Ağ cihazlarına güvenli erişim için bir iletişim sistemi tasarlanması

Designing a communication system for secure access to network devices

Şenol Şen[1], Tarık Yerlikaya[2]

[1]Bilgi İşlem Daire Başkanlığı
Trakya Üniversitesi
senolsen@trakya.edu.tr

[2]Bilgisayar Mühendisliği Bölümü
Trakya Üniversitesi
tarikyer@trakya.edu.tr

Özet

Ağ cihazları genellikle seriport (COM-RS232) üzerinden veya ağ üzerinden telnet protokolü veya ssh protokolü ile programlanırlar. Telnet protokolü ve COM portu üzerinden yapılan haberleşme işlemi şifresiz olarak yapılmaktadır. Dolayısıyla araya giren bir saldırganın iletişimi dinleme ve değiştirebilme ihtimali vardır. Bunu önlemek amacı ile aşağıda anlatılan donanım sistemi tasarlanmıştır. Geliştirilen bu sistem ile PC ile konfigürasyonu yapılmak istenen network cihazları arasına, RSA şifrelemesini kullanan birer donanım eklenerek aradaki seri iletişim şifreli hale getirilmiştir.

Abstract

Network devices are generally serial ports (COM-RS232) are programmed over the network or via the telnet protocol or ssh protocol. The communication process via the Telnet protocol and COM port is done unencrypted. Therefore, an attacker intervening possibility of listening and communication has changed. In order to prevent this, the system is designed in hardware described below. Made by developed this system with PC configuration required between network devices, the addition of a hardware encryption using RSA encrypted communication has been made in between series.

1. Giriş

Bilişim teknolojilerinin kullanımının hızla yaygınlaştığı ve arttığı günümüzde; bilgi, bilgisayar ve bilişim sistemleri güvenliği, en önemli ve kritik konuların başında yer almaktadır. Bilgi güvenliğinin insanlığın var olduğu zamandan beri uygulana gelen ilk örneği şifrelemedir. Şifrelemenin, tarihin ilk dönemlerinden beri kullanılıyor olması, şifrelenen bilginin öneminin farkında olunduğunun bir göstergesidir. Şifreleme sadece eski zamanlarda kullanılan bir yöntem değildir. Günümüzde de bilgi güvenliği açısından önemini artan bir şekilde korumaktadır.

Ağ cihazları genellikle seriport (COM-RS232) üzerinden programlanırken yapılan haberleşme işlemi şifresiz olarak yapılmaktadır. Aradaki iletişimi güvenli hale getirebilmek için yapılması gereken iletişimin güçlü bir şifreleme algortiması ile şifrelenmesi işlemidir. Aradaki iletişim şifrelendiğinde araya giren bir saldırganın iletişimi dinlese bile elde ettiği bilgiler şifreli olacağından bir işine yaramayacaktır. Bu amaçla aşağıdaki donanım sistemi tasarlanarak seriport üzerinden yapılan iletişim RSA şifreleme algortiması kullanılarak şifrelenmiştir.

2. Bilgi ve Bilişim Güvenliği Nedir?

Bilgisayar ağları ve sistemleri üzerinde, sürekli erişilebilen bilginin göndericisinden alıcısına kadar gizlilik içerisinde, başkaları tarafından izinsiz veya yetkisiz bir biçimde erişilmeden, kullanılmadan, değiştirilmeden, ifşa edilmeden, ortadan kaldırılmadan, el değiştirmeden ve hasar verilmeden güvenli bir şekilde iletilmesi anlamına gelmektedir [1].

Bilişim sistemlerine olan bireysel ve toplumsal bağımlılığımız arttıkça bu sistemlerde meydana gelebilecek arıza ve saldırılara karşı duyarlılığımız da o denli artacaktır. Bu duyarlılık arttıkça da bilgisayar sistemlerine ve ağlarına yönelik olarak gerçekleştirilecek olan saldırıların sonucunda; para, zaman, prestij ve değerli bilgi kaybı da artacaktır. Bu saldırıların hastane bilişim sistemleri gibi doğrudan yaşamı etkileyen sistemlere yönelmesi durumunda ise kaybedilen insan hayatı bile olabilecektir.

