, İtalya, Ekim 2004.
[10] A. Moore ve D. Zuev, “Internet traffic classification using Bayesian analysis techniques”, *ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS) 2005*, Banff, Alberta, Kanada, Haziran 2005.
[11] T. Auld, A. W. Moore, ve S. F. Gull, “Bayesian neural networks for Internet traffic classification”, *IEEE Transactions on Neural Networks*, no. 1, sayfa. 223–239, Ocak 2007.
[12] M. Crotti, M. Dusi, F. Gringoli, ve L. Salgarelli, “Traffic classification through simple statistical fingerprinting,” *SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 1, sayfa 5–16, 2007.
[13] J.Y. Chung, B. Park, Y.J. Won, J. Strassner ve J.W. Hong, "Traffic Classification Based on Flow Similarity", *IPOM 2009*, LNCS 5843, sayfa 65-77, 2009
[14] DEEP (Digital Evaluation and Exploitation) Paket İzleri, https://domex.nps.edu/corp/scenarios/2009-m57/net/, Department of Computer Science, Naval Postgraduate School, Monterey, CA, 2009
[15] J. Erman, M. Arlitt, A. Mahanti, “Traffic Classification Using Clustering Algorithms”, *SIGCOMM06 Workshops*, Pisa, Italya, 2006

IPv4 / IPv6 Güvenlik Tehditleri ve Karşılaştırılması

Ayhan Çakın[1] Muhammed Ali Aydın[2]

[1]Enformatik Bölümü, Yıldız Teknik Üniversitesi, İstanbul
[2]Bilgisayar Mühendisliği Bölümü, İstanbul Üniversitesi, İstanbul

[1]e-posta: acakin@yildiz.edu.tr [2] e-posta: aydinali@istanbul.edu.tr

Özetçe

Günümüzde hızla artan ağ ve ağ elemanları göz önüne alındığında, mevcut internet protokolü IPv4; gerek yetersiz adres sayısı, gerekse dahili güvenlik tasarımı açısından sorunlara yol açmaktadır. IPv6 yeni nesil internet protokolü olarak, eski protokoldeki sorunları çözmek üzere sunulmuştur. IPv6 başından beri güvenlik mekanizmaları ve bu mekanizmaları iki uçtaki konağın kontrolünde olmasını sağlamak üzere tasarlanmaktadır. Ancak henüz yeni bir protokol oluşu ve çokça kullanılmayışı, yayılmaya başladığında ne gibi sorunlara yol açabileceğini kestirmek zordur. Bu çalışmada ilk olarak IPv4'de ortaya çıkan ve IPv6 üzerinde de geçerli olan ortak tehditlerden, ikinci bölümde ise IPv6'nın yayılmaya başlaması ile ortaya çıkabilecek güvenlik sorunlarından bahsedilmektedir.

Anahtar Kelimeler: *IPv6, IPv4, IP Tehditleri, IP Güvenliği*

1. Giriş

Bilindiği üzere, mevcut internet protokolü IPv4 yetersiz adres uzayı ve güvenlik açıkları gibi sorunlarla yüzleşmektedir. Bu ve benzeri sorunları temel alarak, IETF (Internet Engineering Task Force) bunları giderebilecek yeni bir protokol için çalışmalar başlatmıştır. IPv6 olarak anılan bu yeni protokol, dahili güvenlik önlemleri, ağ yönetimi araçları ve konfigürasyon kolaylığı temel alınarak birçok RFC(RFC 1752, 2460, 2462 vb.) ile tanımlanmıştır.

IPv4'ü genel olarak değerlendirdiğimizde, iki ana sorun ile karşılaşılmaktadır. En büyük problemlerden birincisi, IPv4'ün sunabildiği adres uzayının sınırlı olması ve günümüzde neredeyse tükenmek üzere olduğudur. İlk başta yaklaşık 4 milyar adres uzayına sahip olarak tasarlanan IPv4, kablosuz ağ bileşenleri, hücresel ağların gelişimi ile yetersiz kalmıştır.

İkinci önemli sorun ise güvenliktir. IPv4 tasarlandığı dönemde "uçtan uca" modeli benimsemiş ve internet "güvenli" bir ortam olarak düşünülmüştür.[1] Bu yüzden hiçbir dahili güvenlik bileşeni olmadan tasarlanmıştır. Uçtan uca olarak tasarlanmış modeli, güvenliğin uçlardaki konaklarda sağlanması üzerine kurulmuş ve güvenlik opsiyonu da sonradan bu amaç ile protokole eklenmiştir. Bu tasarımın doğurduğu açıkları uygulama bazında kapatmak amacı ile PGP ve SSL gibi önlemler alınmaya çalışılsada, tam olarak uçtan uca güvenli bir iletişim sağlanamamaktadır. Örneğin IPv4 ün ötentikasyon mekanizmaları tarafında olan eksikliği ortadaki adam saldırılarına, zayıf tasarımı ve dar adres alanı ile konakların taşırma, servis dışı bırakma ve özellikle keşif tipi(portların kısa sürede taranabilmesinden faydalanılarak) saldırılarılara mağruz kalmasına yol açmaktadır.

2. IPv6'daki Değişiklikler

IPv6'nın esas tanımlamaları; RFC 2460 (Deering & Hinden,1998) IPv6 Protocol, RFC 4443 (Conta, Deering & Gupta, 2006) Internet Control Message Protocol for IPv6 (ICMPv6),

RFC 4291(Hinden & Deering, 2006) IPv6 Addressing Architecture gibi RFC dökümanları ile belirlenmiştir. IPv4 ile arasındaki bazı farklar Tablo 1'de gösterilmiştir.

IPv4	IPv6
32 bit Adres Uzunluğu	128 bit Adres Uzunluğu
IPsec kullanımı seçeneğe bağlıdır.	IPsec uygulama desteği mecburidir.
IPv4 başlığında paket akışını tanımlamak için yönlendiricilerin kullanabileceği ortak bir standart QoS tanımlamaları yoktur.	Başlıkta bulunan "flow label" alanı yönlendiriciler tarafından kullanılır.
Paketin parçalanması işlemi (fragmentation) hem ağdaki ara elemanlar hem de gönderici tarafından yapılabilir.	Paketin parçalanması işlemi (fragmentation) yönlendiriciler tarafından yapılmaz. Sadece paketi gönderen istemci tarafından yapılır.
Checksum vardır.	Checksum içermez.
Seçenekler alanı bulunur.	Seçimli veriler extension header'lar ile taşınır.
ARP kullanılır.	ARP Request paketleri multicast Neighbor Solicitation mesajlarıyla değiştirilmiştir.
Varsayılan en iyi ağ geçidi tespiti için, ICMP Router Discovery kullanılabilir, fakat zorunlu değildir.	ICMP Router Discovery yerine "ICMPv6 Router Solicitation" ve "Router Advertisement" kullanılır ve kullanımı zorunludur.
Ağdaki tüm birimlere "broadcast" adresleri ile erişilir.	IPv6 "broadcast" adresi bulunmamaktadır. Bunun yerine "link-local scope all-nodes multicast" adresi kullanılır.
DHCP server yardımı ile veya elle yapılandırılır.	Otomatik olarak yapılandırılır.

Tablo 1. IPv4 ve Ipv6 Karşılaştırılması

3. IPv4 ve IPv6'daki Benzer Güvenlik Tehditleri

Yeni protokol tasarımı ile gelen güvenlik önlemleri olsa da, IPv6 ağları halen farklı tipte ataklara maruz kalabilmektedir. Bu ataklar üzerinde birçok çalışma mevcuttur [2][3][4]. Bazı atak türleri IPv6 ile değişmiş ve bu protokole özel saldırı türleri bulunmaktadır, ancak IPv4 için mevcut olan tüm saldırı türleri değişmemiş ve bu saldırı mekanizmaları IPv4 ve IPv6 ağları için tehlike oluşturmaktadır.

3.1 Paket Koklama

Paket koklama saldırısı basitçe ağda gezen verinin yakalanıp incelenmesi olarak tanımlanabilir. Koklama atakları hem IPv6 hem de IPv4 üzerinde etkili olan en tipik saldırı biçimidir. IPv4 de veriler ağda şifrelenmeden dolaştığı için saldırı çok çabuk sonuç vermekteydi. Ancak yeni protokolün tanımına göre, IPv4 de yalnızca bir seçenek olan IPSec[5] özelliği, IPv6 da dahili olarak desteklenmek zorundadır. Bu özellik ile veriler uçtan uca şifrelenmiş şekilde transfer edilmekte, paket aradaki bir konakta yakalanıp incelense bile şifreli olacağı için güvenlik açığı kapatılmış olmaktadır. Buradaki önemli nokta, IPv6'da IPSec desteği zorunludur ancak kullanılması tamamen isteğe bağlıdır. Anahtar paylaşımı ve konfigürasyonu gibi karışık konulardan dolayı IPSec özelliğinin IPv6'daki kullanımın eski protokolden daha fazla olup olmayacağı bir soru işaretidir.[6]

3.2 Ortadaki Adam Saldırıları

Bilgisayarın meşruluğu ağ yapısında yada işletim sistemi tarafında IP kurallarına göre belirlenmektedir. Bazı durumlarda IP adresi saldırı yapan bir kişi tarafından taklit edilmekte/uydurulmaktadır (forged ID)[7]. Bu sahte IP'yi kullanarak saldırgan meşru konaktan gelmiş gibi bir paket gönderebilir. Gerekli yetkileri kazandıktan sonra, saldırgan gelen paketlerdeki veriyi birçok yöntemle yönetebilir, yeniden yönlendirebilir veya değiştirebilir.

3.3 Taşırma Saldırıları

Taşırma saldırıları IPv4 ağlarını en çok istismar eden saldırı türü olarak bilinmektedir. Bu tarz saldırılar IPv6 için de geçerli olacaktır. Ağ üzerindeki hedefe kaldırabileceğinden daha fazla istek göndererek hizmet vermesini belirli bir süre boyunca engelleme yöntemi IPv6 için de geçerli olacaktır. Saldırı; bölgesel ya da dağınık hizmet dışı bırakma(DDos) yani farklı makinelerin aynı anda tek bir hedefe istek göndermesi ile uygulanmaktadır. IPv6 ağlarında, bu tarz atakları ağı analiz ederek tespit etmek daha da zorlaşmaktadır. Çünkü IPv6 ile adres uzayı büyümüş ve sahte IP'lerin tespiti zorlaşmıştır.

3.4 Uygulama Seviyesi Saldırıları

Günümüzün en yaygın saldırı türlerinden olan uygulama seviyesi saldırıları, CGI saldırıları, solucan dağılımı, hafıza taşırma gibi saldırıları içermektedir. IPv6'ya geçiş ne yazık ki ağları bu tarz saldırılardan koruyamamaktadır. Çünkü bu saldırıların

hepsi uygulama seviyesindedir. IPv4 ve IPv6 protokolleri ise OSI modelinin ağ düzeyinde işlemektedir.

3.5 ARP, DCHP Saldırıları, Sahte Cihazlar

IPv6 protokolü tanımlanırken, ARP ve DHCP'nin bu protokoldeki karşılıkları ile ilgili dahili bir güvenlik mekanizması eklenmemiştir.[8] Yönlendirici ve komşu istek paketleri sahte olarak üretilip bunlarla komşu tanımlama önbelleğinin üzerine yazılıp, IPv4 deki ARP sorunları tekrarlanmaktadır. Bunlara ek olarak, sahte cihazlar, ağ üzerinde yetkisi olmayan cihazların kablosuz erişim noktası, DHCP sunucusu veya basit bir bilgisayar olarak tanımlanan cihazlardır. Bu cihazların tespit edilmesi için bazı yöntemler bulunmaktadır. Ancak IPv6'da hiçbirisi değişmemiştir. Fakat IPSec özelliğinin IPv6 ağlarında etkin bir şekilde uygulanması ve cihazların yetkilendirilmesi ile bu atakların tespiti bir şekilde mümkün olabilecektir.

4. IPv6 ile Gelen Güvenlik Tehditleri

4.1 Keşif Tipi Saldırılar

Keşif saldırıları bir saldırı türü olmaktan çok, bir saldırının başlangıç aşaması olarak görülebilir. Bir saldırı yapmadan önce ağı analiz etmek ve ağdaki cihazları tanımlamak için kullanılır. Saldırgan çeşitli tarama metotlarını kullanarak hedef ağdaki IP adreslerini belirler ve daha sonra ağdaki cihazlara özel port taraması gibi işlemlere başlar.

Yeni internet protokolünü ele aldığımızda, saldırganlar için tüm ağı taramak neredeyse imkansız hale gelmiştir. Çünkü IPv6'da alt ağ sayısı IPv4'e göre çok büyüktür(64 bit). Buna dayanarak IPv6 ağları keşif saldırılarına daha dayanıklı denilebilir. Ancak IPv6'da bulunan bazı çoklu gönderim adresleri saldırganlar tarafından kullanılarak ağdaki cihazların tespiti ve saldırı amacıyla kullanılabilir.

4.2 ICMPv6

IPv4 ağlarında ağın diğer fonksiyonlarına zarar vermeden ICMP mesajlarını engellemek mümkün olduğundan, bu uygulama zamanla güvenlik sebebiyle sürekli uygulanmaya başlandı. Ancak IPv6'nın tanımlanması ile birlikte, ICMPv6'nın MTU ve komşu tanımlama gibi çok önemli mekanizmalarda kullanıldığı görüldü. Buna bağlı olarak, ağın düzgün bir şekilde işlemesi için ICMPv6 mesajlarının engellenmemesi gerekmektedir. Ancak ICMPv6 tanımlamasındaki en önemli güvenlik açığı olarak; hata mesajlarının hedef adreslerinin çoklu gönderim adresi olarak tanımlanmasına izin vermesidir. Bu özellik bir saldırgan tarafından kolayca istismar edilebilir.

4.3 Ek Başlıklar ile İlgili Tehditler

IPv6 tanımlamasına göre IPv6 ağındaki bütün cihazlar yönlendirme başlıklarını işleyebilmelidir. Bu davranış; hedef adres temel alınarak yetkisiz erişim gibi bazı güvenlik açıklarına yol açabilir. Bir senaryo oluşturarak örnek vermek gerekirse: Bir saldırgan açık bir ağ üzerindeki bir cihaza, yönlendirme başlığında o cihaz üzerinde önceden yasaklı olarak belirlenmiş bir paket yolluyor. Normal koşullar altında bu paketin süzülmesi gerekirken, bu cihaz gelen paketi otomatik olarak iletmektedir. Saldırgan sahte IP adresleri üzerinden açık ağdaki bu cihazı kullanıp gönderdiği paketleri iletmesini sağlayarak hizmet dışı bırakma saldırısı yapabilir. Burada bilinmesi gereken bazı işletim sistemlerinin yönlendirme başlığı olan paketleri otomatik olarak ilettiği, diğerlerinin ise iletmediğidir.

4.4 Başlık Yönetimi ve Parçalama

IPv6 protokolü tanımına göre[9], MTU keşif metodu zorunlu tutulmuş ve paketin parçalanma işleminin aradaki cihazlarda yapılması engellenmiştir. Birçok ek başlık seçeneğinin kullanılması ile birlikte, bugün ağdaki orta elemanlar tarafından yapılan paketlerin yeniden birleştirilmesi işleminde sorunlar çıkması muhtemeldir.

4.5 Tünelleme ve Geçiş Mekanizmaları

IPv4 ağlarının devasa boyutunu ele aldığımızda, IPv6 ağlarına geçişin birçok uyum sorunu sonucunda yavaş olacağı görülmektedir. Bu süreci daha yumuşak hale getirmek için birden fazla geçiş mekanizmaları geliştirilmiştir. Ancak bu mekanizmalar şirketlerin yanlış konfigürasyonu, tünel metotları ve iki protokolün(IPv4 ve IPv6) beraber kullanılması gibi etkenler sonucunda şuanda tahmin edilemeyen yeni güvenlik açıkları doğuracaktır. Bu yüzden IPv6 ağlarına geçiş süreci ağ yöneticileri tarafından dikkatle değerlendirilmelidir.

5. Sonuçlar

Bu çalışmada IPv6 protokolü üzerinde getirdiği faydalı yönler ve eksikleri ile ilgili genel bir değerlendirme yapmaya çalıştık. IPv6; mevcut protokoldeki sorunları çözmeye yönelik tasarlanmış olsa da, güvenlik penceresinden henüz tartışılması gereken birçok nokta bulunmaktadır. IPSec özelliğinin uygulanma desteğinin zorunlu hale getirilmesi, paketlerin ağdaki orta elemanlarda parçalanmasına izin verilmemesi, adres uzayının genişletilmesi ve NAT kullanımının azaltılmaya teşvik edilmesi, IPv6 ile gelen ve bu protokolü daha güvenli bir uygulama hale getiren yönlerden sadece birkaçıdır. Ancak daha yeni bir protokol olması ve şuanda uygulamasının az olması nedeniyle, yayılması anında çıkabilecek sorunlar halen araştırılmaktadır. Şu anki tasarımın daha derin analizi ve yukarıda tartıştığımız konuların incelenmesi ile IPv6 ağlarına geçiş çok daha hızlı ve sorunsuz olacaktır.

6. Kaynakça

[1]. S. Sotillo, “IPv6 Security Issues”, 2006.

[2]. Q Zheng, T. Liu, G. Xiaohong, X.,Q. Yu, N. Wang N, “A new worm exploiting IPv4-IPv6 dual-stack networks,” Proceedings of the 2007 ACM workshop on Recurring malcode, Virginia, 2007

[3]. D. Zagar, K. Grgic, “IPv6 security threats and possible solutions,” World Automation Congress, 2006

[4]. Y. Xinyu, M. Ting, S.Yi, “Typical DoS/DDoS threats under IPv6,” Computing in the Global Information Technology, Guadeloupe, 2007

[5]. Kent & Seo, IETF RFC 4301 “Security Architecture for IP or IPsec”, 2005

[6]. Y.Nikolopoulos, “Security Considerations for IPv6 Networks”, March 2011

[7]. D. Yang, Xu Song, Qiao Guo, “Security on IPv6”, 2010

[8].V.Sharma,”IPv6 and IPv4 Security challenge Analysis and Best- Practice Scenario”, Jan 2010

[9]. Deering & Hinden, IETF RFC 2460 “Internet Protocol, Version 6 (IPv6) Specification”, 1998

3. KISIM: KRİPTOLOJİ

Bilgi Güvenliğinde Kuantum Teknikler

Mustafa Toyran[1] Thomas B. Pedersen[2] A. S. Atilla Hasekioğlu[3]
M. Ali Can[4] Savaş Berber[5]

[1-4]UEKAE, BİLGEM, TÜBİTAK, Gebze, Kocaeli
[5]Fizik Bölümü, GYTE, Çayırova, Kocaeli

[1]e-posta: mustafa.toyran@uekae.tubitak.gov.tr [2]e-posta: pedersen@uekae.tubitak.gov.tr
[3]e-posta: atilla@uekae.tubitak.gov.tr [4]e-posta: can@uekae.tubitak.gov.tr
[5]e-posta: savasberber@gyte.edu.tr

Özetçe

Bu bildiride Kuantum Mekaniği'nin günümüz Bilgi Güvenliği Sistemleri'ne etkisi incelenmeye çalışılacaktır. Bilgi güvenliği, Kriptografi biliminin sahasına giren bir konudur. Modern kriptografide güvenliğin bağlı olduğu başlıca parametre "gizli anahtar"dır. Gizli anahtar, rasgele seçilen, yeterince uzun, sadece bilgi alış-verişi yapanlarca bilinmesi gereken bir bit dizisidir. Gizli anahtar ile ilgili en önemli konular üretimi, dağıtımı ve yönetimidir. Diğer taraftan, modern Kriptanaliz eldeki bütün imkanları kullanarak gizli anahtarı ele geçirmeye çalışır. Modern kriptanaliz, modern kriptografide de olduğu gibi, daha çok Matematik'e ve Klasik Fizik'e dayanmaktadır. En son gelişmelere göre kuantum mekaniği de, özellikle bilgi güvenliğini de ilgilendiren bu konularda, bizlere daha önce bir benzeri görülmemiş birçok olumlu-olumsuz uygulamalara olanak sağlamaktadır.

1. Giriş

Bilgi güvenliği, bilginin ***iletim***i ve ***saklanma***sı esnasında güvenliğinin sağlanmasıdır[1]. İnsanlar çok eski zamanlardan beri [1] daima ***gizli bilgi***lerini ***meraklı***lardan gizleme ihtiyacı duymuştur[2]. Bunu yapmak için kullandıkları temel *araç* ya onları hiç kimsenin bulamayacağı bir yerlere *saklamak* ya da ele geçse dahi gerçek alıcısı dışındaki herkesin ondan birşey anlayamayacağı şekilde *anlamsız hale getirmek* olmuştur.

Bilgiyi hiçbir işleme tabi tutmadan olduğu gibi saklamaya dayalı çözümler ***steganografi*** (*steganography*, aslen Yunanca olan *steganos*: *saklı* ve *gráphein*: *yazı yazma* sözcüklerinin yan yana gelmesinden oluşmaktadır [2]) adlı bilim dalının konusudur. Örneğin, İkinci Dünya Savaşı sırasında kullanılan *mikronokta* yöntemi bir steganografi tekniğidir. Bu teknikte gönderici taraf göndermek istediği mesajın önce resmini çeker, sonra bu resmi bir nokta boyutuna kadar küçültür ve bu noktayı sahte bir mesajın, örneğin en son cümlesinin, sonuna yerleştirirmiş. Alıcı tarafta ise bu nokta bulunup tekrar büyütülerek gerçek mesaj okunurmuş. Steganografide bilgi olduğu gibi saklandığından ve bulunduğunda da kolayca okunabildiğinden güvensiz olabilmektedir. Mesajı *görünmez mürekkeple yazma*, mesajı *yazıp sonra onu yutma*, *vücudun görünmeyen kısımlarına yazma*, *ses/görüntü/video* ya da *başka bir mesaj içine saklama*, vb. yöntemler de çeşitli steganografi teknikleridir. Anlaşılacağı üzere tüm bu yöntemlerde mesajın anlamı üzerinde bir değişiklik olmamakta, mesaj olduğu gibi saklanmaya çalışılmaktadır. Steganografinin kriptografiye başlıca üstünlüğü daha az dikkat çekmesi olarak söylenebilir. Ayrıca, kriptografi kullanımına yasal olarak izin verilmeyen kimi yerlerde steganografi kullanımı daha avantajlı veya tek yol da olabilir. Ancak, kullanımı daha ***risk***li bir yöntemdir.

