# Parola Güvenliği

Elk. Elo. Müh. Melike Demirel
melike.demirel@emo.org.tr

Bilgisayar sistemlerinde parola [1], alışılagelmiş ifadesiyle şifre, sisteme bağlanan kullanıcının kimliğinin doğrulanması amacıyla kullanılır. Parola sahibinin parolasını gizli tutup başka kimseye açıklamaması yeterli olmayıp aynı zamanda ilk seçim anında parolanın, sahibi dışındaki kişiler tarafından kolayca tahmin edilemeyecek şekilde seçilmesi uygundur.

Parola seçiminde, kullanıcıların genelde hatırlanması kolay ve kısa parolalar seçtikleri bilinmektedir, ancak bu tür parolalar bilgisayar korsanları için kolay hedef olup tek bir "zayıf" kullanıcı parolası bile tüm sistemin güvenliğini tehlikeye düşürebilir [2].

Ege Üniversitesi Uluslararası Bilgisayar Enstitüsü Öğretim Üyesi Prof. Dr. Mehmet Emin Dalkılıç ve İzmir Ekonomi Üniversitesi Bilgisayar Mühendisliği Bölümü Öğretim Görevlisi İlker Korkmaz, birlikte hazırladıkları ''Türk Kullanıcıların Parola Seçimindeki Eğilimleri'' isimli araştırmalarında, güvenilir kaynak-lardan elde edilen ve aktif bir sistemde kullanılan 2564 gerçek Türkçe parolayı çeşitli yöntemlerle kırmaya çalıştılar.

Çalışmanın ilk bir aylık sürecinde tüm parolaların %30'una karşılık gelen 777'si tahmin edilebilmiştir. Sözlük atağı yöntemi ile şifrelenmiş hallerinden asıl açık metinleri elde edilmeye çalışılan parolaların % 5'i ilk beş dakika içinde, % 10'a yakını da ilk gün içinde kırılabilmiştir. Kırılan 777 parolanın 564'ü sadece sayısal karakter içermektedir. Sadece rakamları kullanarak parola seçen kullanıcı sayısı da yüksek orandadır. Kırılan parolaların büyük oranının sadece rakamlardan oluştuğu gözlemine dayanarak, bu tür parolaların zayıf nitelikte olduğu belirtilmiştir.

Kırılan parolalar arasındaki diğer bazı dikkat çekici özellikler de çalışmada belirtilmiştir. Sadece 32 parola, en az bir Türkçe alfabeye ait karakter içermekte ki bu da 2 bin 564 Türk kullanıcısı içinde % 98'den daha fazlasının, parola seçiminde Türkçe karakter tercih etmediğini göster-mektedir. Deneylerde, tümü sayılar-dan oluşan parolaların büyük oranı ve en fazla 3 karakter uzunluğundaki şifrelerin tamamı kırılmıştır. Türk kullanıcılarına ait eldeki parolaların % 73'ünün en az 1 rakam karakteri, % 39'unun en az 1 büyük harf içerdiği belirtilmiştir.

Ayrıca, uzunlukları açısından, 4 karakterli parolaların %96'sı, 5 karakterlilerin %42'si, 6 karakterlilerin % 31'i, 7 karakterlilerin % 4'ü, 8 karakterlilerin ise sadece % 2'sinin kırılabildiği açıklanmış ve ***kullanıcıların en az 8 karakterli parolaları tercih etmeleri önerilmiştir.***

Türk kullanıcı parolaları üzerine bulgulara ulaşılan çalışma sonuçları, Türk kullanıcıların eğilimleri olarak ortaya çıkmış olsa da yazarlar diğer ülke kullanıcıları için de bu eğilimlerin genel olarak benzediğini düşünmektedir.

Dünya çapındaki bazı araştırmacılar [3] ***parola seçiminde öncelikle akılda kolay kalabilecek ve aynı anda da karışık karakterleri içerebilecek olan parolaların tercih edilmesini öneriyor***. Bir yöntem olarak, kullanıcının kendine has anlamlı bir cümledeki kelimelerin ilk harflerini bir araya getirmesi ile "anımsatıcı" parola oluşturulabilir. Buna örnek olarak, "Oğlum Deniz 2 yaşında, onu çok seviyorum" cümlesi gösterilebilir. Bu cümlenin baş harfleriyle oluşturulan "OD2y,oçs" parolasındaki gibi; internet kullanıcılarına, kolay hatırlanabilen ve aynı anda da zor

kırılabilecek kendilerine ait cümlelerin baş harfleriyle şifreleme yapmaları öneriliyor.

Araştırma [2] sonucunda belirlenen **'zayıf' parola nitelikleri** şöyle sıralanıyor:

- Parola uzunluğunun 7 karakterden az olması,
- Parolada kullanılan karakterlerin tümünün rakam olması,
- Parolada kullanılan karakterlerin tümünün alfabetik olması,
- İçeriğinde farklı tipte karakterler kullanılsa da, parolaların, rakamlarla sonlandırılması,
- Parolanın, uzunluğu en az 8 karakter olsa da, kullanıcı bilgisi, sözlüklerde yer alan bir kelime, özel isim veya klavye deseni gibi farklı kullanıcılar tarafından da seçilebilecek ya da tahmin edilebilecek bir aday olması.

**'Güçlü' parola nitelikleri** ise şöyle sıralanıyor:

- Parolanın, yukarıda sunulan zayıf parola niteliklerini taşımaması,
- İçerdiği karakterlerde en az 1 adet rakam ve en az 1 büyük harf olacak şekilde, parolanın hem nümerik hem de alfabetik karakterlerin birlikte kullanılması ile oluşturulması,
- Parolanın, en az 1 adet, harf veya rakam olmayan özel bir karakter içermesi (noktalama işareti gibi),
- İngilizce alfabede yer almayıp kullanıcıların kendi alfabelerinde yer alan harfler varsa, parolanın bu tipte en az bir harf içermesi (Türk kullanıcılar için, "ç,ğ,ı,ö,ş,ü" karakterleri gibi).

İnternet kullanıcılarına, parola giriş ekranlarında, parola seçim eğilimlerini güçlü nitelikleri taşıyacak parolaları seçme yönünde geliştirebilecek bilgilerin sunulması yararlı olacaktır. Bu bilgilerin, yukarıda sıralanmış olan nitelikleri temel almasının yanı sıra bunlara ilişkin bazı zayıf ve güçlü parola adayı örneklerini de içermesi önerilebilir. Böylece, bu nitelikler doğrultusunda, kullanıcıların güçlü parola seçme eğilimleri arttırılabilir.

KAYNAKÇA:

*[1]http://tr.wikipedia.org/wiki/Parola*

*[2] Korkmaz İ., Dalkılıç M.E., "Türk Kullanıcıların Parola Seçimindeki Eğilimleri", 3. Ağ ve Bilgi Güvenliği Sempozyumu, Ankara, 2010.*

*[3] Yan, J., Blackwell A., Anderson R., Grant A., "The Memorability and Security of Passwords—Some Emprical Results", Technical Report No. 500, Computer Laboratory, University of Cambridge, 2000.*