3. Ağ Cihazları nelerdir? Nasıl Programlanır?

Birden fazla bilgisayarın bilgi paylaşımı, yazılım ve donanım paylaşımı, merkezi yönetim ve destek kolaylığı gibi çok çeşitli sebeplerden dolayı birbirine bağlandığı yapıya ağ (network) denir. Ağ yapılarını oluşturmak için çok çeşitli ağ cihazları kullanılabilir. Ağ yapılarında kullanılan başlıca cihazlar:

- Göbek (Hub)
- Anahtar (Switch)
- Tekrarlayıcı (Repeater)
- Köprüleyici (Bridge)
- Yönlendirici (Router)
- Güvenlik Duvarı Cihazları (Firewall)
- Erişim Noktası (Access point)
- NIC (Ağ Ara Birim Kartı)
- Modem

Ağ cihazları genellikle seri port(RS232) üzerinden veya ağ üzerinden telnet protokolü veya ssh protokolü ile programlanırlar. Seri port üzerinden yapılan haberleşme işlemi şifresiz olarak gerçekleşmektedir.

4. Seri Port – RS232

Seri portlar isimlerini verilerin porttan seri bir biçimde yani bir seferde tek bit olarak gönderilmesi gerçeğinden almaktadır. Bunun sebebi portun her yön için tek bir veri hattına sahip olmasıdır. Seri portlara COM portlar da denilmektedir. Çünkü harici aygıtlarla PC arasında bir iletişim aracı oluşturmaktadır. Seri portlara bağlanan en yaygın aygıtlar modemler, fareler, yazıcı ve çizici gibi seri yazdırma aygıtlarıdır. Seri portların konnektörleri 2 şekilde olur. 25 ve 9 pin olmak üzere. 25 pinlik bir aygıtı 9 pinlik bir porta ya da 9 pinlik bir aygıtı 25 pinlik bir aygıta bağlamak gerektiğinde, bu gibi durumlarda kullanılabilecek adaptörler vardır [2].

Seri bağlantı noktaları iki seviyeli (ikili) sinyalleme kullanırlar, böylece saniyede bit cinsinden veri hızı bauddaki sembol hızına eşit olur. Asenkron iletişim başlama / durması için kullanılan ortak, saniyede bit hızları 300, 1200, 2400, 9600, 19200 baud, vs.dir. Bağlantı noktasının ve cihazın hızlarının birbirine uygun olması gerekir. Sıkça desteklenen veri hızları; 75, 110, 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600 ve 115200 bit/s'dir.

5. Şifreleme (Kriptoloji)

Bilginin güvenli iletimi yani iletim esnasında bilginin gizliliğinin ve bütünlüğünün korunması önemli bir gereksinim haline gelmistir. Özellikle, e-ticaret ve e-devlet projeleri, internet üzerinden askeri, özel ve resmi yazısmalar, ulusal güvenlik, internet bankacılığı v.b. gibi alanlarda bilginin güvenliğini sağlamak amacıyla çeşitli algoritmalar ve bunları kullanan donanım ve yazılımlar gelistirilmistir. Günlük hayatta karsılastığımız uygulamalardan da anlasılacağı gibi bilgi güvenliği denilince akla gelen sifreleme ve sifre çözme algoritmalarıdır. Şifreleme (encryption), bir verinin uygun bir bilgi olmadan okunabilmesini neredeyse imkansız kılacak bir forma dönüştürülmesidir. Bunun amacı, gizli bilgiyi saklayarak eline geçmesi istenmeyen kişilerden şifrelenmiş veriye ulaşmaya çalışsalar dahi bilginin gizliliğini garanti altına almaktır. Deşifre etme (decryption) ise şifreleme olayının tersidir; şifrelenmiş verinin bilgi alınabilir bir forma yeniden dönüştürülmesidir [3].

Şifreleme ve deşifreleme işlemi genellikle anahtar (key) olarak bilinen gizli bir bilginin kullanımına ihtiyaç duyar. Bazı mekanizmalarda aynı anahtar hem şifreleme hem de deşifreleme işlemi için kullanılır; diğer mekanizmalarda ise her iki işlem içinde farklı anahtarlar kullanılır.