Bilginin birtakım *yerine koyma* (*substitution*) [3], *yer değiştirme* (*transposition*)[4] ya da *matematiksel* (*asal sayılar*, *eliptik eğriler*, *sonlu cisimler*, *modüler aritmetik*, *çarpma*, *üs alma* gibi) işlemler ile görünümünün değiştirilip anlamsız hale getirildiği geriye dönüşümlü yöntemler ise ***kriptografi*** (*cryptography*, aslen Yunanca olan *kryptós*: *gizli* ve *gráphein*: *yazı yazma* sözcüklerinin yan yana gelmesinden oluşmaktadır [3]) biliminin konusudur. Bu bilim, bilgi güvenliğini sağlamak üzere yapılan *şifreleme* (anlamsız hale getirme) ve *şifre çözme* (tekrar anlamlı hale getirme) çalışmaları ile ilgilenmektedir. Kriptografide şifreli bilgi ele geçse bile meraklı kimse bundan hiç birşey anlayamayacaktır. Şifreli bilgiden asıl bilgiyi elde etmesi ise, günümüz ***Matematik bilgisi*** ve ***bilgisayar hesaplama gücü*** ile, *neredeyse* imkansızdır. Bu nedenle, bilgi güvenliği için çoğunlukla modern kriptografik tekniklerden yararlanılır. Modern kriptografinin bilgi güvenliğini sağlamaya yönelik olarak sunduğu başlıca ***servis***leri şunlardır: ***gizlilik***, *bütünlük*, *kimlik doğrulama* ve *inkarın önüne geçme*. İhtiyaç duyulan bilgi güvenlik düzeyine ulaşmak için pratikte bu servislerin birinden, birkaçından veya hepsinden birden yararlanmak gerekebilir. ***Bilgi güvenliği***, *başkası tarafından dinlenme*, *bilginin içeriğinin değiştirilmesi*, *kimlik taklidi* ve *inkar etme* gibi ***tehdit***lerin ortadan kaldırılması ile sağlanır ve günümüzde bu amaçla kullanılan temel araç kriptografidir.

Kriptografi ile steganografinin birlikte kullanıldığı uygulamalar da bulmak mümkündür: örneğin, bilgi önce şifrelenerek anlamsız hale getirilir, daha sonra şifreli bilgi bir dijital görüntü dosyasının içinde saklanır (bu işlem saklanacak bilgiye ait bilgi *bit*lerinin, görüntüyü oluşturan *piksel*ler denen görüntü birimlerinin, örneğin en düşük anlamlı bitlerine yerleştirilmesiyle yapılabilir) ve *iletişim kanalı*ndan da bu görüntü dosyası gönderilirse hem kriptografik hem de steganografik bir uygulama elde edilmiş olur. Böylesi bir çözüm, bilginin önce kriptografik tekniklerle gizlendiği ve

[1] Bilginin, ***işlenme***si esnasında ***bilgisayar virüsü***, ***truva atı*** gibi ***casus yazılım***lara karşı (*güncel* ***antivirüs*** yazılımları kullanmak yoluyla) korunması gerektiği de unutulmamalıdır. Daha genel olarak, bilginin tüm ***casusluk*** türü ***iç***/***dış*** saldırılara karşı da korunması gerekir.

[2] ***Ulusal*** (askeri, diplomatik, vb.) ya da ***bireysel*** (banka hesap ***şifre***leri, özel hayata ilişkin ***sır***lar, vb.) çok ***değerli varlık***ların ***düşman***lar eline geçmesinin doğurabileceği kötü sonuçları düşününüz.

[3] İlk örneği olarak kabul edilen Roma'lıların ***Sezar şifresi***nde her harf alfabede kendisinden sonraki 3. harf ile yer değiştirmekteydi.

[4] *Permutation* da denir. İlk örneği, eski Yunan'lıların, özellikle de Sparta'lıların, kullandığı söylenen ***Scytale*** *cihazı*dır.

arkasından steganografik tekniklerle saklandığı bir yazı yazma yöntemini ifade etmektedir. Steganografi tek başına güvensiz bir teknik olmasına karşın kriptografik tekniklerle birlikte kullanıldığında tüm sistemin güvenliğinin daha fazla artmasına ***katkı**da* bulunabilir (meraklının önce şifreli mesajı bulması gerekecektir!). Ancak, çalışmamızda bundan sonraki incelemelerimiz daha çok modern kriptografi ve kuantum mekaniğinin günümüz modern kriptografik bilgi güvenlik sistemleri'ne ***etkisi***ni incelemek üzerine yoğunlaşacaktır.

Bildirinin sonraki kısımlarında sırasıyla şu konular ele alınmaktadır: Bölüm 2'de ve Bölüm 3'te sırasıyla *modern kriptografi* ve *kuantum mekaniği* bilimleri hakkında temel bilgiler verilmektedir. Daha sonra, Bölüm 4'te *kuantum rasgele sayı üretimi*, Bölüm 5'te *kuantum kriptografi* ve Bölüm 6'da *kuantum kriptanaliz* konuları ele alınmaktadır. Son olarak, Bölüm 7'de *sonuçlar* yer almaktadır.

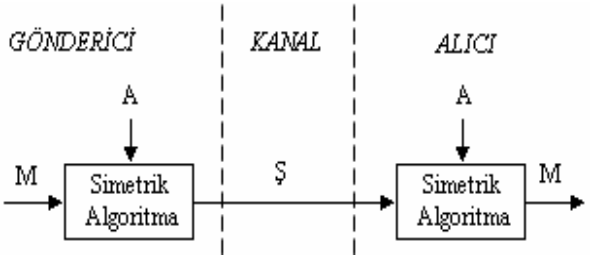
2. Modern Kriprografi

Kriptografinin ***gizlilik*** servisi bilginin gerçek alıcısı dışındaki kimseler tarafından asla anlaşılamamasını ***garanti***ler. Yani, örneğin, sizden başka hiçbir kimsenin size gönderilmiş olan bir elektronik postayı asla okuyamaması gibi. Bu amaçla, kullanılan başlıca yöntem bilgiyi ***şifreleme***dir.

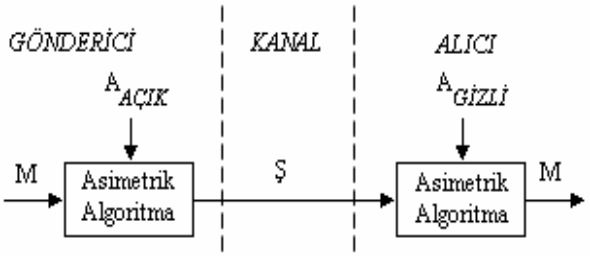
Günümüzde yaygın olarak kullanılan iki tür şifreleme sistemi bulunmaktadır [4]: ***Simetrik*** ve ***Asimetrik*** şifreleme sistemleri. Simetrik sistemlerde tek bir ***gizli anahtar*** vardır (bkz. Şekil 1.a). Hem *gönderici* hem de *alıcı* şifreleme ve şifre çözme işlemleri için aynı gizli anahtarı kullanır. Simetrik sistemler oldukça ***hızlı*** olup şifrelemede öncelikli olarak tercih edilirler. ***Vernam şifresi***, *DES*, *AES*, *IDEA*, *RC4*, vb. en çok bilinen ve kullanılan simetrik şifreleme algoritmalarıdır.

Asimetrik sistemlerde ise ***açık anahtar*** ve ***gizli anahtar***[1] olarak adlandırılan iki farklı anahtar kullanılır (bkz. Şekil 1.b). Her kullanıcı bu anahtar çiftinden kendisine has olan bir tanesine sahiptir. Şifreleme için *açık anahtar* kullanılır ve herkese açıklanmasında bir mahsur yoktur. Şifre çözme için ise *gizli anahtar* kullanılır ve sahibi dışında başka hiç kimse bilmemelidir. Açık anahtarla şifrelenen bir bilgiyi sadece ilgili gizli anahtar, yani o açık ve gizli anahtar çiftinin sahibi, çözebilir. Tersi de geçerlidir; ancak, açık anahtar herkesçe bilindiğinden, gizli anahtarla şifrelenen bir bilgiyi herkes çözebilecek ve okuyabilecektir. Asimetrik sistemler ***yavaş*** olmaları nedeniyle daha çok kısa uzunluktaki mesajları şifrelemede tercih edilir[2]. ***RSA***, *Diffie-Hellman*, *ElGamal* ve *DSS* en çok kullanılan asimetrik şifreleme algoritmalarıdır.

Yukarıda sözü geçen ***anahtar*** kelimeleri şifreleme ve şifre çözme işlemlerinde kullanılan elektronik bir bilgi (*bit dizisi*) anlamındadır. Anahtarlar olmadan şifreleme ve şifre çözme işlemlerini gerçekleştirmek mümkün değildir. Anahtarlar, *şifreleme* ya da *şifre çözme* ***algoritma***sı ile birlikte kullanılarak iletilecek olan bilgiler gönderici tarafta önce şifrelenirler ve alıcı tarafta da tekrar çözülürler. Algoritmaları, tanımlarını ve hatta gerçeklemelerini, rahatlıkla İnternet'te, kitaplarda, dergilerde, vb. pek çok herkese açık ortamlarda bulmak mümkündür. Modern kriptografide algoritmaların gizli olmadığına dikkat ediniz. Algoritmalar herkese açık olup asıl gizlenen parametre, *gizli anahtar*dır. ***Kerckhoff Yasası*** ("*Gizli olması gereken sadece anahtardır.*" [5]) ve ***Shannon***'un ünlü "*Düşman, sistemi bilir.*" sözü de bunu ifade eder [6,7].



***M**: mesaj.*
***A**: **gizli anahtar**.*
***Ş**: şifreli mesaj.*
a)



***M**: mesaj.*
***A**$_{AÇIK}$: **alıcı**nın **açık anahtarı**.*
***A**$_{GİZLİ}$: **alıcı**nın **gizli anahtarı**.*
***Ş**: şifreli mesaj.*
b)

Şekil 1: Kriptografi, *a*) ***Simetrik kriptografi***: gönderici ve alıcı *aynı* gizli anahtarı kullanır. *b*) ***Asimetrik kriptografi***: gönderici ve alıcı *farklı* anahtarlar kullanır.

Modern kriptosistemler ***gizli anahtar***ların *varlığı*na ve *gizliliği*ne güvenmektedir. Güvenliğin bağlı olduğu başlıca parametre gizli anahtardır: ***rasgele*** seçilen, yeterince ***uzun***, sadece bilgi alış-verişi yapanlarca bilinmesi gereken ***gizli*** bir bit dizisi. Sadece gizli anahtar bilinirse, tüm şifreli bilgilerin kolaylıkla çözülebilmesi özelliğine sahiptirler. Gizli anahtar ile ilgili en önemli konular ise ***üretim***i, taraflar arasında güvenli ***dağıtım***ı ve beşikten mezaradek güvenli ***yönetim***idir.

Öncelikle, çok güvenilir ***üreteç***lere ihtiyaç vardır; öyle ki, gizli anahtar asla *tahmin edilemez* olmalıdır (***üretim***). Sonraki aşama, üretilen anahtarların kullanacaklara *güvenli* bir şekilde *ulaştırılması*dır (***dağıtım***). Son aşama, *kullanılan* anahtarların güvenli bir şekilde *imha* edilmesidir (*yönetim*).

3. Kuantum Mekaniği

Kuantum (*quantum*, aslen Latince olan *quantus*: *ne kadar* sözcüğünden gelmektedir) ***mekaniği***, ***atom***ların ve ***atom-altı*** (*çekirdek*, *elektron*, *foton* gibi *mikroskopik*) ***parçacıklar***ın tarifine olanak veren ***fizik yasaları***nın temelidir[3]. Kuantum mekaniğinin keşfi, ısıtılan cisimlerin ışımasını açıklamak için 1900 yılında önerilen Planck yasası (Max Planck: 1858-1947) ile başlar. Gelişimi, Albert Einstein (1879-1955), Niels Bohr (1885-1962), Werner Heisenberg (1901-1976), Max Born

[1] ***Private key***. Türkçe'mize daha çok ***özel anahtar*** olarak da çevrilir.
[2] ***Elektronik imza***, ***gizli anahtar dağıtımı*** ve ***rassal sayı üretimi*** diğer başlıca yaygın kullanım alanlarıdır.
[3] ***Atom***lar ve ***atomik*** parçacıklar düzeyinde ***madde***nin ***davranış***larını ve ***enerji*** ile ***etkileşim***ini ***matematik***sel olarak ifade eder.

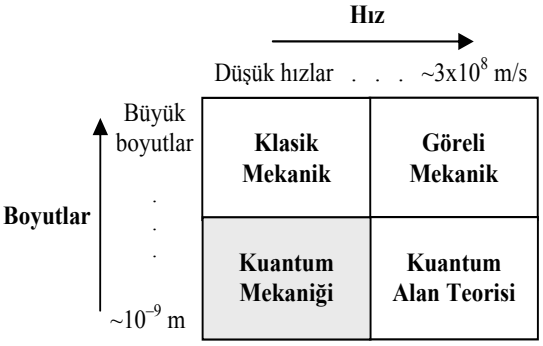
(1882-1970), John von Neumann (1902-1957), Paul Dirac (1902-1984), Wolfgang Pauli (1900-1958) gibi bilim insanlarının çalışmalarını da kapsayan 27 yıllık bir döneme yayılmıştır. 1927 yılında Schrödinger denkleminin (Erwin Schrödinger: 1887-1961) bulunmasıyla, esas olarak bugün öğrendiğimiz son halini almıştır. Kuantum mekaniğinin başarısı, ***Schrödinger denklemi***nin çözümlerinin ***doğa***nın özellikle ***mikro*** yapısında var olan pek çok ***deneysel gerçek*** ile tam ***uyuşum***lu sonuçlar vermesine dayanır. Buna göre kuantum mekaniğinin temel varsayımları (***postüla***ları), pek çok deneysel gerçeğin esasının ele alınmasıdır [8,9].

Kuantum mekaniği, ***doğa***nın/***hareket***in yeni ***teori***sidir. Bu teori atom, elektron, foton gibi ***mikroskopik*** sistemlerin ***davranış***larını açıklar (bkz. Şekil 2). 20. yüzyılın başlarına gelindiğinde artık klasik mekanik ***yasa***ları ile açıklanamayan bir dizi ***gözlem*** bulunmaktaydı [1]. Üstelik, bu gözlemlerin anlaşılması için, klasik fizikte yeri olmayan, *ışığın parçacık* (*tanecik*) *özelliği*, *kütleli parçacıkların dalga karakteri göstermesi* (*maddenin dalga özelliği*) ve hemen hemen tüm *fiziksel niceliklerin kesikli* (*kuantumlu*) *yapısı* gibi yepyeni kavramlardan söz edilmekteydi ve bunlar temel kavramlar olarak kullanılıyordu. Problemler, özellikle atom ve elektron gibi *çok küçük kütle*li ve *çok yüksek hız*lı cisimlerin işe karıştığı ve bunların ışık ve elektromanyetik alanlar ile ***etkileşim*** süreçlerinde ortaya çıkmaktaydı. Bu ***olay***ların en önemlileri şunlardır: *Siyah cisim ışıması*, *Katıların ısı sığası*, *Fotoelektrik olay*, *Compton olayı*, *Elektronlarla kırınım*, *Atomların ışıma ve soğurma spektrumları*. Başlangıçta bu olaylar, amaca uygun özel (ad hoc) ve o zamanlar garip görünen bir takım ***varsayım***larla açıklandı. Zamanla bunların başka olaylar için de geçerli olabileceği öngörüldü. Bu varsayımların sayıları arttıkça ve aralarındaki ilişkiler belirginleştikçe artık mekaniğin yepyeni bir ***formülasyon***u gerekti. 1920'li yılların ikinci yarısına gelindiğinde, sayıca artmış bütün varsayımlar üzerine kurulu yeni bir hareket teorisi gerekiyordu. Sonuç, kuantum mekaniğidir [8].

Kuantum mekaniği ve ***bilgi teorisi*** 20. yüzyılın dünyayı kavrayışımızı değiştiren en önemli buluşlarından ikisidir. Şimdi bilim insanları bu iki farklı disiplini bir şekilde birleştirmenin çabası içindeler. Çalışmamızın bundan sonraki kısımlarında bu gayretlerin, bilgi güvenliğini ilgilendiren sonuçlarına pratiklik sırasıyla yer verilmektedir.

4. Kuantum Rasgele Sayı Üretimi

Rasgele/rassal sayılar[2], kriptografiden istatistiğe, benzetime, örneklemeye, sayısal analize, şans oyunlarına kadar bugün pek çok önemli uygulamada yoğun olarak kullanılmaktadır. Bahsedilen uygulamaların hepsinde de uygulamanın ***başarım***ı açısından rasgele sayıların ***önem***i büyüktür ve hepsinin ***kalite*** gereksinimleri de farklıdır. ***Modern kriptografi***de, gizliliğin doğrudan bağlı olduğu kriptografik ***algoritma*** ve ***protokol*** parametrelerinin (tohum, ilklendirme vektörleri, sorgular, vs.) ve gizli ***oturum*** (şifreleme ve şifre çözme) ***anahtar***larının oluşturulmasında merkezi bir rol oynarlar [11,12].



Şekil 2: Mekaniğin 4 büyük uğraş alanı [10].

Günümüzde yeterince ***kaliteli*** ve ***hızlı*** rasgele sayıları üretmek üzere 2 temel ***üreteç*** türü mevcuttur[3] [13,14]: ***gerçek rasgele sayı üreteci*** (GRSÜ) ve ***sözde rasgele sayı üreteci*** (SRSÜ). GRSÜler ***fiziksel*** bir ***rasgelelik kaynağı***[4] kullanırlar ve daha çok da ürünlere daha sonradan eklenen ayrı bir ***donanım*** olarak tasarlanırlar. SRSÜler ise ***yazılımsal*** olarak gerçeklenirler, bilgisayar ya da ürün içinde koşan ayrı bir ***algoritma***/***program***[5] olarak tasarlanırlar. SRSÜler, GRSÜler kadar *kaliteli*/*güvenilir* olmasalar da daha ***basit***, ***ucuz***, ***hızlı*** ve ***esnek***[6] olmaları nedeniyle daha çok tercih edilirler. Bununla birlikte, SRSÜnün ***durum*** parametresi *fiziksel* bir kaynaktan elde edilen ***entropi***[7] ile en başta ***tohum***lanmalı ve daha sonra da güvenlik için periyodik olarak tekrar tekrar tohumlanmaya devam edilmelidir. SRSÜlerde tüm *entropi* bu *tohum*da yer almaktadır. Bu nedenle, SRSÜ kullanılması durumunda bile tohumu ***beslemek*** üzere GRSÜlere, en azından basit ama *güvenilir* bir GRSÜye, de ihtiyaç olmaktadır. Günümüz GRSÜlerinin *hız*larının henüz çok yüksek olmaması[8], çok hassas olup çalıştıkları ortamın koşullarından çok fazlaca etkilenebilmeleri, zaman zaman ***hata***/***arıza*** da yapabilmeleri SRSÜ kullanımını daha cazip kılan diğer başlıca nedenlerdir.

Yukardaki açıklamalardan da görüldüğü üzere, mevcut ***rasgelelik*** kaynakları, rasgeleliğin doğasına göre iki ana gruba ayrılabilir: sadece *sözde*-rasgele bit dizileri üretebilen ***yazılım*** çözümleri ile *gerçeksi*-rasgele bit dizileri üretebilen ***fiziksel*** kaynaklar. Burada bilinmesi gereken önemli nokta, hem ***klasik bilgisayar***ların hem de ***klasik fizik***in tamamen ***deterministik*** olduğudur. Sonuç olarak, her iki rasgelelik üreteci de rasgele gibi görünen bir bit dizisi üretmek için tamamen ***deterministik***

[1] Klasik mekaniğin en önemli niteliği ***deterministik*** olmasıdır. Buna karşılık, ***kuantum mekaniği***nin en önemli özelliklerinden ikisi ***belirsizlik*** (uncertainty) ve ***ayrıklık***tır (discreteness).

[2] ***Rasgele seçilen***, ***tahmin edilemez***, ***tekrar üretilemez*** olan sayılar. Bir sayının ya da sayı katarının rasgele olup olmadığına karar vermek günümüzün en çok tartışılan konularından biridir.

[3] Diğer bir yöntem, ***hibrid rasgele sayı üreteci***dir (HRSÜ). Bu yöntemde, GRSÜ ve SRSÜ birlikte kullanılır. SRSÜ, rasgele sayıları üretir; GRSÜ ise SRSÜyü *tohum*lamakta kullanılır.

[4] ***Zar*** atma, ***para*** atma, direncin ***termal gürültü***sü, avalanj diyodun ***cığ gürültüsü***, ***atmosferik gürültü*** ya da o anki ***zaman*** gibi kuantum olmayan ama çok ***karmaşık*** klasik ***fiziksel prosesler*** sıkça kullanılan gerçeksi rasgelelik kaynaklarıdır. Bunlar aslında tam rasgele değildir, ***deterministik***tir, ***hesaplanabilir***ler ama çok ***kompleks***tirler. Gerçekte, bunlarda ***determinizm*** karmaşıklığın arkasında gizlidir [12].

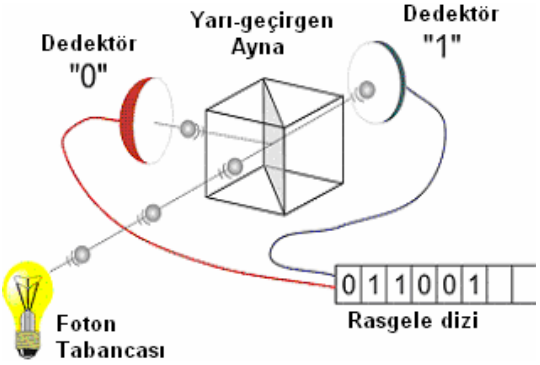
[5] Örneğin, $X_{n+1} \equiv$ **(214013 · X_n + 2531011) (mod 2^{32}) formül**ü (X_0, rasgele atanması gereken ***başlangıç değeri*** ya da *tohum*dur) ya da π **'nin dijitleri** gibi deterministik bir algoritma kullanılır. Daha genel bir ifade ile bilgisayarlar zaten deterministik sistemlerdir.

[6] SRSÜde değişiklik gerektiğinde tek yapılması gereken sadece ***yazılım***ı değiştirmek, *yazılım*la oynamaktır. GRSÜlerde olduğu gibi çok daha pahalı ve çok daha zor bir çözüm olan yeni bir ***donanım*** tasarımına ve donanım değişikliğine gerek yoktur.

[7] ***Belirsizlik***, ***bilinmezlik miktarı***nı ifade eden matematiksel bir terim.

[8] Buna karşılık, ***iletişim*** ve uygulama ***hız***ları çok daha yüksektir.

olan klasik fiziğe dayanır. Dolayısıyla, aslında, her iki üreteç türü için de tam bir rasgelelikten söz edilemez.



Şekil 3: ***Rasgele bitler***, ***foton***un gittiği ***yol*** uyarınca belirlenmektedir [12].

Bir ***kuantum rasgele sayı üreteci*** (KRSÜ), rasgele sayıları üretmek için ***kuantum fiziği***ni kullanan bir üreteçtir. Klasik fiziğin aksine kuantum fiziği ***deterministik değil***dir. ***Kuantum mekaniği***nde ***tamamen rasgelelik*** hakimdir. Ve KRSÜler de ***rasgelelik kaynağı*** olarak kuantum dünyasının bu ***içsel*** rasgeleliğini kullanır. Rasgele sayılar üretmek için çok ***basit*** birtakım kuantum prosesleri, bunlardaki içsel rasgeleliği, bile kullanmak mümkündür. Örneğin, Şekil 3'te şu an ticari bir ürün haline de gelmiş olan basit bir KRSÜ görülmektedir.

Quantis adı verilen bu KRSÜ, rasgelelik kaynağı olarak ***optik***sel bir kuantum proses kullanır. Optik, ışığın bilimidir. Kuantum fiziği bakış açısından ışık, ***foton*** adı verilen temel ***parçacık***lardan oluşur. Fotonlar belirli durumlarda rasgele bir davranış sergilerler. Örneğin, ikili rasgele sayıların üretimine de çok iyi uyan böylesi bir durum, fotonların ***yarı-geçirgen*** bir aynadan geçişleridir. Bir fotonun *yarı-transparan* bir aynadan geçmesi ya da yansıması tamamen rasgele bir olaydır, başka herhangi bir parametreden de etkilenmez. Şekil 3'teki optik sistemde de olduğu gibi *yarı-gümüşlenmiş* bir aynaya ***tek tek*** fotonlar göndermek ve geçtiklerini ya da yansıdıklarını ölçmek sonucunda elde edilen 0 ve 1 katarı ***gerçek rasgele***dir. Yarı-geçirgen bir aynaya fotonlar göndermek ve geçtiklerini ya da yansıdıklarını ölçmek, kuantum belirsizliğini kullanmanın sadece bir yoludur. Konum, momentum, elektrik alan gibi başka fiziksel büyüklüklerdeki herhangi bir belirsizlik de aynı şekilde işimizi görebilecektir. Sonuçta, elde edilen 0 ve 1 dizisi gerçekten rasgele olmalıdır[1].

Sonuç olarak, kuantum rasgele sayı üreteçleri tek gerçek rasgelelik üreteçleridir. Rasgele bitleri üretmek için kuantum proseslere güvenir/dayanır. Klasik fiziğin aksine, kuantum fiziği tamamen rasgeledir. Genel kanı, rasgeleliğin en iyi kaynağının belirsizliğin tek geçerli olduğu yer olan kuantum dünyası olduğu yönündedir. Buradaki başlıca ***problem***lerden biri ise gerçek rasgele sayıların üretilebileceği hızdır. Fotonlar ve yarı-geçirgen aynalarla çalışan ticari cihazlar için şimdilik 16 Mbps hıza kadar rasgele sayı üretimi yapılabilmektedir[2].

5. Kuantum Kriptografi

Kriptoloji (*cryptology*, aslen Yunanca olan *kryptós*: *gizli*, *gizlenmiş* ve *logia*: *çalışma*, *inceleme*, *araştırma* sözcüklerinin yan yana gelmesinden oluşmaktadır [3]) bilimi, Matematiğin alt dalı olup iki kısımdan oluşur: ***Kriptografi*** ve ***Kriptanaliz*** (*cryptanalysis*, aslen Yunanca olan *kryptós*: *gizli* ve *analýein*: *açmak*, *çözmek*, *halletmek* sözcüklerinden oluşmaktadır [16]). Kriptografi, bilgiyi gizli tutma ***sanat***ı ve ***bilim***idir. Çok özel, zekice ve güçlü matematiksel teknikler kullanarak ***bilgi güvenliği***ni ***garanti***lemeye yönelik çalışır. Bu amaç için tasarlanmış ***algoritma*** ve ***protokol***lerden oluşur. Modern ***kriptosistem***lerde bilgi, ***algoritma*** kullanılarak bir ***anahtar***la karıştırılır ve bir ***şifreli bilgi*** elde edilir. ***Güvensiz*** ortamlar üzerinde bu *şifreli bilgi* iletilir veya saklanır. ***İdeal*** bir kriptosistemde *doğru anahtar* olmadan şifreli bilgiyi çözmek ve ***asıl bilgi***ye ulaşmak ***imkansız*** olmalıdır. Sonuç olarak, şifreleme sisteminin gücü anahtarın gücüne dayanmaktadır[3]: ***hesaplanamaz***lığına[4] ve ***tahmin edilemez*** olmasına[5].

Kriptanaliz ise en zeki, güçlü ve kötü niyetli birisiymiş gibi davranıp yine benzer ***matematik***sel teknikleri, eldeki tüm ***teknoloji***k hesaplama gücünü ve tasarımlardaki ***zayıflık***ları da kullanarak geliştirilmiş mevcut bilgi güvenlik sistemlerini alt etmeye çalışır. Bunu başarmanın başlıca yolu aslında ***gizli anahtar***ı ele geçirmektir, yeterince güçlü olan olan günümüz kriptosistemlerinde algoritma ve protokoller zaten herkesçe bilinmektedir. Bu sistemler, gizli anahtar bilindiğinde şifreli bilgileri çözmenin çok kolay; aksi halde, ise imkansız olması özelliğine sahiptirler. Ancak, bilinmesi gereken diğer bir gerçek de hem Kriptografi hem de Kriptanalizin her ikisinin de Matematik yanında aynı zamanda daha çok klasik fiziğe de dayandığı, ***klasik fizik*** yasaları ile sınırlı olduklarıdır.

Gizli anahtarın güvenliği modern kriptosistemlerde çok ciddi bir meseledir. Bu sorun, ***anahtar dağıtım problemi***[6] olarak da bilinir. Hem modern simetrik hem de asimetrik kriptosistemler ***gizli anahtar***ların varlığına güvenirler; ancak, her iki kriptosistemde de esas problem gizli anahtarlarının gizliliğinin hiç bir zaman tam olarak ***garanti*** edilememesidir. Kırılamazlığı ***teorik*** olarak da ***kanıtlanmış*** tek kriptosistem olan ***Vernam şifresi*** [17,18] bilgi ile aynı uzunlukta gizli

[1] Mevcut KRSÜ'ler, bileşenlerinin henüz ***kusursuz*** çalışmaması (örneğin, yarı-geçirgen aynanın ***49%*** geçirgen olması ya da tek foton kaynağının ara sıra ***2*** ya da ***3*** foton da üretebilmesi gibi ***kusur***lar) nedeniyle ***klasik*** ve ***kuantum*** kısımlardan oluşmaktadır:

- ***Kuantum kısım***: Rasgelelik kaynağı olan ***kuantum proses***i içerir. Bileşenlerin henüz ***mükemmel*** olmaması nedeniyle elde edilen 0, 1 dizisi ***düzgün dağılım***lı (*eşit olasılıklı*) değildir.
- ***Klasik kısım***: Düzgün dağılımlı olmayan 0, 1 katarını mümkün olduğunca *düzgün dağılımlı* (*eşit olasılıklı*) hale getirmek için bazı ***son-işleme*** (*post-processing*) adımlarını içerir.

[2] Bir US takımı *detektöre ulaşan fotonlar arasındaki aralıklar*a dayanan ***çözüm***leri ile 100 Mbps, Çinliler *faz gürültüsü*nü kullanan yöntemleri ile 300 Mbps ve bir İsrail takımı bir *lazerin kaotik çıkışı*nı kullanan çözümleriyle 3 Gbps kadar pratik hızlara da çıkabilmektedir. Son yöntem oldukça iyi gibi görünmesine karşın, buradaki rasgelelik tam olarak kuantum-tabanlı bir rasgelelik değildir [15].

[3] Modern şifreleme ve şifre çözme algoritmalarının yeterince ***güçlü*** olduğu kabul edilmektedir. Gerçekten de günümüzde yeterince güçlü şifreler kullanılmaktadır. Tek sorun, güvenliğin henüz ***ispatlanmamış*** birtakım ***matematik***sel ***problem***lere dayanıyor olmasıdır.

[4] Yeterince ***uzun*** olmalıdır. Modern kriptografide ***güvenlik düzeyi***ni ayarlamaya yarayan esas parametre ***anahtar uzunluğu***dur.

[5] Gerçekten ***rasgele*** olmalıdır. ***Tekrar üretilemez*** olmalıdır.

[6] ***Anahtar dağıtımı***, modern kriptografinin en önemli konularından ve en büyük problemlerinden biridir. ***Anahtar dağıtım protokolleri***, birbiriyle *güvenli* haberleşmek isteyen; ancak, *mekan* olarak birbirinden çok uzakta olan iki kullanıcının sadece ikisinin bildiği ***ortak*** ve ***gizli*** bir ***anahtar*** üzerinde anlaşmasını sağlar. En güvenli yollardan ikisi: *i*) *güvenilir* ***kurye***, *ii*) *müdahalelere karşı korumalı*, *özel olarak tasarlanmış*, *çok güvenli taşıyıcı* ***cihaz***lar.

anahtarlar kullanır. Tek kullanımlık bu anahtarların her iki tarafta da olması gerekir. Anahtarın karşı tarafa güvenli olarak ulaştırılması simetrik kriptografide ciddi bir problemdir. Meraklı kişiler anahtar dağıtımı esnasında araya girerek bir şekilde anahtarın bir kopyasını ele geçirebilir.

Asimetrik kriptosistemlerde ise durum daha da kötüdür. Örneğin, özellikle *İnternet* sayesinde dünya çapında yaygın kullanım alanı bulan ***RSA***'de [19] açık anahtarda açıklanan bir sayıyı asal çarpanlarına ayırarak gizli anahtarı elde etmek mümkündür. Çok büyük olan bu sayıyı günümüz ***matematik bilgisi*** ve ***bilgisayar hesaplama gücü***yle ***makul bir süre***de çarpanlarına ayırmak neredeyse imkansızdır[1] [20]. Ancak, eğer teknolojik gelişmelerdeki hız gözönüne alınırsa bunun oldukça ***risk***li bir varsayım olduğu da açıktır. 10-15 yıl içinde geliştirilmesi ümit edilen ***kuantum bilgisayar***ın bu işlemi çok rahatlıkla gerçekleştirebileceği ***ispat***lanmış durumdadır[2].

Dolayısıyla, bahsedilen anahtar dağıtım sorunlarının ve ***risk***lerinin olmadığı bir kriptosisteme ihtiyaç vardır. Ulaşılan sonuç ise yepyeni bir alan olan ***kuantum*** *kriptografi*dir[3].

Kuantum kriptografi (KK), *bilgi güvenliğ*inin *kuantum mekaniğ*ine ait (***belirsizlik ilkesi***, ***foton polarizasyonu***, ***dolaşıklık*** gibi) ***yasa***lar ile ***garanti*** edildiği kriptografi tekniğidir[4] [21,22]. Temel avantajı, ***kanıtlanmış evrensel*** kuantum mekaniği yasalarına dayanıyor olması[5], güvenliğin ***ispatlanabilir*** olmasıdır. En bilinen ve ilk pratik uygulaması ***kuantum anahtar dağıtımı***dır (KAD) [23]. Yakın zamana kadar KK ve KAD aynı anlamda kullanılmaktaydı. Doğrusu, KK'nın KAD'ı da içine alan daha geniş bir disiplin olduğudur. ***Kuantum bilgisayar***a karşı tüm bilgi güvenliğini sağlama çalışmaları (klasik ya da kuantum olsun) da KK'nın kapsamı içinde kabul edilmektedir[6] [24,25]. Mevcut KK, şimdilik klasik ve kuantum kısımlardan oluşmaktadır:

- ***Kuantum kısım***: Kuantum anahtar dağıtımı (KAD).
- ***Klasik kısım***: Geleneksel kriptografi ile şifreleme.

Mutlak (*koşulsuz*, asla *kırılamaz*) ***güvenlik***te bir iletişim için KK'nın günümüzdeki temel çalışma prensibi şöyledir:

- ***Anahtar***, taraflar arasında ***KAD*** ile dağıtılır. Dolayısıyla, KK'da *anahtar dağıtım problemi* KAD ile çözülmektedir. KAD, güvenliği ***kanıtlanmış***, *tamamen* güvenli tek anahtar dağıtım yöntemidir.
- ***Şifreleme***, ***Vernam şifresi*** ile yapılır. Vernam şifresi kırılamazlığı ***kanıtlanmış*** tek şifredir.

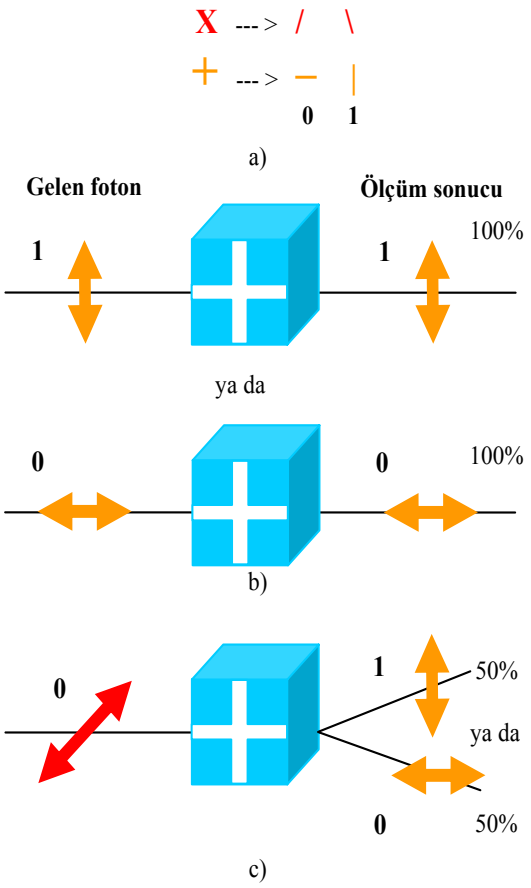
Böylece, KK'da ***mutlak*** (asla *kırılamaz*) güvenlikte bir iletişim ortamı ***garanti*** edilmiş olmaktadır.

KAD protokolleri, birbirinden çok uzakta olan iki kullanıcı arasında ***aynı***, ***rasgele*** ve ***güvenli*** bir ***gizli anahtar*** oluşturulmasını sağlar. Kuantum mekaniği yasaları, anahtar dağıtımı esnasında, gerçekleştirilen iletişime herhangi bir müdahale olup olmadığını (kuantum bilgi ile etkileşimde olan meraklı kimselerin varlığını) açığa çıkarabilmeyi de sağlar[7]. KAD'ın, temel çalışma ilkesi ise şu şekildedir:

- ***Anahtar***, tam ***güvenli*** bir şekilde dağıtılır.
- Aksi halde, protokol ***iptal*** edilir ve ***tekrar*** denenir.

Böylece, anahtarın taraflar arasında ***mutlak*** güvenli bir şekilde dağıtılması ***garanti*** edilmiş olmaktadır.

KAD, güvenli iletişim (birbirinden uzak iki kullanıcı arasında güvenli anahtar dağıtımı) için kuantum mekaniğinin en temel ***postüla***larından olan ***Heisenberg belirsizlik ilkesi***ne güvenir[8]. İletişim için temel kuantum taneciklerden olan ***foton***lar kullanılır ve anahtar bitlerini temsil etmek üzere de fotonların ***polarizasyon*** özelliğinden yararlanılır[9].



Şekil 4: Fotonlarla kuantum iletişim ve belirsizlik ilkesi [26]. a) ***Kodlama*** kuralı, b) Alıcıda gerçekleşen ***uyumlu ölçüm***lerin sonucu ***kesinlikle*** doğru olmaktadır. c) Alıcıda gerçekleşen ***uyumsuz ölçüm***lerin sonucu ***50%*** doğru olur.

[1] Gereken sürenin evrenin ömrü ($10^{10} \approx 2^{34}$ yıl, yaklaşık 10 milyar yıl civarı bir süre) ile sınırlı olduğu öngörülmektedir.

[2] Bu işi gerçekleştirecek ***kuantum algoritma*** şimdiden hazır bile: ***Shor'un algoritması***. Dolayısıyla, tek eksik bu algoritmanın üzerinde koşturulabileceği geniş ölçekli bir kuantum bilgisayardır.

[3] Klasik kriptografi sınırlı bir ***zaman dilimi*** ve ***teknolojik düzey*** için gizlilik sağlarken, kuantum kriptografi teknolojik gelişmelerden dahi etkilenmeyen çok daha ***uzun vade***li ve ***kalıcı*** gizlilik sağlar.

[4] ***Kriptografik servisler***i gerçeklemek üzere ***kuantum mekaniği***nin sonuçlarından (***foton***, ***Heisenberg belirsizlik ilkesi***, vb.) yararlanılır.

[5] Ve bunların klasik olarak bir eşdeğerlerinin de bulunmamasıdır.

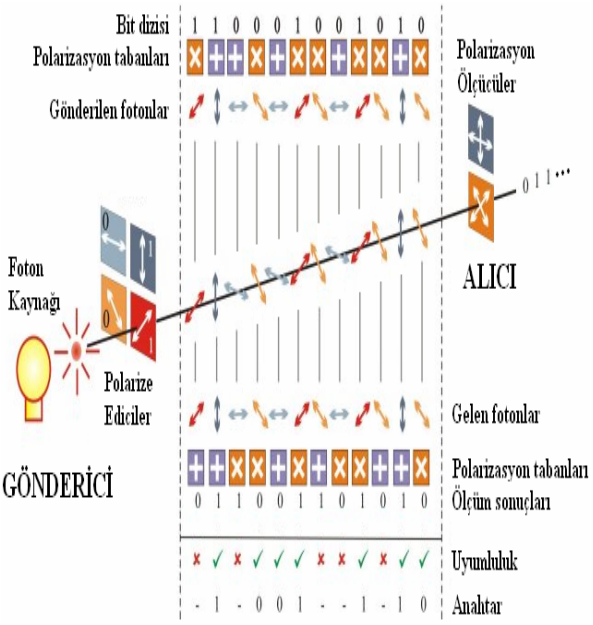
[6] Halen kuantum bilgisayar tarafından bir saldırı keşfedilmemiş klasik problemler ve ***post-kuantum*** kriptosistemler de mevcuttur.

[7] Bu klasik iletişimde bir eşdeğeri olmayan özelliklerdendir.

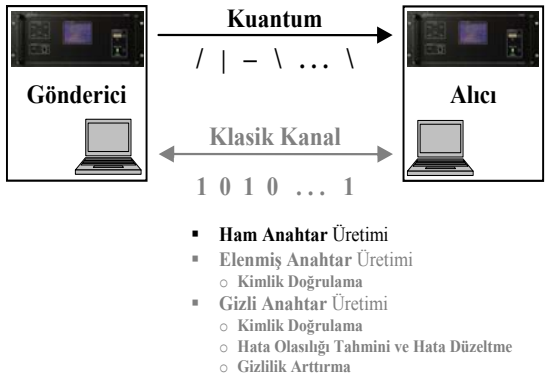
[8] Bu ilke özetle, "(***Bilinmeyen***) *Bir kuantum sistemi* ***ölçmek*** *o sistemi* ***değiştirecektir***." der. Bunun bir sonucu olarak, böylesi bir kuantum sistemle (ya da *bilinmeyen* bir *kuantum durum* ile) temsil edilmiş olan ***kuantum bilgi*** de değişmiş olacaktır. İlke aynı zamanda, bir kuantum sistemin (*bilinmeyen*) belirli özellik çiftlerinin (*konum* ile *momentum*, bir *doğrusal polarizasyon* ile bir *dairesel polarizasyon*, vb.) ***aynı anda*** asla tam olarak ölçülemeyeceğini de ifade eder Dolayısıyla, *belirsizlik yasası*nın gereği olarak, kuantum bilgiyi rahatsız etmeden üzerinde ölçümler yapmak ve bilgiyi elde etmek mümkün değildir. Bu da bizleri (*bilinmeyen*) ***kuantum bilgi kopyalanamaz*** sonucuna götürür. Bu sonuçlar, bizlere bilgi ile etkileşimde olan saldırganların varlığını çok rahatlıkla tespit edebilme olanağını da verir.

[9] Anahtarı taşıyıcı güvenilir ***kurye*** olarak ***foton***lar kullanılmaktadır. ***İdeal***de her bir anahtar ***bit***i tek bir ***foton*** ile taşınır.

Şekil 4'te tek tek fotonlarla gerçekleştirilen bir kuantum haberleşme örneği görülmektedir[1]. Alıcı, gelen herbir fotonu (/, \, – veya |) ölçeceği yönteme (X veya +) ***rasgele*** olarak[2] karar verir[3]. Eğer ***uyumlu*** bir ölçüm yaparsa foton bu ölçümden rahatsız olmaz ve ölçüm sonucu da kesinlikle doğru olur. Eğer ölçüm uyumsuz olursa, yapılan ölçüm hem fotonu rasgele olarak değiştirir hem de ölçümün sonucunu[4].



a)



b)

Şekil 5: ***BB84 protokolü*** [27]: a) *Gizli anahtar* bitleri, tek tek fotonlarla taşınmaktadır. b) ***Gizli anahtar***, ***kuantum*** ve ***klasik iletişim***ler sonucu belirlenmektedir

Şekil 5.a'da, anlatılan bu ilkelere dayanan ve şu an ticari bir ürün [28] haline de gelmiş olan basit bir KAD protokolü görülmektedir. Protokol ilk olarak Charles **B**ennett ve Gilles **B**rassard tarafından ve 19**84** yılında önerilmiş olması [29] nedeniyle ***BB84*** protokolü olarak da adlandırılır.

BB84 KAD protokolü, hem kuantum hem de klasik kısımlardan oluşmaktadır (bkz. Şekil 5.b):

- ***Kuantum kısım***: İlk aşama, aday anahtar bitlerinin tek tek foton tanecikleriyle taşınmasından oluşur.
- ***Klasik kısım***: Sonraki aşama ise alıcının ölçüm sonuçlarının değerlendirilmesidir.

Protokol, özetle şu şekilde gerçekleşmektedir:

BB84 PROTOKOLÜ:

Kuantum kısım

Adım 1: Gönderici, *ham anahtar* bitlerini rasgele olarak oluşturur. Bunun için bir KRSÜ kullanır. Herbir bitini bir *fotonun polarizasyon durumu* ile ifade edip fotonları ***kuantum kanal*** üzerinden teker teker alıcıya gönderir. Herbir bitini hangi tabanda kodlayacağına *rasgele* karar verir.