6. RSA Algoritması

1977 yılında Ron Rivest, Adi Shamir ve Leonard Adleman tarafından oluşturulan RSA algoritması geliştiricilerinin soy isimlerinin ilk harfleriyle anılmaktadır. Bir genel anahtarlı şifreleme tekniği olan RSA, çok büyük tamsayıları oluşturma ve bu sayıları işleminin zorluğu üzerine düşünülmüştür. Anahtar oluşturma işlemi için asal sayılar kullanılarak daha güvenli bir yapı oluşturulmuştur. İki asal sayının çarpımını kullanarak anahtar oluşturulmasının sebebi, iki asal sayının çarpımını asal çarpanlarına ayırmak asal olmayan sayıları ayırmaktan daha zorlu olmasındandır [4].

RSA kriptosisteminde, anahtar üretimi mesajı almak isteyen taraf tarafından yapılır. Genel ve özel anahtarları üreterek, genel anahtarı kamuya açık olarak herkesin kullanımına sunar. Bu kişiye mesaj göndermek isteyen bir kişi bu genel anahtarı kullanarak elindeki mesajı şifreler ve karşı tarafa gönderir. Şifrelenmiş mesajı alan taraf kendi üretmiş olduğu özel anahtarı kullanarak şifreli mesajın şifresini çözer ve orijinal mesajı elde eder. Anahtar üretimi, şifreleme ve şifre açma adımlarını aşağıda inceleyelim.

Anahtar oluşturma algoritması şu şekildedir:

- p ve q gibi çok büyük iki asal sayı seçilir.
- Bu iki asal sayının çarpımı n = p.q ve bu bir eksiklerinin φ(n) = (p-1).(q-1) hesaplanır.
- 1'den büyük φ(n)'den küçük φ(n) ile aralarında asal bir e tamsayısı seçilir.
- Seçilen e tamsayısının mod φ(n)'de tersi alınır, sonuç d gibi bir tamsayıdır.
- e ve n tamsayıları genel anahtarı, d ve n tamsayıları ise özel anahtarı oluşturur [4].

Genel ve özel anahtarları oluşturduktan sonra gönderilmek istenen bilgi genel anahtar ile şifrelenir. Şifreleme işlemi şu şekilde yapılmaktadır:

- Bilgiyi gönderecek taraf, bilgiyi alacak tarafın genel anahtarı olan e,n 'yi elde eder.
- Açık metin M elemanı [0, n - 1] olacak şekilde bir tam sayıya dönüştürülür.
- Şifreli metni C ≡ M^e mod n olarak hesaplanır.
- Bilgiyi gönderecek taraf şifreli metin C'yi bilgiyi alacak tarafa gönderir [4].

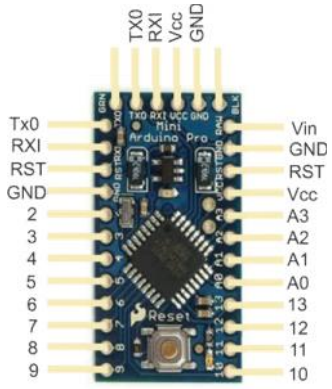
Şifre açma işlemi:
Bilgiyi alan taraf özel anahtarını kullanarak açık metni
M ≡ C^d mod n olarak tekrar elde eder [4].

7. Geliştirilen Sistem

Seriport (COM-RS232) ile yapılan iletişim RSA şifreleme algortiması kullanılarak şifreli hale getirilirken aşağıda tasarlanan sistem geliştirilmiştir.

Donanım sistemi olarak Arduino Pro Mini Atmega 328, LCD ekran ve kutusu kullanıldı. 0–255 arası tüm Ascii [5] karakterler RSA şifrelemesi ile şifrelenerek LUT (look up table) tablosu oluşturuldu. Kullanılan donanımın işlem kapasitesi 8 bitlik olmasına rağmen 16 bit şifreleme yapıldı.

Arduino [6] yazılımı ile seri port iletişimi şifreli hale getirilerek, aradaki iletişimin güvenli hale getirildi.