Adım 2: Alıcı, gelen herbir fotonu *rasgele* seçtiği[5] bir tabanda ölçer. Eğer seçtiği taban gönderici ile aynı ise, *ideal* durumda ölçüm sonucu da göndericinin biti ile kesinlikle ***aynı*** olacaktır. Farklı bir taban seçmişse, ölçüm sonucu ***50%*** ihtimalle/şansla doğru olacaktır. Ancak, henüz bunu bilmemektedir. Aynı durumlar aradaki bir saldırgan için de sözkonusudur.

Klasik kısım

Adım 3: Tüm iletim ve ölçümler tamamlandıktan sonra alıcı, sadece gelen fotonları hangi ***taban***larda ölçtüğünü bir ***klasik kanal*** üzerinden[6] açıklar. Gönderici, alıcıya aynı tabanı kullandıkları indeksleri açıklar. İdealde (gürültü, kusurlar, dinleme, vb. yoksa) bu indekslerdeki bitler de kesinlikle aynı olmalıdır.

Adım 4: Arada bir meraklının varlığını tespit etmek için bitlerin bir alt kümesi de açıklanır. Aynı tabanların kullanıldığı bitler de kesinlikle aynı olmalıdır. Eğer aynı değilse, bu ilgili fotonlara bir müdahale olduğu anlamına gelir ve protokol ***iptal*** edilir[7].

Adım 5: Herşey güvenli ise kalan ortak bitler **gizli anahtar** olarak kabul edilir.

BB84 protokolünün bahsedilen tüm aşamalarını standart kuantum optik laboratuvarı ekipmanları ile gerçekleştirmek mümkündür. Anahtar dağıtımı için hem gönderici hem de alıcının temel olarak şu iki ana bileşene ihtiyacı vardır:

- **Kuantum Kanal**: İletişim ***tek yönlü***dür. Göndericiden alıcıya ***kuantum sinyal***leri (***kübit***: *kuantum bit*) oluşturmak ve göndermek için kullanılır. İletim ortamı (*fiber optik kablo*, *hava boşluğu*, vb. optik ortamlar) ve tüm diğer iletim ekipmanları (*tek foton üreteci*, *foton polarize edici*, *foton polarizasyon ölçücü*, *foton detektörü*, vb. optik bileşenler) kuantum

[1] Alıcının gelen her bir fotonu ölçmeden önce göremeyeceğine ve bilemeyeceğine dikkat ediniz. KAD'da, hem alıcı hem de saldırgan bilmedikleri kuantum durumları ölçmek zorundadır.

[2] Rasgelelik için KRSÜ'lerden yararlanılması protokolün güvenliği açısından büyük önem taşımaktadır.

[3] ***Heisenberg belirsizlik ilkesi*** gereği, alıcının aynı anda hem X hem de + tabanında ölçümler yapması kesinlikle yasaktır. Aynı durum meraklı kişi için de geçerlidir.

[4] Alıcının yaptığı bir ölçümün sonucunun doğru mu ya da yanlış mı olduğunu bilemeyeceğine de dikkat ediniz. Aynı durum saldırgan için de söz konusudur.

[5] Bunun için bir KRSÜ kullanır.

[6] İnternet, telefon, cep telefonu, vb. yaygın kablolu/kablosuz ya da optik/elektriksel iletişim yöntemleri olabilir.

[7] Gerçek hayatta arada bir saldırgan olmasa bile kanal gürültüsü, optik ve elektriksel bileşenlerin henüz kusursuz olmaması gibi nedenlerle de bu bitler farklı olabilmektedir. Dolayısıyla, örneğin, 15%'lik bir hata olasılığına kadar protokolün devamına izin verilir.

kanal olarak ifade edilebilir. Kuantum kanalın dış ortam ile etkileşimden yeterince izole edilmiş olması gerekir. Ayrıca, kanalın kendisi de kuantum sinyal ile herhangi bir etkileşime girmemelidir. Sonuç olarak, ortamın fotonları değiştirmez olması önemlidir. Meraklı kişiler kuantum kanalda fotonları hem gözleyebilir hem de tekrar gönderebilirler. Fizik yasaları dışında kısıtlama olmaksızın kanala erişip istediği ***aktif*** ve ***pasif*** müdahaleleri yapabileceği varsayılır. Ancak, yaptığı ölçümler ilgili kübitleri değiştirecektir, bu da meraklıyı ele verecektir.

- **Klasik Kanal**: İletişim ***iki yönlü***dür. Göndericinin ve alıcının birbirlerine sıradan ***klasik sinyal***leri (klasik ***bit***ler) oluşturması ve gönderip alması için kullanılır (İnternet, cep telefonu, vb. telli/telsiz ortamlar). ***Kimlik doğrulama***lı olmak zorundadır; yani, gönderici ve alıcı birbirlerinin kimliklerini doğrulayabilmelidir. Bu nedenle, meraklı kişiler kimlik doğrulamalı klasik kanaldan gidip gelen mesajları sadece ***pasif***çe dinleyebilir, gözleyebilir; aktif herhangi bir müdahalede ise bulunamazlar. Sonuç olarak, meraklıların klasik kanalda gidip gelen bilgileri sadece gözleyebileceği varsayılır. Klasik iletişimin dinlendiği ise anlaşılamaz.

BB84 protokolü, bu iki ana bileşen üzerinde yer yer içiçe geçmiş şu 3 ana aşamadan oluşmaktadır:

- **Ham anahtar değiş-tokuşu**[1]: Kuantum durumların iletildiği ve ölçüldüğü kısımdır. İki taraf arasında ***kübit***ler (*polarize edilmiş foton*lar) değiş-tokuş edilir. KAD'ın tek kuantum olan kısmıdır, iletişim kuantum kanal üzerinden gerçekleştirilir. Bu adımın sonucunda ***ham anahtar***lar oluşur. Göndericinin ham anahtarı kuantum kanaldan gönderdiği tüm bitlerdir. Alıcının ham anahtarı ise ölçebildiği tüm bitlerdir. Gönderici ve alıcı ellerindeki ***bit***lerinin ve polarizasyon ***taban***larının bir kaydını tutarlar. *Ham anahtar*lardan *gizli anahtar*a götüren sonraki tüm adımlar ve iletişimler *kimlik doğrulama*lı bir klasik haberleşme kanalı üzerinden gerçekleştirilir.
- **Anahtar eleme**[2]: Kuantum kanaldaki kayıplardan dolayı göndericinin ve alıcının ham anahtar uzunlukları farklı olabilir. Öncelikle, alıcı tespit ettiği kübitlerin indeksini *kimlik doğrulamalı* klasik kanaldan açıklayarak göndericiyi haberdar eder. Daha sonra, bu bitlerden de polarizasyon tabanlarının uyumlu olduğu durumlardakiler seçilir. Bu adımın sonucunda ortaya bir ***elenmiş anahtar*** çıkar. Göndericinin ve alıcının elenmiş anahtarı büyük ölçüde aynıdır ve uzunlukları da eşittir.
- **Damıtma**[3]: Gönderici ve alıcı elenmiş anahtarlarını birlikte işleyerek daha güvenli ve tamamen aynı bir hale getirirler. ***Gizli anahtar***, bu adımın sonucunda ortaya çıkar. Bu adımın kendisi de yine içiçe şu 3 temel aşamadan oluşmaktadır [30]:
  1) Kimlik doğrulama,
  2) Hata düzeltme ve
  3) Gizlilik arttırma.

[1] ***Raw key Exchange (RKE)***.

[2] ***Key sifting***. Kaynaklarda bu aşama ***information reconciliation***: *anahtar uzlaştırma* (*hata düzeltme* teknikleriyle) olarak da verilir.

[3] ***Key distillation***. Kaynaklarda bu aşama ***privacy amplification***: *gizlilik arttırma* (*özet fonksiyonları* yoluyla) olarak da verilir.

Böylece, ***güvenli***, ***rasgele*** ve her iki tarafta da ***aynı*** olan bir ***gizli anahtar*** oluşturulmuş olur.

Görüldüğü üzere, mevcut KAD protokollerinin güvenliği şu üç ana etkene bağlıdır [31]:

- ***Kuantum mekaniği***nin doğru olmasına.
- Gönderici ve alıcı arasındaki ***kimlik doğrulama***nın koşulsuz güvenlikte olmasına: *Aksi halde, protokol* ***ortadaki adam saldırısı****na karşı savunmasız hale gelmektedir.* ***Simetrik anahtarlı kimlik doğrulama*** *yöntemleri, koşulsuz güvenlikte kimlik doğrulama olanağı sağlayabilirler; ancak, taraflar arasında bir öngörüşme ile dağıtılmış simetrik anahtarların varlığını gerektirirler. Diğer bir yöntem olarak, güvenli* ***asimetrik anahtarlı kimlik doğrulama*** *yöntemlerinden de yararlanılabilir.*
- Kullanılan ***ekipman***ların güvenli olmasına: *Gönderici ve alıcı arasında doğrudan bir bağlantı gerektirir. KAD'da rasgeleliğin gerektiği yerlerde bir KRSÜ'nün kullanılması ise özellikle önerilen bir diğer önemli noktadır. Gerçeklemelerde de herhangi bir zayıf nokta olmamalıdır.*

İlk KAD protokolü olan BB84'ten sonra, başka protokol önerileri de olmuştur: B92, E91, SARG04, vb.. KK, KAD ve protokolleri hakkında daha detaylı bilgi için [32,33]'ten ve kaynaklarından da faydalanılabilir.

6. Kuantum Kriptanaliz

Kriptanaliz, kriptografinin aksine, şifreleri çözme ve şifreli bilgileri okuma ***sanat***ı ve ***bilim***idir[4]. ***Kuantum kriptanaliz***, ***kuantum bilgisayar***lar kullanarak[5] şifreleri kırmakla ilgilenen kriptografik bir uygulama alanıdır [34].

Kuantum kriptanalizin şu an için en çok bilinen örneklerinden birisi 1994 yılında matematikçi Peter W. Shor (1959) tarafından önerilen ***Shor algoritması***dır [35][6]. Bu algoritma, çarpanlara ayırma problemini çözmenin verimli bir yoludur. Geleneksel kriptografik teknikler anahtar iletiminin güvenliğini sağlamak için daha çok matematiksel yaklaşımlara güvenirler[7]. Ancak önerdikleri güvenlik, henüz *kanıtlanmamış* bazı *varsayım*lara dayanmaktadır ve teknolojiye de çok bağımlıdır. Örneğin, henüz araştırılma safhasında olan ***kuantum bilgisayar*** kariptanalizde kullanılma potansiyeline sahiptir. Shor'un algoritması geniş ölçekli bir kuantum bilgisayar ile çok büyük tamsayıları kolaylıkla çarpanlarına ayırabilecektir. Böylece, yaygın kullanımda olan bazı açık-anahtarlı şifreleme algoritmaları da kırılmış olacaktır.

Aynı şekilde, bilgisayar bilimci Lov K. Grover (1961) tarafından önerilen ***Grover algoritması***nın [38] bir kuantum bilgisayarda çalıştırılmasıyla, kaba-kuvvetle anahtar aramaları

[4] Gizli anahtarı bir şekilde ele geçirerek ya da geçirmeden. Genellikle, kriptanaliz gizli anahtarı ele geçirmenin en zor yolu olarak kabul edilir. Sistemdeki zayıflıklarla aynı iş daha kolayca yapılabilir.

[5] Dolayısıyla, bazı ***kuantum mekaniksel sistem***lerden, birtakım ***kuantum mekaniksel etki***lerden yararlanılmış olmaktadır.

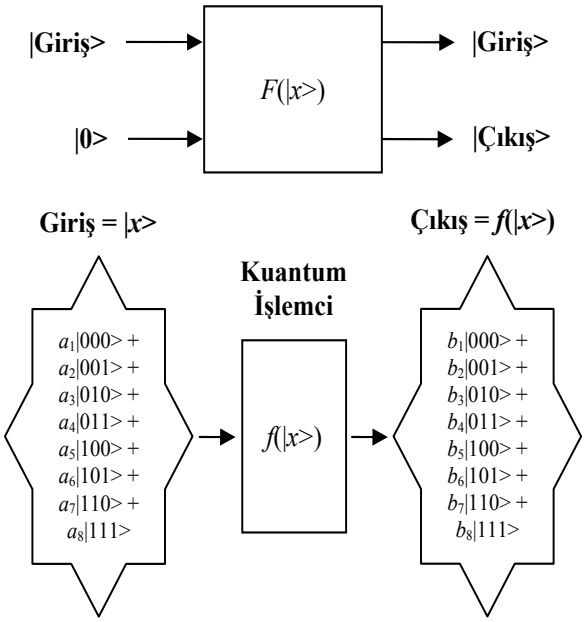
[6] Fizikçi Richard P. Feynman (1918-1988) [36] ve teorik fizikçi David E. Deutsch (1953) [37] gibi bilim insanlarının 1980'lerdeki çalışmaları ile Kuantum hesaplama konusu gündeme gelmişti. Ancak, esas reklamını aslen bir matematikçi olan Peter Shor yapmıştır. Ancak Shor'un algoritmasından sonra çeşitli ulusal ve özel güvenlik kurumları, bankalar, vs. bu işin peşine ciddiyetle düşmüştür.

[7] Hesapsal karmaşıklığa güvenir. Çözülmesi neredeyse imkansız kabul edilen bazı matematik problemlerinin çözülemezliğine bağlıdır.

da karesel olarak daha hızlı yapılabilir. Bununla birlikte, anahtar uzunluğu iki katına çıkartılmak suretiyle bu tehditten kurtulabilmek şimdilik mümkündür.

KAD'ın aksine, diğer birçok kuantum uygulama[1] gibi kuantum kriptanaliz de büyük ölçekli bir kuantum bilgisayarın yapılmasını beklemektedir.

Kuantum bilgisayar, bilgi üzerinde birtakım işlemler gerçekleştirmek için doğrudan ***süperpozisyon***[2], ***dolaşıklık***[3] gibi kuantum fenomenleri kullanan aşırı derecede paralel bir hesaplama makinesidir [39]. Henüz var olan şeyler değildir; ancak, eğer teknik problemlerin üstesinden gelinir ve geniş ölçekli kuantum bilgisayarlar yapılırsa, kriptografiye ve dolayısıyla da bilgi güvenliğine etkisi çok büyük olacaktır. Şu an ki versiyonları henüz sadece birkaç kübiti (***kübit***: kuantum bit [40]) idare edebilmektedir ve en son haberlere göre 128 kübite kadar çıkılabildiği de görülmektedir [41].



Şekil 6: Kuantum bilgisayarın çalışma prensibi. *n* kübitlik bir kuantum saklayıcı, olası 2^n değerin hepsini birden aynı anda tutabilir. Kuantum işlemci de bu olası 2^n değerin hepsi üzerinde aynı anda işlem yapabilir.

Bir kuantum bilgisayarın ne olduğunu ve neler yaptığını daha iyi anlayabilmek için öncelikle bir klasik bilgisayarın neler yaptığına bakabiliriz. Klasik bilgisayar, bir ***ikili*** giriş alır (örneğin, 100010) ve bir ikili çıkış verir (belki, 0101). Eğer birden çok giriş varsa, herbiri üzerinde tek tek çalışması gerekir. Benzer şekilde, bir kuantum bilgisayar da giriş olarak belirli sayıda kübit alır ve birkaç kübit çıkarır. Ana fark, kuantum bilgisayarda hem giriş hem de çıkış kübitlerinin belirli temel durumların lineer kombinasyonları olabilmesidir. Kuantum bilgisayar, bu lineer kombinasyondaki tüm temel durumlar üzerinde aynı anda çalışabilir (bkz. Şekil 6). Gerçekte, kuantum bilgisayar bir paralel makinedir[4].

Örneğin, üç parçacığı temsil etmek üzere |100> temel durumunu[5] düşünelim: ilk parçacık 1 durumunda ve son ikisi ise 0 yönelimindedir[6]. Kuantum bilgisayar, sadece bu |100> durumunu alabilir ve bir çıkış üretebilir. Bununla birlikte,

$$\frac{1}{\sqrt{3}}(|100> + |011> + |110>) \qquad (1)$$

gibi temel kuantum durumların normalize edilmiş[7] lineer bir kombinasyonunu[8] da giriş olarak alabilir ve yine tek bir temel durumla çalıştığı kadar hızlıca çalışarak bir çıkış üretebilir. İşte bir kuantum bilgisayarı potansiyel olarak çok daha güçlü yapan bu, durumların lineer kombinasyonu ile aynı anda çalışma, yeteneğidir. Buna rağmen, kuantum bilgisayar üzerinde çalıştığı bir kuantum durumun temel durumlardan sadece birisi mi yoksa temel durumların lineer bir kombinasyonu mu olduğunu ölçüm yapmadan bilemez. Ancak, böylesi bir ölçüm de girişi değiştirecektir[9].

Bir klasik bilgisayarda x girişiyle çalıştırılabilen bir $f(x)$ fonksiyonumuz olduğunu varsayalım. Klasik bilgisayar bir x girişi ister ve bir $f(x)$ çıkışı üretir. Diğer taraftan, bir kuantum bilgisayar, giriş olarak aşağıdaki gibi tüm olası x giriş durumlarının bir toplamını kabul edebilir:

$$\frac{1}{C}\sum_x |x\rangle = \frac{1}{C}(|x_0> + |x_1> + \dots) \qquad (2)$$

(C bir normalizasyon faktörüdür/sabitidir) ve aşağıdaki gibi bir çıkışı da üretebilir:

$$\frac{1}{C}\sum_x |x, f(x)\rangle = \frac{1}{C}(|x_0, f(x_0)> + |x_1, f(x_1)> + \dots) \qquad (3)$$

Burada, $|x, f(x)>$ kübitlerin daha uzun bir dizisidir: hem x hem de $f(x)$ değerlerini temsil eder[10]. Böylece, $f(x)$'in tüm değerlerinin bir listesini elde edebiliriz. Bu noktada sorun, hesaplamanın sonucuna ulaşmaktır. Eğer bir ölçüm yaparsak, kuantum durumu ölçümün sonucuna zorlarız. Yani, rasgele seçilen bir x_0 değeri için $|x_0, f(x_0)>$ sonucunu elde ederiz, ve çıkıştaki tüm diğer durumlar yok edilir. Bu nedenle, $f(x)$'in değerlerinin listesine bakacaksak eğer, tek bir şansımız olduğu için, bunu çok dikkatlice yapmalıyız. Özellikle, onu daha çok istenilen bir şekle sokmak için belki çıkışa bir dönüşüm uygulamak gerekir. İşte, bir kuantum bilgisayarı programlamadaki temel hedef de hesaplamayı tasarlamak şeklindedir; öyle ki, görmek istediğimiz çıkışlar diğerlerinden çok daha yüksek bir olasılıkla görünsün. Shor'un çarpanlara ayırma algoritmasında[11] yapılan da tam olarak budur[1].

[1] Kuantum özel kanallar, kuantum açık anahtarlı şifreleme, kuantum zar atma, kör kuantum hesaplama, kuantum para, vs..

[2] Bir kübitin aynı anda hem 0 hem de 1'i tutabilmesi kuantum sistemlerin süperpozisyon (ya da *üst üste binme*) özelliğinin bir sonucudur. *n* durumlu bir kuantum sistem belli bir anda bu olası *n* durumun hepsinde birden bulunabilir. Bu özelliğe süperpozisyon ya da üst üste binme denir. Üstkonum dendiği de olur.

[3] Dolaşıklık, iki kübitin birbiriyle ilişkili olmasıdır. Öyle ki, birinde yapılan bir değişiklik diğerini de etkiler.

[4] *n* kübitlik tek bir kuantum bilgisayarın işlem gücü açısından *n* bitlik 2^n adet klasik bilgisayara eşit olduğu söylenebilir.

[5] Özdurum: $|\psi> = a_0|0> + a_1|1>$, $a_1 = 0$ veya $a_2 = 0$, a_1, a_2 kompleks.

[6] $|x>$: x kuantum durumunu ifade etmek üzere Dirac notasyonudur. Bir kuantum parçacığı, istenilen bir kuantum duruma sokmak için, örneğin Şekil 4'teki gibi işlemler uygulanabilir.

[7] Yani, 1 uzunluklu.

[8] Süperpozisyon: $|\psi> = a_0|0> + a_1|1>$, $a_1 \neq 0$ ve $a_2 \neq 0$.

[9] Bir kuantum bilgisayar belirli işlemleri oldukça verimli olarak yapabilmektedir: örneğin, ***periyot bulma***.

[10] Bazı kuantum parçacıkları da f(x) değerine değiştirmek üzere girişi $(1/C)\sum|x, 00\dots0\rangle$ şeklinde yapmak notasyon olarak daha iyi olabilirdi; ancak, basitlik için bu yapılmamıştır.

[11] Yeteri kübitlikte bir kuantum bilgisayar ile çarpanlara ayırma işini polinomsal zamanda yapmaktadır.

KRSÜ, KK ve KAD'da olduğu gibi Shor'un algoritması da klasik ve kuantum kısımlardan oluşmaktadır[2]:

- ***Klasik kısım***: Klasik bir bilgisayarda yapılabilecek olan bu kısımda, çarpanlara ayırma problemi bir *mertebe/periyot-bulma*[3] problemine indirgenir. Bu kısım, eskiden beri bilinmekte olan bir kısımdır.
- ***Kuantum kısım***: Mertebe-bulma problemini çözmek üzere bir kuantum algoritma içerir. Yani, kuantum mekaniği kullanılarak ***mertebe***/***periyot-bulma*** işlemi yerine getirilmektedir.

Shor algoritması belirli bir olasılık dahilinde periyodu bulur. Algoritma özetle aşağıdaki gibidir [42]:

SHOR ALGORİTMASI:

Klasik kısım: *N*'nin asal çarpanları

1. Rasgele bir $a < N$ sayısı üretilir.
2. $OBEB(a, N)$ hesaplanır[4]. Eğer, $OBEB(a, N) \neq 1$ ise a, N'nin bir asal çarpanıdır. Durulur.
3. $N^2 \leq Q = 2^m \leq 2N^2$ olan bir Q belirleyip $f(x) = a^x \bmod N$ fonksiyonunun r periyodunu[5] bulmak üzere *kuantum kısım*a geçilir ve aşağıda verilen *kuantum periyot-bulma altyordamı* çalıştırılır.
4. Eğer bulunan r tek ise, ***1. adım***a dönülür.
5. Eğer $a^{r/2} \equiv -1 \pmod N$ ise, ***1. adım***a dönülür.
6. $OBEB(a^{r/2} \pm 1, N)$ değeri, N'nin asal çarpanıdır. Durulur.

Kuantum kısım: Periyot-bulma altyordamı

Adım 1. (Kuantum) Saklayıcılar ilklendirilir: $Q^{-1/2}\sum_{x=0}^{Q-1}|x,0\rangle$. İlk yarıda (giriş), tüm olası x değerlerinin bir listesi yer almaktadır. m kübitlik olan giriş (gerekli kübit sayısı $\lceil \log_2 2^m \rceil$ ile hesaplanır, $0 \leq x < Q$), $Q = 2^m$ durumun bir süperpozisyonunda olup 0'dan $(Q-1)$'e kadar tüm değerleri içerir. $m/2$ kübitlik olan çıkış (kübit sayısı $\lceil \log_2 N \rceil$ ile hesaplanabilir, $0 \leq r < N-1$) saklayıcısı (ikinci yarı) ise henüz hep 0'dır. Ayrıca, giriş ve çıkış saklayıcıları dolaşıktır.

Adım 2. $f(x)$, kuantum bir fonksiyon olarak gerçeklenip yukarıdaki kuantum duruma (ilk yarısına) uygulanır: $Q^{-1/2}\sum_x |x, f(x)\rangle$. Son durum, halen tüm olası $Q = 2^m$ durumun bir süperpozisyonudur. İlk yarı, tüm x değerlerinin bir listesini; çıkış ise tüm $a^{|x>} \pmod N$ değerlerinin listesini içerir. Dolayısıyla, şu an itibariyle tüm olası girişler ve çıkışlar saklayıcılardadır.

Adım 3. İkinci yarı üzerinde bir ölçüm yapılır: $\frac{1}{C}\sum_{\substack{0\leq x<2^m \\ a^x \equiv u \pmod N}} |x,u\rangle$. ($C$, vektör uzunluğunu 1 yapmak için gereken faktördür; aslında, toplamdaki terimlerin sayısının kareköküdür). Böylesi bir ölçüm, bize bir $u \pmod N$ sayısı verir ve tüm sistemi $|x, u>$ formundaki durumların bir lineer kombinasyonuna zorlar; öyle ki, tüm $a^x \equiv u \pmod N$ durumlarını elde etmiş oluruz.

Adım 4. Giriş saklayıcısına Kuantum Fourier Dönüşümü (QFT: Quantum Fourier Transform) uygulanır: $U_{QFT}|x\rangle = Q^{-1/2}\sum_y w^{xy}|y\rangle$, burada, $w = e^{2\pi i/Q}$, $0 \leq y < Q$. QFT, periyodu bulmak için gerekli olan frekansları ölçer. Eğer r değeri 2^m değerinin bir böleni ise, bu durumda elde edeceğimiz frekanslar bir f_0 temel frekansının katları olur ve $rf_0 = 2^m$ sağlanır. Genel olarak, r değeri 2^m değerinin bir böleni değildir. Böylesi durumlarda ise bazı baskın frekanslar olacaktır ve bunlar bir f_0 temel frekansının yaklaşık olarak katları olacaktır; öyle ki, $rf_0 \approx 2^m$. QFT sonucu olan kuantum durum üzerinde ölçüm yapılır ve sonuçta bir $f = j.f_0$ frekansı belirlenir.

Adım 5. r'yi elde etmek için aşağıdaki oran üzerinde sürekli bölmeler açılımı uygulanır[6]:

$$\frac{j \cdot f_0}{r \cdot f_0} \approx \frac{f}{2^m} \Rightarrow \frac{j}{r} \approx \frac{f}{2^m} \qquad (4)$$

ilişkisinden bir r değeri hesaplanır, $r \leq Ø(N)$[7] $< N$. Genellikle, bu bölmenin açılımındaki N'den küçük en son payda aranılan r periyodu olmaktadır.

Adım 6. $a^r \equiv 1 \pmod N$ olup olmadığı kontrol edilir? Evet ise, işlem tamam.

Adım 7. Aksi halde, ***altyordam***ın ***1. adım***ına geri dönülür ve işlem tekrarlanır.

Bu algoritmanın kuantum kısmına ilişkin kuantum devreler her bir N ve a için özel olarak tasarlanırlar. Yöntemin doğru çalışmadığı da olmaktadır, bu durumda algoritma yeniden tasarlanır ve baştan çalıştırılır.

Konularla ilgili daha detaylı bilgi için [43-54]'teki kaynaklardan da faydalanılabilir.

7. Sonuçlar

Kuantum mekaniği ve bilgi teorisi 20. yüzyılın dünyayı kavrayışımızı değiştiren en önemli buluşlarından ikisidir. Şimdi bilim insanları bu ikisini bir şekilde birleştirmenin çabası içindeler ve büyük ölçüde de başarmışlardır.

Kriptograflarla kriptanalistler arasında asırlardan beridir devam etmekte olan mücadele bundan sonra da kuantum

---

[1] Bugün bazı açık anahtarlı kriptosistemlerin güvenliği bu problemin çözülmesinin zorluğuna dayanmaktadır.

[2] Shor'un algoritması ilk olarak 2001 yılında IBM'de ilk 7-kübitlik kuantum bilgisayar üzerinde çalıştırılmış ve 15 sayısını asal çarpanlarına ayırmıştır. Eğer büyük ölçekli bir kuantum bilgisayar yapılırsa bunun kriptografide önemli etkileri olacaktır.

[3] ***Order-finding***: mertebe bulma, ***period-finding***: periyot bulma.

[4] Bu hesaplama ***Öklid algoritması*** ile çok kolayca yapılabilir.

[5] $(Z_N)^x$ grubunda (tamsayılar mod N'nin çarpımsal grubu), a elemanının mertebesi, $f(x + r) = f(x)$ koşulunu sağlayan en küçük r tamsayısıdır. Grup, cebirsel yapılardan biridir.

[6] ***Frekans***, ***uzunluğun periyoda bölümü*** olup dizinin kaç kere tekrar ettiğini ifade eden matematiksel bir terimdir: $f\,(frekans) = \frac{L\,(uzunluk)}{T\,(periyot)}$. Dolayısıyla, ***uzunluğu*** belli olan bir dizinin ***frekansı*** bulunabilirse ***periyodu*** da çok rahatlıkla bulunabilir.

[7] Euler'in Ø-fonksiyonu. p, q asal ve $N = p \cdot q$ ise $Ø(N) = (p-1)\cdot(q-1)$.

dünyada devam edecek gibi görünmektedir. İlk büyük-ölçekli kuantum bilgisayarın henüz yıllarca uzakta olmasına ve olabilirliğinden birçoklarının şüpheli olmasına rağmen, KRSÜ (*gizli anahtar üretimi* için) ve kuantum kriptografi (*anahtar dağıtımı* için) şimdiden ticari ürünler haline bile geldi. Kuantum kriptocular, 150 km'den daha uzak bir mesafe için güvenli mesajlar iletmeyi başardı. Bununla birlikte, çok az sayıda kübiti idare edebilen ilk kuantum bilgisayarlar da yapıldı ve 15'i asal çarpanlarına ayırabildi. Daha büyüklerini yapabilmek için çalışmalar hızlı bir şekilde sürmektedir.

Ulusal güvenlik açısından en önemli konulardan biri de ***ulusal bilgi***lerin güvenliğidir. Ve ulusal güvenliğin en büyük gereklerinden birisi de ***dışa bağımlılık***tan kurtulmaktır. Çağın ve yaşanmakta olan bilimsel-teknolojik gelişmelerin gerisinde kalmamak için acilen kuantum teknolojileri (*KRSÜ*, *kuantum kriptografi*, *kuantum kriptanaliz*, *kuantum bilgisayar*, *kuantım haberleşme*, vb.) üzerinde çalışmalar yapacak bir ***Ulusal Kuantum Teknolojileri Araştırma (Geliştirme ve Test) Merkezi*** (UKTAM) kurulması çalışmalarına başlanması çağrımızı [55] burada da tekrarlamak istiyoruz[1].

8. Kaynakça

[1] Çeşmeci, M. Ü., "Kriptoloji Tarihi", UEKAE Dergisi, Sayı 1, s21-31, http://www.uekae.tubitak.gov.tr. Erişim: Haziran 2011.
[2] Steganography, http://en.wikipedia.org/, Wikipedia The Free Encyclopedia. Erişim: Haziran 2011.
[3] Cryptography, http://en.wikipedia.org/.
[4] Boyacı, U. K., "Günümüzde Kriptoloji", UEKAE Dergisi, Sayı 1, s32-41, http://www.uekae.tubitak.gov.tr.
[5] Kerckhoffs, A., "La cryptographie militaire", *Journal des sciences militaires*, vol. IX, pp. 5–83, Jan. 1883, pp. 161–191, Feb. 1883.
[6] Auguste Kerckhoffs, http://en.wikipedia.org/.
[7] Claude Shannon, http://en.wikipedia.org/.
[8] Dereli, T., Verçin, A., *Kuantum Mekaniği Temel Kavramlar ve Uygulamaları*, Ciltli, Tüba Yayınları, Ağustos 2009.
[9] Quantum mechanics, http://en.wikipedia.org/.
[10] Classical mechanics, http://en.wikipedia.org/.
[11] Geçkinli, C. N., "Rasgelelik (Rastlantısallık) Kavramına Genel Bir Bakış", UEKAE Dergisi, Sayı 1, s96-103, http://www.uekae.tubitak.gov.tr.
[12] QUANTIS, True RANDOM NUMBER Generator Exploiting QUANTUM PHYSICS, http://www.idquantique.com/. Erişim: Haziran 2011.
[13] Pseudorandom number generator, http://en.wikipedia.org/.
[14] Hardware random number generator, http://en.wikipedia.org/.
[15] Quantum Noise Breaks Random Number Generator Record, http://www.technologyreview.com/blog/arxiv/25355/, Erişim: Haziran 2011.
[16] Cryptanalysis, http://en.wikipedia.org/.
[17] Shannon, C.E., 1949, "Communication theory of secrecy systems", *Bell System Technical Journal*, 28, 656-715.
[18] Vernam, G., 1926, "Cipher printing telegraph systems for secret wire and radio telegraphic communications", *J. Am. Institute of Electrical Engineers*, Vol. XLV, 109-115.
[19] Rivest, R.L., Shamir A. and Adleman L.M., 1978, "A Method of Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, 21, 120-126.
[20] Schneier, B., *Applied Cryptography: Protocols, Algorithms and Source Code in C*, 2nd Edition, John Wiley & Sons. Inc, 1996.
[21] Kalem, Ş., "Kuantum Bilgi Güvenliğine Doğru", UEKAE Dergisi, Sayı 1, s42-47, http://www.uekae.tubitak.gov.tr.
[22] Quantum cryptography, http://en.wikipedia.org/.
[23] Quantum key distribution, http://en.wikipedia.org/.
[24] Post-quantum cryptography, http://en.wikipedia.org/.
[25] Bernstein, D. J., Buchmann J., Dahmen, E., *Post-Quantum Cryptography*, 1 edition, Springer, November 17, 2008.
[26] Raw Key Exchange, http://swissquantum.idquantique.com/?Raw-Key-Exchange, SwissQuantum, Erişim: Haziran 2011.
[27] Key Sifting, http://swissquantum.idquantique.com/?Key-Sifting.
[28] CLAVIS^2, QUANTUM KEY DISTRIBUTION FOR R&D APPLICATIONS; CERBERIS, A fast and secure solution: high speed encryption combined with quantum key distribution, http://www.idquantique.com/.
[29] Bennet, C. H., Brassard, G., "Quantum Cryptography: Public Key Distribution and Coin Tossing", *Proc. Int'l Conf. Computers, Systems & Signal Processing*, CS Press, 1984, pp. 175–179.
[30] Quantum Key Distribution Protocols, http://swissquantum.idquantique.com/?Quantum-Key-Distribution-Protocols.
[31] Stebila, D., Mosca, M., Lütkenhaus, N., "The Case for Quantum Key Distribution", *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, volume 36, page 283--296. Springer, 2010. DOI: 10.1007/978-3-642-11731-2_35.
[32] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., 2002, "Quantum Cryptography", 57 pages, 32 figures, submitted to *Reviews of Modern Physics*, quant-ph/0101098. DOI: 10.1103/RevModPhys.74.145.
[33] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dusek, M., Lutkenhaus, N., Peev, M., 2009, "The Security of Practical Quantum Key Distribution", 50 pages, 9 figures, submitted to *Reviews of Modern Physics*, arXiv:0802.4155. DOI: 10.1103/RevModPhys.81.1301.
[34] Quantum Cryptoanalysis, http://www.qubit.org/. Erişim: Haziran 2011.
[35] Shor, P. W., 1994, "Algoritms for quantum computation: discrete logarithms and factoring", *Proceedings of the 35th Symposium on Foundations of Computer Science*, Los Alamitos, edited by Shafi Goldwasser (IEEE Computer Society Press), 124-134.
[36] Richard Feynman, http://en.wikipedia.org/.
[37] David Deutsch, http://en.wikipedia.org/.
[38] Grover, L. K., 1996, "A fast quantum mechanical algorithm for database search", *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, STOC'96 (ACM, New York), p. 212.
[39] Quantum computer, http://en.wikipedia.org/.
[40] Qubit, http://en.wikipedia.org/.
[41] Integrated quantum computing system with 128 qubit chipset, http://www.dwavesys.com/, D-Wave, Erişim: Haziran 2011.
[42] Shor's algorithm, http://en.wikipedia.org/.
[43] Elliott, C., "Quantum cryptography", *Security & Privacy Magazine*, IEEE, Vol. 2, Issue: 4, July-Aug. 2004, sf. 57–61.
[44] Mullins, J., 2002, "Making unbreakable code", *Spectrum*, IEEE, Volume: 39, Issue: 5, sf 40–45.
[45] Nielsen, M. A., Chuang, I. L., *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
[46] Williams, C. P., Clearwater, S. H., *Explorations in QUANTUM COMPUTING*, Springer-Verlag NewYork, Inc. TELOS,1998.
[47] Trappe, W., Washington, L. C., *Introduction to Cryptography with Coding Theory*, Prentice-Hall, Inc. 2002.
[48] http://www.biltek.tubitak.gov.tr/
[49] http://www.quantum-computer.com/
[50] http://ww.magiqtech.com.
[51] http://www.quantiki.org/.
[52] http://www.random.org/.
[53] http://www.qubit.org/.
[54] http://arxiv.org/.
[55] Toyran, M., "EEB Mühendisliklerinde Kuantum Hesaplama Eğitimi", *3. EEB Mühendislikleri Eğitimi Sempozyumu*, 2006.

[1] Böylece, ülkemizin örneğin klasik kriptolojide elde ettiği ***bağımsızlık*** ve ülke dışına yayılan ***başarı***sı kuantum kriptolojide de tekrarlanabilir.

Kaos Tabanlı Yeni Bir Blok Şifreleme Algoritması

Fatih Özkaynak[1] Ahmet Bedri Özer[2] Sırma Yavuz[3]

[1]Yazılım Mühendisliği Bölümü, Fırat Üniversitesi, Elazığ
[2]Bilgisayar Mühendisliği Bölümü, Fırat Üniversitesi, Elazığ
[3]Bilgisayar Mühendisliği Bölümü, Yıldız Teknik Üniversitesi, İstanbul

[1]ozkaynak@firat.edu.tr [2] bedriozer@firat.edu.tr
[3] sirma@ce.yildiz.edu.tr

Özetçe

Bilimin birçok dalında uygulama alanı bulunan kaos teorisinin bilgisayar bilimlerindeki yaygın kullanım alanlarından biride kaotik sistemleri kullanarak yeni kriptolojik sistemlerin tasarlanmasıdır. Bu çalışmada kaos ve kriptoloji bilimleri arasındaki doğal ilişkiden yararlanılarak simetrik şifreleme algoritmalarının nasıl tasarlanabileceği açıklanmıştır. Çalışmada ilk olarak kaos tabanlı kriptolojik sistemlerin teorisi açıklanmış ardından kaos tabanlı blok şifreleme algoritması örneği verilmiştir. Teorik analizler ve bilgisayar simülasyonları önerilen algoritmaların blok şifreleme tasarımları için gerekli tüm performans gereksinimlerini karşıladığını, etkili ve uygulanabilir bir yapıda olduğunu göstermiştir.

1. Giriş

Kriptoloji, haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan, temeli matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bütünüdür. Kriptoloji biliminin kriptografi ve kriptanaliz olarak adlandırılan iki temel alt dalı bulunmaktadır. Kriptografi, belgelerin şifrelenmesi ve şifresinin çözülmesi için kullanılan yöntemleri araştırırken; kriptanaliz ise kriptolojik sistemlerin kurduğu mekanizmaları inceler ve kırmaya çalışır [1].

Bazı araştırmacılar kaotik sistemlerin gösterdikleri özel davranışlardan dolayı; kaos ve kriptoloji bilimleri arasında güçlü bir ilişki olduğunu vurgulamıştır [2]. 1990'lardan beri blok şifreler, akan şifreler, özet (hash) fonksiyonları, görüntü şifreleme algoritmaları gibi birçok şifreleme sisteminin tasarlanmasında da kaotik sistemleri kullanmışlardır.

Kaos doğrusal olmayan dinamik sistemlerde bulunan gerekirci (deterministik) ve rasgele benzeri bir süreçtir. Kaotik sistemlerin önemli karakteristiklerinden biri sistem parametreleri ve/veya başlangıç koşullarına duyarlı olmasıdır [3]. Sistem parametrelerinde ve/veya başlangıç koşullarında yapılan küçük bir değişiklik, sistem yörüngelerinde büyük değişimlere sebep olmaktadır. Kaosun bu temel karakteristiği; Shannon'un mükemmel gizlilik teorisi için vurguladığı ve modern şifreleme sistemleri için temel karakteristikler olan karıştırma (confusion) ve yayılma (diffusion) özellikleri ile örtüşmektedir [2–4].

Bu çalışmada kaos ve kriptoloji bilimleri arasındaki doğal ilişkiden yararlanılarak kaos tabanlı yeni kriptolojik sistemlerin nasıl tasarlanabileceğine ilişkin teorik temel açıklandıktan sonra kaotik sistemleri temel alan bir blok şifreleme algoritması örneği verilmiştir. İncelenen blok şifreleme mimarisi kaos tabanlı dinamik yer değiştirme kutularını temel almaktadır. Teorik analizler ve bilgisayar simülasyonları önerilen yeni kaos tabanlı dinamik yer değiştirme tablosunun blok şifreleme tasarımları için gerekli tüm performans gereksinimlerini karşıladığını, etkili ve uygulanabilir bir yapıda olduğunu göstermiştir.

Çalışmanın geri kalan kısmı aşağıdaki gibi düzenlenmiştir. Kaos ve kriptoloji bilimleri arasındaki ilişkinin teorik temelleri bölüm 2'de açıklanmıştır. Blok şifreleme algoritmaları hakkında özet bilgiler bölüm 3'de verilmiştir. Çalışmada önerilen algoritmanın detaylı mimarisi bölüm 4'de açıklanmıştır. Önerilen algoritmanın performans ve güvenlik analizleri bölüm 5'de yapılmıştır. Son bölümde ise sonuçlar tartışılarak çalışma özetlenmiş ve önerilerde bulunulmuştur.

2. Kaos Tabanlı Kriptoloji

Daha önce belirtildiği gibi kaos ve kriptoloji bilimleri arasında doğal bir ilişki bulunmaktadır. Bu ilişki Shannon'un herhangi bir şifreleme sisteminin güvenilir olması için sahip olması gereken özellikler olan karıştırma ve yayılma özellikleri ile kaotik sistemlerin başlangıç koşullarına duyarlı olması ve doğrusal olmaması özellikleriyle örtüşmesinden ortaya çıkmaktadır [2–4].

Karıştırma özelliğine sahip şifreleme sistemlerinde; her anahtar için şifreleme algoritması öyle olmalıdır ki, açık metin ve şifreli metin arasındaki yapılar arasında istatistiksel bağlılık olmamalıdır. Bu özelliğin olabilmesi için anahtar ve açık metinin her bitinin şifreli metini etkilemesi gerekmektedir [1].

Yayılma özelliğine sahip bir şifreleme sistemi için ise; şifreli metin ile anahtar arasındaki ilişkiyi mümkün olduğunca karmaşık olmalıdır. Diğer bir deyiş ile yayılma, anahtarın açık ve şifreli metine bağlılığının kriptanaliz için faydalı olmayacak kadar karmaşık olması demektir. Yani şifreleme sistemini tanımlayan eşitliklerin doğrusal olmaması ve karışık olması sağlanmalı böylece şifreleme algoritmasından anahtarı bulmanın imkânsız olması gerekir [1].

Karıştırma ve yayılma özellikleri dinamik sistemlerin sahip olduğu özelliklerdir. Kaotik sistemlerin başlangıç koşulları ve/veya kontrol parametrelerine bağımlılığı bir kaotik sistemden üretilen yörüngeler boyunca yayılma özelliğini sağlar. Başka bir ifade ile herhangi bir yörünge üzerinde alınan her bir değer başlangıç koşulları veya kontrol

parametrelerine bağımlıdır. Başlangıç koşulları ve/veya kontrol parametrelerindeki en ufak bir değişiklik ile tamamen farklı yörüngeler oluşacağından bu bağımlılık çok güçlüdür. Sonuç olarak kaotik sistemler başlangıç koşulları ve/veya kontrol parametrelerine bağımlılığı yayılma özelliğine sahiptir [5].

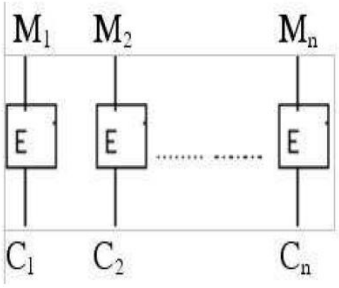
Kaotik sistemlerin ergodiklik özelliği kaotik yörüngenin uzun vadeli davranışının başlangıç koşulları veya kontrol parametrelerine bağımlılığını ortaya koymaktadır. Buradan bir kaotik sistemden üretilen yörüngelerin bir kümesi ile istatistikî olarak başlangıç koşulları ve/veya kontrol parametrelerinin tam değerlerinin çıkarılmasının mümkün olmadığı görülebilinir. Sonuç olarak kaotik sistemler karıştırma özelliğini göstermedir [5].

Özetleyecek olursak kaotik sistemlerin başlangıç koşullarına ve/veya kontrol parametrelerine duyarlılığı yeni kriptolojik sistemlerin tasarlanmasında kullanılabilir.

3. Blok Şifreleme Algoritmaları

Blok şifreleme algoritmaları birçok uygulamada kullanılan simetrik şifreleme algoritmaları için temel birleşenlerden biridir. Blok şifreleme algoritmaları açık metinleri ardışık bloklara böler ardından her bloğu şifreleyerek şifreli metin bloklarına dönüştürmektedir. Şekil 1'de bir blok şifreleme sistemi şematik olarak gösterilmiştir. Şekilden görülebileceği gibi $M_1, M_2, \ldots, M_n$ her biri k bitten oluşan açık metinlerin bloklarını göstermektedir. Benzer şekilde $C_1, C_2, \ldots, C_n$ ise açık metin bloklarına karşılık gelen şifrelenmiş metin bloklarını göstermektedir. Şekilde E şifreleme algoritmasını temsil etmektedir. Çoğu blok şifre sistemlerinde blok uzunluğu 64 bittir. İşlemcilerin hızı arttıkça blok uzunluğu da artabilmektedir. Son yıllarda üretilen şifreleme sistemlerinde 128 bit blok uzunluğu kullanılmaktadır [1].