Şekil 1: Arduino Pro Mini

Şekil 2: Geliştirilen Donanım Sistemi

Şekil 3'te oluşturulan tablodaki 65 decimal değerinin RSA ile şifrelenmiş hali olan 3316'nın elde edilmesi aşağıda gösterilmiştir. Aynı yöntemle 0'dan 255'şe kadar olan bütün decimal değerler şifrelenmiş ve Şekil 3'teki tablo oluşturulmuştur. Oluşturulan bu tablodaki değerler Donanımımızdaki Arduino Pro Mini'ye aktarılarak sistemimiz tasarlandı.

Anahtar üretim işlemi,

- p = 211 ve q = 233 olan iki asal sayı seçildi.
- n = p.q = 211x233= 49163 değerini hesaplandı.
- φ(n) = (p - 1).(q - 1) = 210x232 = 48720
- φ(n) ile aralarında asal 1< e < φ(n) şartlarını sağlayan rastgele bir e =2^16+1 sayısı seçildi.
- 1< d < φ(n) ve e.d ≡ 1 mod φ(n) denkliğini sağlayan d = 44273 olarak bulundu.
- Bilgiyi alacak tarafın açık anahtarı e = 2^16+1, n = 49163 gizli anahtarı ise d = 44273, n = 49163 oldu.

Şifreleme işlemi,

- Bilgiyi alacak taraf açık anahtarı olan e = 2^16+1, n = 49163 sayı çiftini bilgiyi gönderecek tarafa herkesin bilgisine açık olan bir kanaldan gönderir.
- Bilgiyi gönderecek tarafın açık metni M = 65 idi.
- Bilgiyi gönderecek taraf C ≡ 65^(2^16+1) mod 49163 Denkliğini sağlayan şifreli metin olan C = 3316 sayısını hesaplar.
- Bilgiyi gönderen taraf C = 3316 sayısını bilgiyi alacak tarafa herkesin bilgisine açık bir kanaldan gönderir.

Şifre açma işlemi,
Bilgiyi alan taraf M ≡ 3316^44273 mod 49163 denkliğini sağlayan M sayısını hesaplayarak açık metni 65 olarak elde edilir.

decimal	şifreli	decimal	şifreli	decimal	şifreli	decimal	şifreli	decimal	şifreli	decimal	şifreli
0	0	43	7141	87	36203	130	29190	177	27667	220	26089
1	1	44	47242	88	39399	131	39242	178	34932	221	48219
2	45406	45	12529	89	28282	132	46395	179	24788	222	2716
3	14282	46	4897	90	26701	133	27617	180	26026	223	31479
4	5268	47	32750	91	13495	134	35258	181	33490	224	37878
5	31030	48	34324	92	38096	135	35021	182	35501	225	43029
6	28522	49	36712	93	29716	136	22970	183	3780	226	30792
7	1595	50	4608	94	13239	137	8641	184	35984	227	48368
8	20813	51	1313	95	18830	138	29168	185	47226	228	12541
9	47400	52	15906	96	48444	139	37555	186	6161	229	38070
10	34926	53	44340	97	18504	140	32728	187	40771	230	40240
11	32467	54	9463	98	24394	141	47881	188	14033	231	34513
12	18186	55	2814	99	35574	142	7708	189	42463	232	27027
13	10026	56	11710	100	42283	143	5919	190	1247	233	8388
14	5471	57	36520	101	7428	144	11095	191	28154	234	21204
15	15178	58	11120	102	32522	145	13026	192	46481	235	33290
16	23892	59	42628	103	12284	146	32765	193	15524	236	36883
17	43769	60	18666	104	23366	147	46552	194	46117	237	16918
18	35749	61	43332	105	20714	148	41977	195	15143	238	36389
19	23782	62	35198	106	28027	149	29790	196	40737	239	12678
20	48228	63	39469	107	30861	150	31362	197	37151	240	6488
21	17321	64	5776	108	41521	151	35139	198	22679	241	6600
22	44047	65	3316	109	33521	152	1682	199	38362	242	20605
23	18672	66	38669	110	47010	153	21163	200	37585	243	23742
24	11768	67	26463	111	34310	154	1038	201	28585	244	9167
25	3545	68	622	112	6415	155	47792	202	17588	245	17487
26	40339	69	13392	113	7045	156	36432	203	29616	246	18414
27	41453	70	5291	114	8293	157	4252	204	34064	247	46945
28	44750	71	9472	115	6205	158	46179	205	37732	248	29391
29	19992	72	31442	116	10710	159	44440	206	13069	249	19232
30	5334	73	37508	117	22842	160	8393	207	20474	250	20236
31	4780	74	46430	118	19658	161	38225	208	19056	251	24332
32	9394	75	40963	119	95	162	1479	209	25279	252	12365
33	37441	76	16252	120	27439	163	11252	210	2531	253	44034
34	10102	77	16226	121	2206	164	588	211	13504	254	25709
35	34872	78	29564	122	29532	165	23377	212	9707	255	35426
36	4323	79	39271	123	22424	170	1772	213	31691		
37	22639	80	39883	124	9584	171	8373	214	30740		
38	29360	82	25674	125	23719	172	9093	215	7589		
39	28676	83	559	126	39738	173	42380	216	48965		
40	22222	84	500	127	24398	174	19350	217	3835		
41	40428	85	24195	128	29614	175	530	218	17209		
42	16815	86	14261	129	23700	176	7750	219	9208		