Bir blok şifreleme sisteminde, şifreli metin bloklarından birinin kaybolması, diğer blokların deşifre işleminde bir yanlışlığa neden olmaz. Bu blok şifreleme sistemlerinin en büyük avantajıdır. Blok şifre sistemlerinin en büyük dezavantajı ise şifreli metindeki birbirinin aynısı olan blokların, açık metinde de birbirinin aynı olmasıdır.



Şekil 1: Blok şifreleme sisteminin genel görünümü.

4. Önerilen Algoritma

Çalışmada önerilen yeni blok şifreleme algoritmasında kaotik sistemler kullanılarak oluşturulmuş dinamik yer değiştirme kutularını (Substitution Box, S-Box) temel alan bir tasarım mimarisi benimsenmiştir. Bu yüzden öncelikle S-Box oluşturmak için kullanılan algoritma açıklanmış ardından oluşturulan dinamik S-Box'lar kullanılarak blok şifreleme algoritmasının nasıl tasarlanacağı açıklanmıştır.

4.1. S-Box Tasarım Algoritması

S-Box DES, IDEA, AES gibi geleneksel blok şifreleme sistemlerindeki karıştırma özelliğini sağlayan doğrusal olmayan tek birleşendir. Bu yüzden güçlü şifreleme sistemlerinin tasarlanması için kriptolojik özellikleri iyi olan S-Box'ların tasarlanması gerekmektedir [6].

Literatürde S-box tasarımları için cebirsel teknikleri temel alan, sözde rasgele tabanlı veya sezgisel tabanlı yöntemler gibi birçok yöntem önerilmiştir. Bu yöntemlerden en popüleri AES şifreleme algoritmasında da kullanılan ters dönüşüm yöntemidir [7, 8]. Ancak son zamanlarda geliştirilen kriptanaliz yöntemlerinden cebirsel saldırı teknikleri bu tasarımlar için önemli bir tehdit oluşturmaktadır [9–14]. Bu yüzden cebirsel saldırılara karşı alternatif olabilecek yeni yöntemler araştırılmalıdır. Kaos tabanlı tasarımlar da modern şifreleme sistemlerinde kullanılan katı cebirsel teknikleri temel alan tasarımlara alternatif olmaya aday tasarımlardır.

Matematiksel olarak *n x n* boyutunda bir S-Box GF(2) üzerinde $S:\{0,1\}^n \rightarrow \{0,1\}^n$ şeklinde doğrusal olmayan bir dönüşümdür. n x n boyutunda S-Box'lar oluşturmak için kullanılan algoritma kaotik sistemin çıkışını 0 ile 2^n arasındaki sayılara dönüştürerek S-Box tasarımını gerçekleştirmektedir. Algoritmanın çalışması adım adım aşağıda açıklanmıştır. Ayrıca sözde kodu tablo 1'de verilmiştir.

Adım 1. Belirlenen başlangıç koşulları ve kontrol parametreleri için kaotik sistemin çıkışı hesaplanır.

Adım 2. Hesaplanan çıkış değeri A,$y_0y_1y_2y_3y_4y_5$ biçimindedir ve S-Box tablosunun hücreleri virgülden sonraki 6 dijit kullanılarak hesaplanmaktadır.

Adım 3. Her adımda kaotik sistemin çıkışından belirlenen 6 dijit içerisinden 3 dijit seçilerek işleme devam edilir bu seçim aşağıdaki şekilde yapılır.

$$y_0y_1y_2 \rightarrow y_1y_2y_3 \rightarrow y_2y_3y_4 \rightarrow y_3y_4y_5 \rightarrow y_4y_5y_0 \rightarrow y_5y_0y_1 \rightarrow y_0y_1y_2$$

Adım 4. $y_py_qy_r$ şeklinde 3 dijit seçildikten sonra bu üç dijitin oluşturduğu decimal değerin 2^n'e göre kalanı (modu) hesaplanarak 0 ile 2^n arasındaki sayılara dönüştürülür.

Adım 5. Elde edilen sayı tabloda mevcut değilse tabloya eklenir. Aksi takdirde adım 1'e gidilerek yeni bir değer hesaplanır ve işleme devam edilir.

Adım 6. Tablodaki tüm hücrelerin değerleri hesaplanıncaya kadar adım 1'den işleme devam edilir.

4.2. Şifreleme ve Şifre Çözme Algoritması

Önerilen şifreleme algoritmasının detayları aşağıda adım adım açıklanmıştır. Detaylı mimari için [15] incelenebilir.

Adım 1. Şifrelenecek *m* mesajı *l* byte (burada *l*=32 seçilmiştir) uzunluğunda bloklara (B_j) bölünür. Eğer blok uzunluğu *l*'den küçük ise bloğun sonuna 0 eklenir.

Adım 2. Bölüm 4.1'de açıklanan algoritma kullanılarak 32 tane 8 x 8 boyutunda S-Box üretilir. Farklı S-Box'lar üretmek için seçilen kaotik haritanın başlangıç koşulu veya kontrol parametreleri değiştirilebilinir.

Adım 3. Her bir bloğun S-Box'lar kullanılarak karıştırılması sağlanır. Ardından sola kaydırma işlemi gerçekleştirilir. Bu işlem *l*-1 defa tekrarlanır. Şifreleme mimarisi görsel olarak şekil 2'de gösterilmiştir.

Adım 4. $C_j = c_0 \oplus c_1 \oplus \ldots \oplus c_{l-1}$ hesaplanarak bloğun şifrelenmesi işlemi tamamlanır.

Şifre çözme işlemi de şifreleme sürecine benzer şekilde yapılır. Tek fark sola kaydırma işlemleri yerine sağa kaydırma yapılır. Yer değiştirme işlemleri için ise S-Box'ların tersi alınır.

5. Performans ve Güvenlik Analizleri

Güvenli blok şifreleme sistemleri geliştirmek için kriptolojik olarak güçlü S-Box tasarımlarının yapılması gerektiği daha önce belirtilmişti. Buradan hareketle şifreleme algoritmasının performans ve güvenlik analizleri için S-Box tasarım kriterleri göz önüne alınmıştır.

5.1. S-Box Tasarım Kriterleri

Kriptolojik olarak güçlü S-box'lar tasarlamak için genellikle beş kriter seçilmektedir [16–21]. Bunlar bijektif olma özelliği, doğrusal olmama kriteri, katı çığ kriteri, çıkış bitlerinin bağımsızlık kriteri ve olası giriş/çıkış XOR dağılımıdır.

5.1.1. Bijektif Olma Özelliği

Bir fonksiyon hem bire bir özelliğini hem de örten özelliğini sağlıyorsa bijectif bir fonksiyon olarak adlandırılmaktadır. Önerilen S-Box tasarım algoritmasıyla oluşturulan yapılar bu özelliği sağlamaktadır.

5.1.2. Doğrusal Olmama Kriteri

f(x) boolean fonksiyonun doğrusal olmaması Walsh spektrumuyla gösterilmektedir.

$$N_f = 2^{n-1}\left(1 - 2^{-n} \max_{\omega \in GF(2^n)} \left|S_{(f)}(\omega)\right|\right) \quad (1)$$

Walsh spektrumu aşağıdaki gibi tanımlanabilir.

$$S_{(f)}(\omega) = \sum_{\omega \in GF(2^n)} (-1)^{f(x) \oplus x \cdot \omega} \quad (2)$$

5.1.3. Katı Çığ Kriteri

Katı çığ kriteri ilk olarak Webster ve Tavares tarafından yayınlanmıştır [18]. Fonksiyon katı çığ kriterini sağlıyorsa tek bir giriş bitinde değişiklik olduğunda çıkış bitlerinin her birinin yarısının değişmesi olasılığı anlamına gelmektedir.

Verilen S-kutusunun tamamının katı çığ kriterini sağlayıp sağlamadığını tespit etmek için etkili bir metot [14]'da gösterilmiştir.

Tablo 1: S-Box tasarım algoritması sözde kodu

```
// S-Box'ın tüm elemanlarına başlangıçta -1 atanır
tablo[2n][2n]=-1
i=0, j=0, p=0, q=1, r=2;
while(i<2n)
{
      while(j<2n)
      {
            data=-1
            while(data tabloda mevcutsa)
            {
                  y=f(x)    //y=A.y0y1y2y3y4y5
                  x=y
                  data=ypyqyr mod (2n)
                  p=p+1(mod 6)
                  q=q+1(mod 6)
                  r=r+1(mod 6)
            }
            tablo[i][j]=data
            j=j+1
      }
      i=i+1;        j=0;
}
```

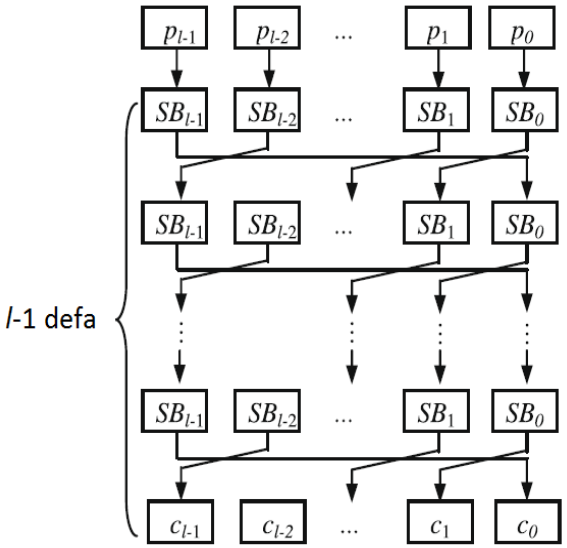
5.1.4. *Çıkış Bitlerinin Bağımsızlık Kriteri*

Bu kriter de ilk olarak Webster ve Tavares tarafından gösterilmiştir [18]. Şifreleme sisteminin güvenliği için gerekli olan diğer bir özelliktir. Tekbir açık metin bitlerinin tersiyle üretilen çığ vektörlerinin kümesi için tüm çığ değişkenleri çiftlerinin bağımsız olması anlamına gelmektedir. Çığ değişken çiftleri arasındaki bağımsızlığın derecesini ölçmek için çiftler arasındaki korelasyon katsayı hesaplanmaktadır. Webster ve Tavares çalışmalarında S-Box'un iki çıkış bitlerinin boolean fonksiyonları olan f_j ve f_k BIC kriterini sağlıyorsa $f_j \oplus f_k$ ($j \neq k$, $1 \leq j, k \leq n$) nında doğrusal olmama ve katı çığ kriterlerini sağlamalıdır.

5.1.5. *Olası Giriş/Çıkış XOR Dağılımı*

Biham ve Shamir bir S-Box için giriş/çıkış XOR dağılım tablosundaki dengesizlikleri temel alan diferansiyel kriptoanalizi göstermişlerdir [22]. Çıkış değişimleri giriş değişimlerin bilgisinden elde edilebilir ve her bir çıkışın XOR değeri her giriş XOR için eşit olasılıklı olmalıdır. Yani eğer S-Box giriş/çıkış olasılık dağılımında kapalı ise S-Box'ın diferansiyel kriptoanalize karşı dirençlidir. Verilen bir f haritası için diferansiyel yaklaşım olasılığı diferansiyel dayanıklılık ölçülerek aşağıdaki gibi hesaplanır.

$$DP_f = \max_{\Delta x \neq 0, \Delta y} \left(\frac{\#\{x \in X \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^m} \right) \quad (5)$$



Şekil 2: Blok şifreleme mimarisi.

5.2. Performans Karşılaştırmaları

Son zamanlarda Wang ve diğerleri [15] kaotik Tent haritasını temel alarak oluşturdukları dinamik S-Box'ları kullanan bir blok şifreleme algoritması önermişlerdir. Karşılaştırma yapabilmek için bu çalışmada önerilen S-Box tasarımı içinde kaotik Tent harita temel alınarak dinamik S-Box'lar üretilmiştir.

Doğrusal olmama ölçütü bakımından Wang ve diğerlerinin çalışmasında ortalama değer 104 civarında iken bizim çalışmamızda ise bu değer 105 civarındadır.

Katı çığ kriteri için ise Wang ve diğerleri değerlerin 0.485 ile 0.515 arasında değiştiğini göstermişlerdir. Bizim çalışmamızda ise minimum ve maksimum değerler 0.375 ile 0.601 arasında değişmektedir. Ancak ortalama değere bakıldığında 0.5002 ile ideal değer olan 0.5 değerine çok yakın olduğu görülmektedir.

Olası giriş/çıkış XOR dağılımı ölçütü bakımından karşılaştırıldığında ise Wang ve arkadaşlarının çalışmasında maksimum değerlerin 10 ile 12 arasında değiştiği görülmektedir. Bizim çalışmamızda ise maksimum değerler 8 ile 10 arasında değişmektedir.

6. Sonuçlar

Bu çalışmada dinamik S-Box'ları kullanan yeni bir blok şifreleme algoritması önerilmiştir. Literatürdeki benzer çalışmalarla kıyaslandığında kaotik S-Box üreteç algoritması kriptolojik olarak daha güçlüdür. Ayrıca önceki çalışmalarda önerilen algoritmaların kriptolojik olarak güçlü olması önemli ölçüde seçilen kaotik sisteme bağımlı iken bu çalışmada önerilen dinamik S-Box tasarım algoritmasında ise farklı kaotik sistemler için bile başarılı sonuçların elde edildiği gözlenmiştir.

Literatürdeki birçok kaos tabanlı S-Box tasarım algoritması incelendiğinde kaotik yörüngenin kullanılarak tablonun oluşturulmasının yanı sıra satır ve sütün bazında döndürme, başka bir kaotik sistem yardımıyla karıştırma, optimizasyon süreçlerinden faydalanma gibi çeşitli yöntemlerinde kullanıldığı görülmektedir. Bu tip ek işlemler kriptolojik özelliklerin artırılması bakımından olumlu

sonuçlar doğurmasına rağmen pratik uygulanabilirlik bakımından şifreleme süresinin artmasına sebep olduğu için önemli bir kısıt olarak ortaya koyulmaktadır. Bu çalışmada önerilen algoritmanın bu tip ek işlemlere ihtiyaç duymaması geliştirilen yöntemin önemli avantajlarından biridir.

İlerideki çalışmalarda hem dinamik S-Box oluşturma algoritmasının hem de blok şifreleme mimarisinin daha fazla nasıl geliştirileceği araştırılacaktır.

7. Kaynakça

[1] Paar, C. Pelzl, J., Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010.

[2] Amigo J. M., Kocarev L., Szczapanski J., Theory and practice of chaotic cryptography, Physics Letters A, 366:211-216, 2007.

[3] Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers. IEEE Trans Circ Syst—I, 48(2):163–169, 2001

[4] Alvarez, G. Li, S., Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems, International Journal of Bifurcation and Chaos,16: 2129-2151, 2006

[5] Arroyo D., Framework for the analysis and design of encryption strategies based on discrete time chaotic dynamical system, Instituto de Fı´sica Aplicada, 2009

[6] T. Cusick, P. Stanica, Cryptographic Boolean Functions and Applications, Academic Press, 2008.

[7] K. Nyberg, Differentially uniform mappings for cryptography, Proceedings of Eurocrypt'93 Lecture Notes in Computer Science Springer Berlin 765 (1994) 55-64.

[8] J. Daemen, V. Rijmen, AES Proposal: Rijndael, First Advanced Encryption Conference, California, 1998.

[9] G. Bard, Algebraic Cryptanalysis. Springer-Verlag, 2009.

[10] N. Courtois, G. Bard, Algebraic Cryptanalysis of the Data Encryption Standard. Lecture Notes in Computer Science 4887 (2007) 152-169.

[11] M. Youssef, S. E. Tavares, G. Gong, On Some probabilistic approximations for AESlike s-boxes. Discrete Mathematics 306 (2006) 2016-2020.

[12] L. Jing-mei, W. Bao-dian, C. Xiang-guo, W. Xin-mei, Cryptanalysis of Rijndael S-box and improvement, Applied Mathematics and Computation 170 (2005) 958-975.

[13] M. Youssef, S. E. Tavares, Affine equivalence in the AES round function, Discrete Applied Mathematics 148 (2005) 161-170.

[14] Y. Nawaz, K. C. Gupta, G. Gong, Algebraic Immunity of S-Boxes Based on Power Mappings: Analysis and Construction. IEEE Transactions on Information Theory, 55-9 (2009) 4263-4273.

[15] Wang Y, Wong K, Liao X, Xiang T. A block cipher with dynamic S-boxes based on tent map. Commun Nonlinear Sci Numer Simulat, 14:3089–3099, 2009

[16] M. Dawson, S. Tavares, Adv Cryptol Proc Eurocrypt_91. Lecture Notes Computer Sci, 352–367, 1991

[17] Detombe J, Tavares S. Constructing large cryptographically strong S-boxes. In: Advances in cryptology: Proc. of crypto'92. Lecture notes in computer science, 1992.

[18] Webster, S. Tavares, On the design of S-boxes, In: Advances in cryptology: Proc. of crypto'85. Lecture notes in computer science, 1986 pp. 523–534.

[19] C. Adams, S. Tavares, Good S-boxes are easy to find, In: Advances in cryptology: Proc. of crypto'89. Lecture notes in computer science, 1989. p. 612–615.

[20] J. Detombe, S. Tavares, Constructing large cryptographically strong S-boxes, In: Advances in cryptology: Proc. of crypto'92. Lecture notes in computer science, 1992.

[21] M. Dawson, S. Tavares, An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks, In: Advances in cryptology: Proc. of eurocrypt'91. Lecture notes in computer science, 1991. pp. 352–367.

[22] E. Biham, A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Journal of Cryptology, 4 (1991) 3-72.

Kısmi Anahtarlı Çok Alıcılı Bir Şifreleme Anahtar Yönetimi Algoritması

Dindar Öz[1] Ersin Gülaçtı[2] Işıl Öz[3]

[1,2]TÜBİTAK BİLGEM, Gebze Kocaeli
[3]Boğaziçi Üniversitesi, Bilgisayar Mühendisliği, İstanbul

[1]e-posta: oz@uekae.tubitak.gov.tr [2] e-posta: egulacti@uekae.tubitak.gov.tr
[3] e-posta: isil.oz@boun.edu.tr

Özetçe

Bu bildiride, RFC 5652'de belirtilen Kriptografik Mesaj Biçimi (Cryptographic Message Syntax) standardında tanımlanan şifreli zarf veri yapısı temel alınarak geliştirilen bir gruba şifreleme yöntemi önerilmektedir. Eşik kriptolojisinin temel çalışma alanlarından biri olan sır paylaşımı tekniklerinden biri kullanılarak simetrik anahtarın alıcılar arasında şifreli bir şekilde paylaştırıldığı bu yöntemle, birden fazla alıcının aynı anda hazır bulunması koşuluyla erişim sağlanabilmesi gereken verilerin şifrelenmesi amaçlanmıştır.

1. Giriş

Bir elektronik belgenin oluşturulması ve kullanılması sırasında karşı karşıya kaldığı çeşitli tehditler bulunmaktadır. Bu tehditler kullanılan sistemlerdeki açıklık ve zayıflıklar, belge içeriğini yetkisiz kişilerin görmesi, belge içeriğini yetkisiz kişilerin değiştirmesi, belgeyi hazırlayanın bunu sonradan inkar etmesi, belgeyi hazırlayan kişinin kimliğinin doğru bir şekilde belirlenememesi, belgenin hazırlandığı tarihin saptanamaması olarak sıralanabilir.

Bir elektronik belge oluşturulurken bu tehditlere karşı önlemler alınmalıdır. Bu önlemler standartlarda tanımlandığı üzere belge üzerinde uygulanmalıdır. Buna göre elektronik belge oluşturulurken:

- Belgeyi oluşturan kişinin kimliğinin önemli olduğu durumlarda, inkar edememezliği sağlamak ve belge değiştirmeyi engellemek amacıyla oluşturan kişi ve onay silsilesindeki amirleri tarafından elektronik olarak imzalanmalıdır (CADES [1] veya XADES [2] standardında tarif edildiği şekilde).
- Belgenin oluşturulma tarihi önemliyse belgeye zaman damgası eklenmelidir (CADES [1] veya XADES [2] standardında tarif edildiği şekilde).
- Belgenin içeriği yetkisiz kişilerden korunmak isteniyorsa şifrelenmelidir (RFC 5652 (CMS) [3] standardında tarif edildiği şekilde).

Bir elektronik belgenin güvenlik nedeniyle sadece belirli kişilerce görülebilmesi gerekebilir. Belgeyi hazırlayan taraf, belge içeriğinin gizli kalmasını ve yetkisiz kişilerce okunmasını engellemek isteyebilir. Bu amaçla belgenin taşıdığı verinin gizliliğini sağlamak için şifreleme yöntemleri kullanılmalıdır. Elektronik belgenin şifrelenmesi CMS (Cryptographic Message Syntax) standardında tanımlanmıştır [3]. Bu standartta belirtilen yapı kullanılarak farklı amaç ve kapsamda şifreleme işlemleri yapılabilmekte, şifreli zarf veri yapısı (enveloped data) oluşturulabilmektedir.

Bu çalışmada eşik kriptolojide [5, 7] kullanılmakta olan sır paylaşım tekniklerinin [5, 6] CMS standardına uyarlanması amaçlanmıştır. Bu sır paylaşım metodu ile içerik şifreleme anahtarının şifreli veri alıcıları arasında paylaştırılması sağlanmıştır. Çalışma kapsamında CMS standardında belirtilen yapı temel alınarak gruba şifreleme anahtar yönetimi algoritması önerilmektedir. Bu algoritma, standartta tanımlanan şifreli zarf yapısının alıcı bilgisi kısmı için yeni bir yapı sunarak gruba şifreleme sürecini mümkün kılmaktadır. Bu veri yapısı kullanılarak şifreli verinin bir tek alıcının erişimine açılmaması gereken birden fazla alıcının bir arada erişebileceği ya da şifreli veriye güvenilir bir özel alıcının kontrolünde erişim sağlanması gereken durumlarda şifreli belge oluşturmayı sağlamaktadır.

Bildirinin bundan sonraki kısmı şu şekilde düzenlenmiştir: 2.bölümde belge şifreleme ve belge şifreleme sürecinin tanımlandığı standartlar hakkında genel bilgi verilmiştir. Önerilen grup alıcı bilgisi algoritması 3.bölümde açıklanarak, 4.bölümde algoritmanın kriptografik açıdan ve performans açısından değerlendirilmesi yapılmıştır. 5.bölümde bu algoritma ile oluşturulmuş zarf yapısının kullanım alanları tartışılmıştır. Bildiri sonuç bölümüyle tamamlanmaktadır.

2. Belge Şifreleme

Elektronik verinin korunmasına yönelik veri yapıları, CMS (Cryptographic Message Syntax) standardında tanımlanmıştır [3]. CMS yapısı, genel olarak elektronik imza, özet, şifre mesaj yapılarını ASN1 [4] formatında tanımlayan standarttır. Bu standarda göre oluşturulacak kriptografik mesaj yapısı, içerik tipi ve içerik bilgilerinden oluşmaktadır. Şifreleme işleminde, veri bir *ContentInfo* ASN1 yapısı içerisinde şifreli olarak saklanır.

```
ContentInfo ::= SEQUENCE {
    contentType ContentType,content [0]
    EXPLICIT ANY DEFINED BY contentType
}

ContentType ::= OBJECT IDENTIFIER
```

Zarf verisi olarak adlandırılan şifreli belge (*EnvelopedData*) hazırlanırken *ContentType* değeri *id-EnvelopedData* olarak belirtilir ve içerik *EnvelopedData* yapısı içerisinde kodlanarak *ContentInfo* yapısının *content* değerine kaydedilir.

```
EnvelopedData ::= SEQUENCE {
    version CMSVersion,
    originatorInfo [0] IMPLICIT
          OriginatorInfo OPTIONAL,
    recipientInfos RecipientInfos,
    encryptedContentInfo
          EncryptedContentInfo,
    unprotectedAttrs [1] IMPLICIT
          UnprotectedAttributes OPTIONAL }

OriginatorInfo ::= SEQUENCE {
    certs [0] IMPLICIT CertificateSet OPTIONAL,
    crls [1] IMPLICIT RevocationInfoChoices
    OPTIONAL
}

RecipientInfos ::= SET SIZE (1..MAX) OF
RecipientInfo

EncryptedContentInfo ::= SEQUENCE {
    contentType ContentType,
    contentEncryptionAlgorithm
    ContentEncryptionAlgorithmIdentifier,
    encryptedContent [0] IMPLICIT
        EncryptedContent OPTIONAL
}

EncryptedContent ::= OCTET STRING

UnprotectedAttributes ::= SET SIZE (1..MAX) OF
Attribute
```

EnvelopedData veri yapısındaki *version* değeri olarak RFC5652'de belirtilen koşul ağacına uygun olarak 0 kullanılır. *OriginatorInfo* alanı kullanılmaz. *EnvelopedData* veri yapısında, şifreli belgeyi açması istenen alıcılar ile ilgili bilgiler *RecipientInfo* listesi şeklinde saklanır.

```
RecipientInfo ::= CHOICE {
       ktri KeyTransRecipientInfo,
       kari [1] KeyAgreeRecipientInfo,
       kekri [2] KEKRecipientInfo,
       pwri [3] PasswordRecipientinfo,
       ori [4] OtherRecipientInfo
}
```

Şifreli zarf veri yapısı oluşturulurken aşağıdaki adımlar takip edilir:

- İçerik şifreleme algoritmasına uygun simetrik bir içerik şifreleme anahtarı (K) rastgele şekilde üretilir.
- Üretilen K her bir alıcı için anahtar yönetimi algoritmasına göre şifrelenir. Bu şifrelemenin detayları anahtar yönetim algoritmasına göre değişir.
- Şifreli K ve alıcıya ait bilgiler kullanılarak her bir alıcı için Alıcı Bilgisi (*RecipientInfo*) yapısı oluşturulur.
- İçerik, K ile simetrik olarak şifrelenir.
- Alıcı Bilgisi yapıları ve şifreli içerik bir araya getirilerek şifreli zarf veri yapısı oluşturulur.

RFC5652'de anahtar taşıma (key-transport), anahtar anlaşma (key-agreement), anahtar şifreleme anahtarı (key-encrption-key) ve parola tabanlı (password-based) olmak üzere dört farklı anahtar yönetimi algoritması tanımlanmıştır.

KeyTransRecipientInfo veri yapısı, içerik anahtarının tamamının her bir alıcıya asimetrik olarak şifrelenerek aktarıldığı anahtar taşıma modelidir. Alıcının veriyi şifreleyen ile gizli bir anahtar üzerine anlaştığı anahtar anlaşması algoritmaları için *KeyAgreeRecipientInfo* veri yapısı kullanılır. İçerik şifreleme anahtarının daha önceden alıcılara dağıtılmış simetrik bir anahtar ile şifreli bir şekilde aktarıldığı yöntemde *KEKRecipientInfo* veri yapısı kullanılır. *PasswordRecipientInfo* yapısı ise içerik şifreleme anahtarının alıcılara parola tabanlı olarak şifrelenerek aktarıldığı anahtar yönetim algoritmasında kullanılır. Bunlardan farklı bir anahtar yönetimi uygulanmak istenildiğinde *OtherRecipientInfo* veri yapısı kullanılabilir.

3. Grup Şifreleme

Bu çalışmada RFC 5652'de tanımlanan anahtar yönetim algoritmalarına ilave olarak anahtarı gruba şifreleme tipinde özel bir anahtar yönetimi algoritması sunulmaktadır.

3.1. Grup Alıcı Bilgisi

Grup Alıcı Bilgisi (*GroupRecipientInfo*) olarak tanımlanan bu yapı, RFC 5652'de belirtilen *KeyTransRecipientInfo* yapısına benzemektedir. Temel fark simetrik şifreleme anahtarının şifreli olarak *KeyTransRecipientInfo* yapısındaki tamamının saklanması yerine grup içerisindeki bütün alıcılara paylaştırılarak saklanmasıdır. Anahtarın alıcılara paylaştırılması için eşik kriptolojisinde kullanılan temel sır paylaşımı algoritmalarından Basit Sır Paylaşımı (Trivial Secret Sharing) yöntemi [8] kulanılmıştır. Bu yöntemde her bir alıcı için simetrik anahtar ile aynı uzunlukta rastgele bir veri üretilir. Üretilen bu verilerin mantıksal XOR işlemine tabi tutulması neticesinde oluşan değer, simetrik anahtar olarak kullanılır. Grup alıcı bilgisi elemanları ASN gösterimi olarak aşağıdaki gibidir:

```
GroupRecipientInfo ::= SEQUENCE {
  gid                 INTEGER,
  groupSize           INTEGER OPTIONAL,
  rid                 RecipientIdentifier,
  keyEncryptionAlgorithm
       KeyEncryptionAlgorithmIdentifier,
  encryptedPartialKey EncryptedKey
}
```

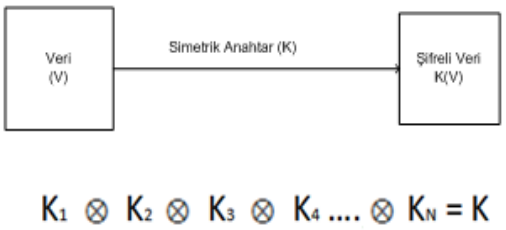
rid ve *keyEncryptionAlgorithm* alanlarının kullanımı ve içerikleri *KeyTransRecipientInfo* yapısındaki ile aynıdır. rid alıcının kimliğini tanımlamak için kullanılırken *keyEncryptionAlgorithm* alanı ise simetrik anahtarı şifrelemek için kullanılan asimetrik şifreleme algoritmasını belirtir. *gid* alanında alıcının simetrik anahtarı paylaştığı grup belirtilmektedir. *groupSize* alanı seçeneğe bağlı olarak eklenmiştir. Grubun eleman sayısını belirtir ve bir gruptaki bütün elemanların zarf yapısı içerisinde bulunup bulunmadığı kontrolü yapılırken kullanılabilir. Bu alanın olmadığı durumlarda gruptaki eleman sayısı zarf yapısı içerisinde aynı *gid* ile belirtilen *GroupRecipientInfo* yapısındaki alıcı sayısı kadardır. Alıcının kendisine verilen simetrik anahtarın kendi kapalı anahtarı ile şifrelenmiş hali *encryptedPartialKey* alanında yer alır.

3.2. Grup Alıcı Bilgisi Algoritması

Grup alıcı bilgisi algoritması ile zarf verisi oluşturmak için aşağıdaki adımlar takip edilir:

1) Simetrik Şifreleme (Şekil 1):

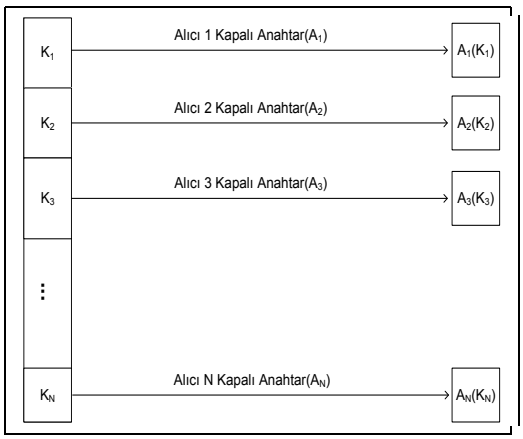
- İçerik şifreleme algoritmasına göre uygun anahtar boyunda ve alıcı sayısı adedince K_i kısmi anahtarları oluşturulur.
- Oluşan kısmi anahtrarların mantıksal XOR işlemine tabi tutulması neticesinde K simetrik anahtarı oluşturulur.
- Veri (V) simetrik anahtar (K) ile şifrelenerek şifreli veri (K(V)) oluşturulur.



*Şekil 1:*Simetrik şifreleme

2) Asimetrik şifreleme (Şekil 2):

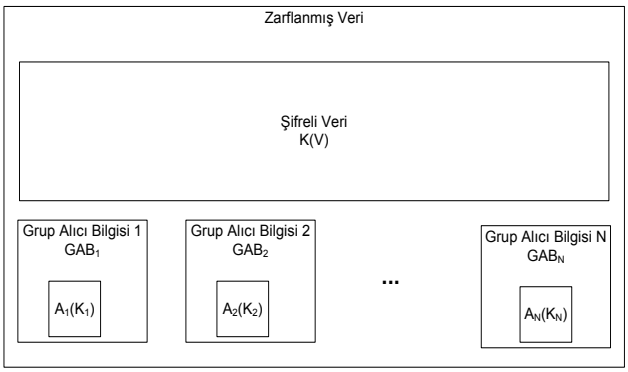
- Her alıcı (A_i) kendi kapalı anahtarı ile kendisine düşen kısmi anahtarı (K_i) asimetrik olarak şifreleyerek şifreli anahtar parçacığını ($A_i(K_i)$) oluşturur.
- Bu şifreli anahtar parçacıkları her alıcı (A_i) için İlgili Grup Alıcı Bilgisi yapısı (GAB_i) içerisine yerleştirilir.



*Şekil 2:*Asimetrik şifreleme

3) Zarf yapısının oluşturulması (Şekil 3):

- Şifreli veri (K(V)) ve grup alıcı bilgilerinden (GAB) oluşan AlıcıBilgisi listesi bir araya getirilerek şifreli zarf veri yapısı oluşturulur.



Şekil 3: Grup alıcı bilgisi algoritmasına sahip zarf yapısı

Önerilen grup alıcı bilgisi algoritması, ASN1 veri yapılarına dayalı olarak gerçeklenmiştir. Bu algoritma kullanılarak oluşturulan şifreli zarf yapısına sahip örnek bir şifreli dosyanın ASN1 yapısı, Şekil 4'te gösterilmektedir. Bu örnekte şifreli veri, 10 ve 11 seri numaralı (*SerialNumber*) sertifikaya sahip iki (*GroupSize*) kullanıcının birlikte açabilecekleri bir yapıya sahiptir. Veriyi şifreleyen simetrik anahtarı parçalayarak oluşturulan kısmi anahtarlar, her bir kullanıcının açık anahtarı kullanılarak verilen şifreleme algoritması (*Key Encryption Algorithm*) ile şifrelenmiştir. Oluşturulan şifreli kısmi anahtar (*Encrypted Partial Key*) ilgili alıcı bilgisi alanına yerleştirilmiştir. Yapı içerisindeki şifreli verinin (*Encrypted Content*) çözülebilmesi için, her iki kullanıcının kapalı anahtarı kullanılarak şifreli kısmi anahtarlar çözülmelidir. Daha sonra bu şifresi çözülen kısmi anahtarlarla oluşturulan simetrik anahtar, şifreli verinin şifresini çözmede kullanılmalıdır.

```
  0 NDEF: SEQUENCE {     // ContentInfo
  2   9:    OBJECT IDENTIFIER envelopedData (1 2 840 113549 1 7 3)
 13 NDEF:  [0] {                        // Content-Start
 15 NDEF:   SEQUENCE {// EnvelopedData
 17   1:     INTEGER 0                  // Version
 20 452:     SET {                      // RecipientInfos
 24 223:      [4] {                     // RecipientInfo - OtherRecipientInfo
 27  11:       OBJECT IDENTIFIER '1 3 6 1 4 1 11311 10 3 1 3'
 40 207:       SEQUENCE {               // GroupRecipientInfo
 43   1:        INTEGER 1// GroupID
 49   1:        INTEGER 2// GroupSize
 52  50:        SEQUENCE {// RecipientIdentifier - IssuerAndSerialNumber
 54  45:         SEQUENCE {             // Issuer Name
 56  11:          SET {
 58   9:           SEQUENCE {
 60   3:            OBJECT IDENTIFIER countryName (2 5 4 6)
 65   2:            PrintableString 'tr'
      :           }
      :          }
 69  13:          SET {
 71  11:           SEQUENCE {
 73   3:            OBJECT IDENTIFIER
      :             organizationalUnitName (2 5 4 11)
 78   4:            PrintableString 'test'
      :           }
      :          }
 84  15:          SET {
 86  13:           SEQUENCE {
 88   3:            OBJECT IDENTIFIER commonName (2 5 4 3)
 93   6:            PrintableString 'issuer'
      :           }
      :          }
      :         }                        // END-OF IssuerName
101   1:        INTEGER 10               // SerialNumber
      :       }
104  13:       SEQUENCE {               // Key Encryption Algorithm
```

```
106   9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
117   0:         NULL
      :       }
119 128:       OCTET STRING             // Encrypted Partial Key
      :       A3 DD 77 76 EA 7C 82 1C EC 70 0C C7 89 4A C9 F2
      :       4D 54 2A 95 B5 B5 81 91 DF 5D D8 65 A2 43 23 33
      :       E0 A1 DA 32 70 78 10 7F 8C 6E 20 58 EF 85 B6 F9
      :       9A 60 43 61 A7 82 8A 35 3D E0 3B 24 54 8A 75 CC
      :       4B 90 D0 B6 81 BA BC 62 87 6B DA 08 08 3E E2 63
      :       A3 8B D8 89 D6 34 1A B2 43 1B EF FD BA 3F 74 D8
      :       DB F9 31 A1 B8 2F 02 98 FD BE 65 47 43 C6 61 AC
      :       23 8B F4 A3 E0 13 01 4D B7 13 0F 55 D3 2E 7D C2
      :     }
      :   }
250 223:    [4] {                      // RecipientInfo - OtherRecipientInfo
253  11:     OBJECT IDENTIFIER '1 3 6 1 4 1 11311 10 3 1 3'
266 207:     SEQUENCE {                // GroupRecipientInfo
269   1:      INTEGER 1                // GroupID
272   1:      INTEGER 1                // GroupIndex
275   1:      INTEGER 2                // GroupSize
278  50:      SEQUENCE {// RecipientIdentifier - IssuerAndSerialNumber
280  45:       SEQUENCE {              // Issuer Name
282  11:        SET {
284   9:         SEQUENCE {
286   3:          OBJECT IDENTIFIER countryName (2 5 4 6)
291   2:          PrintableString 'tr'
      :         }
      :        }
295  13:        SET {
297  11:         SEQUENCE {
299   3:          OBJECT IDENTIFIER
      :           organizationalUnitName (2 5 4 11)
304   4:          PrintableString 'test'
      :         }
      :        }
310  15:        SET {
312  13:         SEQUENCE {
314   3:          OBJECT IDENTIFIER commonName (2 5 4 3)
319   6:          PrintableString 'issuer'
      :         }
      :        }
      :       }                        // END-OF IssuerName
327   1:      INTEGER 11               // SerialNumber
      :     }
330  13:    SEQUENCE {                 // Key Encryption Algorithm
332   9:     OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
343   0:     NULL
      :   }
345 128:    OCTET STRING               // Encrypted Partial Key
      :     44 31 4B C3 A2 B7 50 F1 75 6B A7 23 0A 52 34 C7
      :     C6 3C 8B BE C8 50 B7 4E 26 3E 3E 76 EF AC 20 3A
      :     A8 78 7D 05 5E B1 FA 38 C6 2E 4D E4 B1 29 0C 3B
      :     3B 70 E3 C9 47 28 4E 02 9B 17 34 35 03 2B B0 7C
      :     05 F1 1E EE 78 29 01 58 89 B9 AD 6C 76 61 29 A4
      :     F5 A3 FE 13 FC 71 15 1D B6 42 1D 38 33 DD 74 E3
      :     5A 40 16 A6 F9 44 90 1A FE 97 B2 CE 2E E5 AF 9E
```

```
    :          2A 27 92 ED 87 A9 0C CB 18 A3 B2 34 5A 0F F1 DB
    :        }
    :      }
    :    }
476 NDEF:    SEQUENCE {
478  9:      OBJECT IDENTIFIER data (1 2 840 113549 1 7 1)     // Content Type
489  20:     SEQUENCE {
491  8:      OBJECT IDENTIFIER des-EDE3-CBC (1 2 840 113549 3 7)
501  8:      OCTET STRING AF 03 0C A3 12 F3 50 FD
    :    }
511 NDEF:    [0] {                    // Encrypted Content
513  8:      OCTET STRING 44 D1 51 F4 D7 AE A9 AC
523  8:      OCTET STRING A4 0D 38 76 22 40 4F C7
    :      }
    :    }
    :  }
    : }
```

Şekil 4: Grup alıcı bilgisi algoritması ile üretilmiş şifreli veri örneği

4. Kriptografik Değerlendirme

Gruba şifrelemede sır paylaşımı metodu olarak seçilen "Basit Sır Paylaşımı" tekniği uygulaması son derece basit olmasına karşın kriptografik olarak oldukça güvenli bir tekniktir. Gizli bilginin aralarında paylaştırıldığı kişi sayısı, kişi başına düşen sır parçacığının boyunu değiştirmediği için kişi sayısının artması asimetrik şifrelenen veri uzunluğunu etkilememektedir. Dolayısıyla gruptaki eleman sayısı, kullanılan asimetrik ve simetrik algoritmaların ve anahtar boylarının güvenliğini etkilememektedir.

Basit sır paylaşımının bir diğer karakteristik özelliği alıcılardan bir kısmının bir araya gelmesi ve kendi kısmi anahtarlarını birbirleriyle paylaşmalarının simetrik anahtar hakkında bir ipucu elde etmelerini sağlamamasıdır. Bu da gizli belgenin güvenliği açısından önemlidir.

Alıcılardan birinin kapalı anahtarını kaybetmesinin gizli veriye erişimi imkansız kılması, gruba şifrelemenin temel dezavantajlarından biridir. Bu açıdan değerlendirildiğinde gruba şifreleme, bilginin güvenliğini arttırırken erişilebilirliğini azaltmaktadır. Bir diğer problem, sır paylaşım metodunun esnek olmayışı mevcut şifreli bir belgeye yeni bir alıcı eklemenin bütün alıcıların şifreli kısmi anahtarlarının tekrar hesaplanması ve güncellenmesini gerektirmesidir. Şifre çözme işleminin standart anahtar şifreleme yönteminde bir tek asimetrik şifre çözme işlemi gerektirmesine karşın simetrik anahtarın sır paylaşımıyla saklandığı bu yöntemde gruptaki eleman sayısı adedince asimetrik şifre çözme gerektirmesi performans açısından bir diğer negatif özellik olarak düşünülebilir. Sır paylaşımı tekniği olarak basit sır paylaşımı tekniğinin seçilmesi, bir yandan da bu performans yükünü minimuma indirmeyi amaçlamaktadır. Çünkü basit sır paylaşımında kısmi anahtarlardan gerçek simetrik anahtarı elde etmek sadece mantıksal XOR işleminden ibarettir.

5. Grup Şifreleme Kullanım Alanları

Zarf yapısı için tanımlı standart alıcı bilgisi yapıları içerik şifreleme anahtarının tamamını bir alıcının erişimine sunar. Bu durum içeriğin alıcı tarafından başka bir bilgiye ve denetime ihtiyacı olmaksızın açılmasını mümkün kılar. Ancak gerek iş dünyasında gerekse şifrelemenin gerekli olduğu kurumsal, askeri vb benzeri diğer yerlerde şifreli verinin bir tek alıcının erişimine açılmaması gereken birden fazla alıcının bir arada erişebileceği ya da şifreli veriye güvenilir bir özel alıcının kontrolünde erişim sağlanması gereken senaryolar bulunmaktadır. Örneğin bir kurumda özel bir görevli (denetmen, yönetici vb.) nezaretinde erişilmesi istenen ve bu görevli onayı olmaksızın açılması istenmeyen dosyalar olabilir ya da kurumun gizli dosya yönetim protokolleri bunu gerektirebilir. Yine mesela bir şirketin sadece şirket binası içerisinde açılmasını istediği dökümanlar ve değerli şirket verileri bulunabilir. Bu dökümanların ilgili alıcılar tarafından açılabilmesini ancak sadece şirket içerisinde açılmasını dışarıya çıkarıldığında hiç bir şekilde açılamamasını garanti altına almak gerekir. Bazı özel belgelerin hukuki ve idari mevzuat gereği ancak tarafların tamamının aynı anda bir arada bulunmasıyla erişime sağlanması gerekebilir. Örneğin birçok ülkede uygulanmaya başlanan elektronik seçim sistemlerinde seçmenlerin oy verme bilgisi gibi bazı gizli veriler birçok yetkilinin aynı anda bir arada bulunmasıyla erişilebilecek şekilde düzenlenmiştir. Buna ilaveten, gizli verinin tek bir alıcının erişimine açılmasındansa; erişim hakkının birden fazla alıcıya paylaştırılması, tüm bu alıcıların gizli anahtarlarına aynı anda ulaşımı zorunlu kılacağından böyle bir şifreleme modeli erişim kolaylığını azaltsa da bilgi güvenliğini arttıracaktır.