Şekil 3: Ascii karakterlerin RSA ile şifrelenmiş halleri (oluşturulan LUT tablosu)

8. Sonuçlar

Günümüzde kişiler, kurumlar ve kuruluşlar arasında birden çok bilgisayarla yapılan haberleşme, elektronik ağ ortamında yapılmaktadır. Bu büyük elektronik ağ ortamında meydana gelebilecek herhangi bir sorunun tüm ağı olumsuz yönde etkileyebileceği göz önüne alınırsa, veri güvenliğinin günümüzde daha da önem kazandığı görülecektir [7].

Ağ ortamında verinin bir noktadan diğerine aktarımı farklı teknolojiler kullanılarak gerçekleştirilmektedir. Haberleşme sırasında kullanılan ağ cihazları da bilgisayarlar gibi tehdit altındadırlar. Bu cihazlar, tüm ağı dinleyen yazılımlar tarafından da rahatlıkla dinlenebilmektedirler.

Herhangi bir kurum veya kişiye bilgisayar ağları üzerinden veri gönderimi yapılırken, veri bir veya daha fazla bilgisayar üzerinden hedef bilgisayara iletilir. Gönderilen veri veya verilerin birçok bilgisayar ve ağ donanımı üzerinden karşı tarafa iletilmesi esnasında, verinin gizliliği ve bütünlüğünün korunabilmesi gerekmektedir [7].

Bilgisayarlarda olduğu gibi, kullanılan ağ cihazlarının da kontrolünün yapılması ve belirli politikalar doğrultusunda yönetilmesi günümüzde önem arz etmektedir. Bilgisayar ağlarının güvenliği kurumsal bilgi güvenliği yaklaşımları ile sağlanmalı ve güvenliği sağlamak için önleyici yazılımlar ve donanımlar kullanılmalıdır.

9. Kaynaklar

[1] Pro-G Bilişim Güvenliği ve Araştırma Ltd., http://www.pro-g.com.tr, Whitepapers/bilişim-guvenligi-v1.pdf.

[2] Seri port iletişimi, http://tr.wikipedia.org/wiki/Seri_port..

[3] Stinson D. R., Cryptography: Theory and Practice, Second Edition, *CRC Press*, 2002.

[4] Schneier B., Applied Cryptography, Second Edition, *John Wiley & Sons, Inc*., New York, Ny, 1996.

[5] Ascii tablosu, http://www.asciitable.com/.

[6] Arduino software, http://www.arduino.cc/en/Main/Software.

[7] Canberk, G. ve Sağıroğlu, Ş., Bilgi ve Bilgisayar Güvenliği Casus Yazılımlar ve Korunma Yöntemleri, *Grafiker Ltd. Şti*., Ankara, 2006.