Bütün bu senaryolardaki gereksinimleri diğer bütün önlem, kural ve düzenlemelere ilaveten kriptografik olarak veri üzerinde de karşılamak için kısmi anahtarlı grup alıcı bilgisi yapısı kullanılabilir. Özel görevli nezaretinde ulaşılması istenen dosyalar her bir alıcısı bu özel görevliyle gruplanarak bir grup alıcısı olarak tanımlanarak zarf yapısı oluşturulursa, her alıcı ancak bu özel görevliyle bir araya gelerek anahtarın tamamına ulaşabilir ve dosya şifresini çözebilir. Şirket dışarısında açılamaması istenen veriler için alıcılar şirketin fiziksel lokasyonu içerisinde sabitlenmiş bir donanımsal güvenlik modülünde saklı bir kapalı anahtarla gruplanarak grup alıcısı olarak tanımlanırsa, bu veriler şirket dışarısında hiç bir şekilde açılamayacaktır.

6. Sonuçlar

Bu çalışma kapsamında RFC 5652 Cryptographic Message Syntax (CMS) standardında tanımlanan şifreli zarf veri yapısı temel alınarak geliştirilen bir gruba şifreleme algoritması önerilmiş ve bu algoritma ASN1 yapıları kullanılarak gerçeklenmiştir. Önerilen yöntemde eşik kriptolojisinde kullanılan sır paylaşımı tekniklerinden Basit Sır Paylaşımı kullanılmıştır. Şifreleme işleminde kullanılan simetrik anahtar grup kullanıcılarına verilen rastsal kısmi anahtarların mantıksal XOR işlemine tabi tutulmasıyla oluşturulmuş ve bu sayede gizli veriye erişim hakkı alıcılar arasında paylaştırılmıştır. Veriye erişilebilirliğin azaldığı ve performans açısından şifre çözme ve yeni şifreci ekleme işlemlerinin daha zorlaştığı bu yöntemde temel motif, bilginin güvenliğinin arttırılması ve açık veriye erişim hakkının dağıtılmasıdır.

7. Kaynakça

[1] ETSI TS 101733 (v1.8.3) CMS Advanced Electronic Signatures (CADES), ETSI Electonic Signatures and Infrastructures (ESI), Ocak 2011 (http://pda.etsi.org/exchangefolder/ts_101733v010803p.pdf)

[2] ETSI TS 101903 (v1.4.2) XML Advanced Electronic Signatures (XADES), ETSI Electonic Signatures and Infrastructures (ESI), Aralık 2010 (http://pda.etsi.org/exchangefolder/ts_101903v010402p.pdf)

[3] RFC 5652 Cryptographic Message Syntax, Internet Engineering Task Force, Eylül 2009 (www.rfc-editor.org/rfc/rfc5652.txt)

[4] CCITT. Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1), 1988.

[5] Applied Cryptography, Second Edition, Bruce Schneier 527-528

[6] J.C. Benaloh,Secret Sharing Homomorphisms: Keeping Shares of a Secret. Advances in Cryptography – CRYPTO '86. Lecture notes in Computer Science, vol. 263. Springer-Verlag, New York, LNCS 263

[7] Yvo Desmedt. Threshold Cryptography. In GBrassard, editor, European Transactions on Telecommunications, 5(4): 449-457, July 1994.

[8] Giorgio Zanin, Secret Sharing Schemes and their Applications – SMART Periodic Meetings

Blakley'in Gizli Sır Paylaşımına dayalı DataMatrix ECC200 Kodlama

Vasif Nabiyev[1] Katira Soleyman Zadeh[2]

[1,2]Department of Computer Engineering, Karadeniz Technical University, Trabzon 61080, Turkey

[1] e-posta: vasif@ktu.edu.tr [2]e-posta: katirasole@gmail.com

Özetçe

Barkodlar, ticari ürünlerle birlikte, sağlık sistemi, askeri belgeler ve hassas iş verileri gibi sayısız uygulamalarda kullanılmaktadır. Bu bilgilerin çoğu gizli ve güvenli tutulmalıdır. Ancak barkodun içeriği doğrudan mobil cihazlar tarafından okunabilir. Makalede verilerin güvenliğinin artırılması için DataMatrix ECC200 kodu ile gizli paylaşıma dayalı şema önerilmektedir. Korumalı veri paylaşımı Blakley'in gizli paylaşım şemasına dayalı olarak gerçekleştirilmiştir. Önerilen bu şema içerisinde gizli veri paylara ayrılır ve sonra pay bilgileri DataMatrix etiketleri içerisine gömülür. Önerilen şema veri iletiminde güvenliği artırmaktadır.

1. Giriş

Barkodlar geleneksel sembol açısından anahtar alfanümerik bilgileri kodlamak için kullanılır ve sayısal sistemler bilgileri tarayarak okumaktadır. 1D ve 2D barkodların farklı türleri Tablo-1'de gösterilmiştir. Sayısal verinin kodlanması, tek-boyutlu (1D) barkodlar, ürün sevkıyat ve izleme, sistem güvenliği, süpermarketler vb gibi uygulamalar son iki yılda önemli bir rol oynamaktadır [1,2,3,4]. 2D barkod ile veri hem yatay hemde dikey yönde kodlanır. 2D sembolünde veri miktarı önemli ölçüde 1D sembolünde depolanandan daha büyüktür. 2D barkod çözümleri, özellikle açık olarak bilgi kodlama yerine basit bir kod bilgisi gerektiren uygulamalar için, geleneksel 1D barkodlarına göre daha fazla bilgi yoğunluğu sağlar. 2D barkod teknolojisinin birkaç uygulamaları, ürün etiketleme, izleme ve kontrol, mobil güvenlik, göç çek hizmetleri, sağlık hizmetleri, e-ticaret vb. dir. 2D barkodları üzerinde depolanan ürün açıklamalarını insanlar mobil cihazlar yardımıyla kolayca okuyabilirler. Bu gizli olması istenen veriler için de geçerlidir. Bu nedenle, verilerin güvenli şekilde korunması çok önemlidir. Gizli paylaşım, bu sorunu çözmek için sunulmuştur. Çalışmada, paylar için Blakley sır paylaşımı yöntemi ile oluşturulan veriler DataMatrix kodları içerisine gömülerek sistemin güvenirliği artırılmıştır [5,6,7].

1.1. Sır Paylaşımı

Gizli paylaşım şemaları, verinin iletiminde tek bir kişiye güvenmeden gerçekleştirilen uygulamalarda kullanılmaktadır. Gizli paylaşım şeması verilerin bütünlüğünün korunmasında güvenli bir yöntemdir. Bu şemada gizli bilgiyi ileten bir dağıtıcı ve sonlu sayıda katılımcılar $P=\{p_1,\ldots,p_n\}$ bulunmaktadır. d verisi n parçalara ayrılır $d_1,\ldots,d_n$ ve her d_i payı ilgili katılımcılar p_i $(1 \le i \le n)$ arasında dağıtılır. Bunun sonucunda, paylaşılan veri, veri bozulması ve kaybı sorununu azaltmak için ayrı ayrı paylarda saklanabilir. Gizli paylaşım şemasında:

1) eğer $P' = \{p_{i_1},\ldots,p_{i_j}\} \subset P$ yetkili pay kümesiyse, gizli veri elde edilmektedir.

2) eğer $P' = \{p_{i_1},\ldots,p_{i_j}\} \subset P$ yetkisiz pay kümesiyse, o zaman gizli veri bu paylardan yeniden elde edilmemektedir.

1979 yılında, Shamir ve Blakley ilk (k,n) eşik gizli paylaşım yöntemini önerdiler[8,9,10]. Bu şemalar sırasıyla, Lagrange polinomial interpolasyon ve afin hiperdüzlemlere dayanmaktadır. Makalede, Blakley yöntemine dayalı gizli bir paylaşım yöntemi önermektedir.

***Tablo1**:* 1D Barkodları ve 2D Barkodlar

1D barcodes	2D barcodes
Codabar 	Maxicode 
Extended Code 39 	DataMatrix 
EAN bookland 	Aztec Code 
UPC-A 	QR Code 

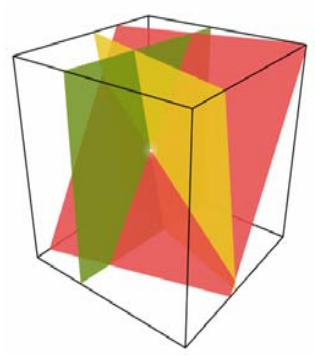
1.2. Blakley gizli paylaşım şeması

Blakely şeması, altdüzlem geometriye dayalıdır [11,12]. T boyutlu uzayda bir nokta sır olarak alınır ve paylar, bu nokta üzerinden geçen bir afin altdüzlemidir.

Afin altdüzlemi lineer denklem tarafından gösterilmektedir.

$$a_1 x_1 + \ldots + a_t x_t = b$$

T hiperdüzlemler alındığında, gizli nokta, bu t hiperdüzlemlerin kesişme noktasında yer alır. Şekil 1'de üç hiperdüzlemin sadece bir noktada (gizli noktası) nasıl kesiştiği gösterilmiştir.



Şekil 1: Gizli nokta üç düzlem arasındaki kesişme noktasında[12]

1.3. DataMatrix

Genel olarak, 2D barkodlarının iki türü vardır: PDF417 ve Kod 49 gibi yığılmış 2D barkod, QR kod ve DataMatrix gibi matrisli barkod. Makalede DataMatrix barkod teknolojisi kullanılmaktadır.DataMatrix barkodların CRC ve konvolüsyon hata düzeltme ve Reed-Solomon(RS) hata düzeltme tekniği olmak üzere iki versiyonu vardır. ECC200 Reed-Solomon hata düzeltmeli DataMatrix'ler yeni uygulamalar için tavsiye edilir [13,14,15]. 2D DataMatrix barkodu, MxN boyutlu bir görüntüdür. DataMatrix kare veya dikdörtgen yapılı bir semboldür. DataMatrix, daha fazla veri içermek için, hizalama şablonuyla ayrılmış ve böylece birden fazla veri bölgeleri sağlamaktadır. Veri bölgesi, bir vizör şablonu ile çevrilidir. DataMatrix barkod, barkodun %60'ı bulanık olsa bile çözülebilmektedir (barkod boyutuna bağlıdır) [16].
DataMatrix özellikleri kısaca aşağıda verilmiştir:

- Yüksek veri kapasitesi: Tek bir DataMatrix sembolü teorik olarak 3116 rakam, 2335 alfanümerik karakterleri veya 1556 byte tutabilir.
- Varsayılan karakter seti Latin-1 veya ANSI ASCII dir.
- Data Matrix baskı kalitesi: DataMatrix barkodunun kalitesini optimize etmek için 4 ila 5 pikselden daha küçük nokta ile basılmamaktadır.
- Veri Temsilciliği: 1 değeri için siyah piksel, 0 değeri için ise beyaz piksel kullanılır.
- Seçilebilir hata düzeltme tekniği:
  ECC 200: Reed-Solomon hata düzeltme.
  ECC 000 - 140: Konvolüsyonel hata düzeltme,
- Kodunu türü: Matrix
- Oryantasyon bağımsızlık: vardır

2. Önerilen Yöntem

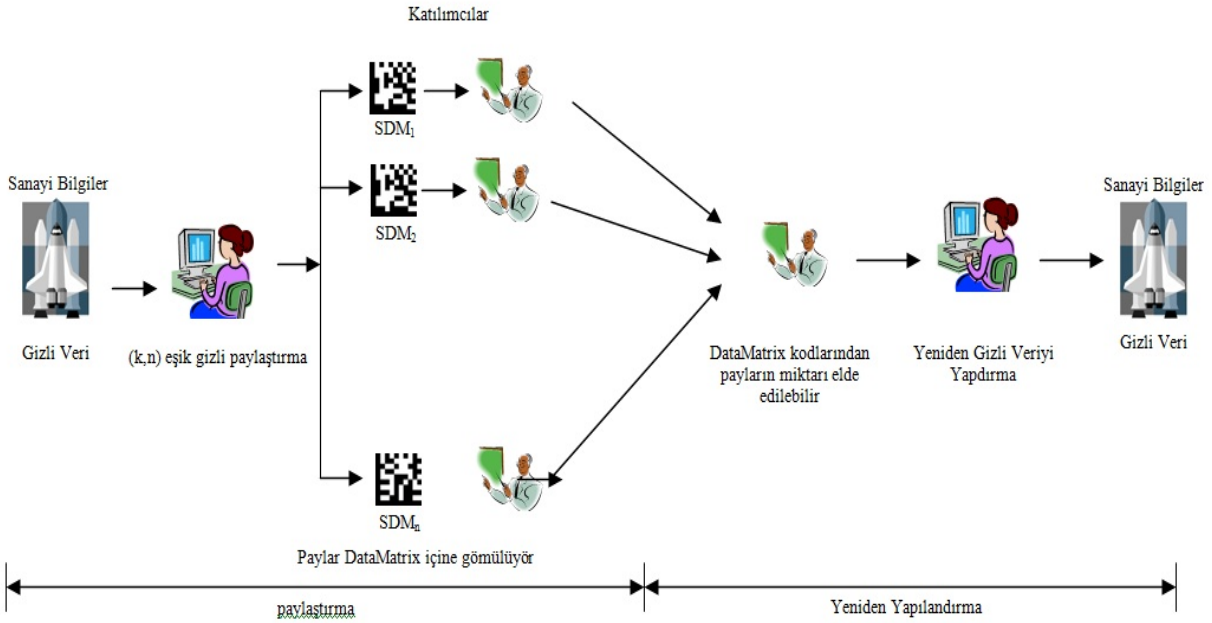
Önerilen yöntemde DataMatrix barkodların veri güvenliğini artırmak için, bir gizli paylaşım tekniği tasarlanmaktadır. Bu yöntemde, Blakley'in şeması aracılığıyla gizli veri paylara ayrılır ve her pay, bir DataMatrix taşıyıcı içine gömülür. Bu paylar katılımcılar arasında dağıtılır. Katılımcıların herhangi birisi kendi DataMatrix'inden gizli veriye ulaşmak isterse, ortaya çıkan veri anlamsız olacaktır. Gizli veri, sadece pay sayısı önceden tanımlanmış bir eşik değere eşit veya daha büyük olduğu zaman elde edilebilir.

2.1. Paylaştırma Algoritması

Önerilen şemada gizli veri, x dizisi için $x=(x_1,\ldots, x_n)$ aşağıdaki şekilde n hiperdüzlemlere ayrılacaktır.

$$a_1x_1+\ldots+a_nx_n=b \qquad (1)$$

Gizli veri, (k,n) eşik şemasına göre herhangi k ($k \leq n$) yada daha fazla hiperdüzlemlerin kesişme noktasını bularak, elde edilebilir. Şekil 2, sistemin genel yapısını göstermektedir.



Şekil 2: Sistemin genel şeması

Paylaşım algoritması aşağıdaki adımları içermektedir:
Adım 1: (k, n) eşik şeması seçilir.
Adım 2: Gizli veri, k karakterli örtüşmeyen kümeler haline bölünür.
Adım 3: Her bir k karakter için
3.1. k karakter değerleri (ASCII değeri) alınır
3.2. Rastgele n farklı çözüm seti $(a_1,a_2,\ldots,a_k)$ seçilir ve n pay değerlerini üretmek için denklem 1'e koyulur.
Adım 4: Her bir pay DataMatrix içerisine gömülür.

2.2. Yeniden Yapılandırma Algoritması

Yeniden yapılandırma algoritması (k, n) eşik şemasına göre k veya daha fazla DataMatrix barkodlarından gizli veriyi yeniden hesaplamaktadır. Herhangi bir DataMatrix barkodlardan gizli veri kesinlikle elde edilemez, bu barkodlarda yalnız anlaşılamayan pay bilgileri bulunmaktadır. Yeniden yapılandırma algoritması aşağıda verilmiştir.
Adım 1: (k,n) aynı eşik şeması kullanılır ve k veya daha fazla DataMatrix barkod seçilir.
Adım 2: k adet DataMatrix barkodlarının bilgileri yeniden elde edilir.
Adım 3: Elde edilen bilgiler denklem 1'e koyulur ve x dizisi hesaplanır. Sonuçta gizli veri tekrar elde edilir.

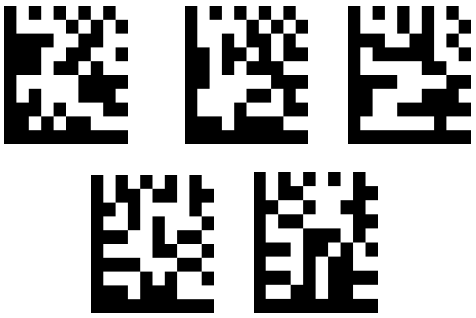
Örnek olarak "SECRETEST" kelimesini ele alalım. Önce kelime Blakley gizli paylaşım şemasıyla k paya bölünür, sonra ise DataMatrix kodlarına gömülür. (3,5) eşik gizli paylaşımı kullanılarak "SEC" karakterleri "-=h" karakterlerine denk gelecek. Bu karakterlere karşı düşen ASCII değerler sırasıyla (45, 61, 104)'dür. Bu değerler aşağıdaki bağıntıya göre kelime koduna çevrilir:

Kelime_kodu=(karakterlerin sayısal miktarı) +1

Reed-Solomon hata düzeltme tekniği kullanılır ve 5 tane hata düzeltme kelime kodu oluşturulur ve sonra her bir sayı ikili hale çevrilir. İkili sayılar DataMatrix barkodlarını oluşturmaktadır. Sonuçta parçalanmış bilgiler birleştirilerek başlangıç veriler güvenli şekilde tekrar elde edilir.

3. Deneysel Sonuçlar

Son zamanlarda ürün hakkındaki bilgiler ve özellikler, DataMatrix barkodlarına taşınmaktadır. Ancak doğrudan Datamatrix kod içeriğinin okunması mümkündür. Önerilen şema DataMatrix kodlarının gizli verilerinin güvenliğini artırmaktadır. Gizli veri Blakley gizli paylaşım teknikleri ile paylara bölünür ve sonra DataMatrix kodlarının içerisine gömülür. Katılımcılar ayrılıkta kendi payından gizli veriyi elde edememektedir. Pay sayısı önceden tanımlanmış bir eşik değerine eşit veya daha büyük olduğu halde gizli veriler tekrar elde edilmektedir. Bu şemada veriler doğrudan DataMatrix içerisine gömülmektedir ve bu nedenle DataMatrix barkodların verilerini aramak için ayrıca bir veritabanı olmasına gerek olmamaktadır. Önerilen çalışmada pay boyutu, gizli verinin sadece dörtte biridir, böylece sistem maliyeti çok daha düşüktür ve Datamatrix içerisine daha çok gizli veri kodlanabilir. DataMatrix barkod kısmen hasarlı olsa bile okunabilir.
Şekil 3'te (3,5) eşik gizli paylaş şeması örneği verilmiştir. İlk olarak, gizli veri Blakley gizli paylaşım tekniği ile paylara bölünür. Sonra üretilen paylar her DataMatrix kodları içerisine kodlanır. (3,5) eşik gizli paylaşım şemasında alınan Datamatrix kodlarının sayısı üçe eşit veya daha büyük olması durumunda, gizli veri elde edilmektedir. Yeniden yapılandırma aşamasında, herhangi üç pay ve ya üçten büyük pay alınırsa gizli veri tekrar elde edilebilir.



Şekil 3: "SECRETEST" kelimesini içeren DataMatrix barkod görüntüleri

4. Değerlendirme

Bu çalışma, DataMatrix kodlarındaki verinin güvenliğini artırmak için bir yöntem sunmaktadır. Önerilen teknik, ilk gizli veriyi Blakley gizli paylaşım yöntemi ile paylara ayırır ve paylaşılan veriler daha sonra doğrudan DataMatrix etiketleri içerisine gömülür. Böylece herkes doğrudan DataMatrix içeriğini okuyamamaktadır. Veri kaybını önlemek için barkod %60 bulanık olsa bile, Reed-Solomon algoritmasına dayalı hata düzeltme kod kelimeleri ile çözülmektedir. Önerilen teknik, tıbbi e-sağlık sistemi, askeri belgeler, ticari işlemler, elektronik bilet, posta hizmetleri ve diğerleri gibi bazı uygulamalarda kullanılabilir.

5. Kaynakça

[1] ISO/IEC16022, "Information technology-Automatic identification and data capture techniques-Data Matrix barcode symbology specification"
[2] NATO Standard Barcode Handbook, AAP-44(A), September 2010.
[3] National Aeronautics and Space Administration," Application of Datamatrix identification symbols to Aerospace parts using direct part marking methods/techniques", NASA-HDBK-6003C,2008.
[4] M.Krasikov, "DataMatrix barcode search algorithm on post envelope and decoding program development", Information Technology, Management and Society, Volume 2, No.1, 13-22, ,2009.
[5] Tso, H.-K., "Sharing secret images using Blakley's concept", Optical Engineering, vol. 47, no. 7, 2008.
[6] C.C. Thien and J.C. Lin, "Secret image sharing," Comput. Graph. 26, 765–770, 2002.
[7] Jun-Chou Chuang, Yu-Chen Hu & Hsien-Ju Ko," A Novel Secret Sharing Technique Using QR Code", International Journal of Image

Processing (IJIP), Volume (4) : Issue (5), pp.468-475, 2010.
[8] Blakley,G.R., "Safeguarding Cryptographic Keys", Proceedings of the National Computer Conference, pp. 313-317, 1979.
[9] A. Shamir, "How to share a secret," Communications of the ACM, Vol. 22, pp. 612-613, 1979.
[10] M.Naor and A.Shamir,"Visual cryptography," in Proceedings of Advances in Cryptology-EURPOCRYPT, LNCS 950, pp. 112, , 1995.
[11] Chen, C.-C., Fu, W.-Y, "A Geometry Based Secret Image Sharing Approach", Journal of Information Science and Engineering, Vol 24, No.5, pp. 1567-1577, 2008.
[12] Esam Elsheh1 and A. Ben Hamza2," SECRET SHARING OF 3D MODELS USING BLAKELY SCHEME", 25th Biennial Symposium on Communications, IEEE, pp.92-95, 2010.
[13] Jie Gao," Reed Solomon Code", February 19, 2007.
[14] C.K.P. Clarke,"Reed Solomom Error Correction", BBC R&D white Paper, WHP 031, july 2002.
[15] Jasmin Oz and Assaf Naor," Reed Solomon Encoder/Decoder on the StarCore™ SC140/SC1400 Cores, With Extended Examples", Freescale Semiconductor Inc., Document Order No. AN2407, Rev.1 ,12/2004.
[16] GSI DataMatrix, www.gs1.org,2010

DÜZENLEYEN KURULUŞLAR

ELEKTRİK MÜHENDİSLERİ ODASI TMMOB 1954 ANKARA ŞUBESİ

1996 ATILIM ÜNİVERSİTESİ

ODTÜ

DESTEKLEYEN KURULUŞ

TÜBİTAK

İLETİŞİM SPONSORLARI

87.7 radyohacettepe

radyo odtü 103.1

YAKA KARTI SPONSORU

symturk