Parola Güvenliği

Melih KIRLIDOĞ
Nişantaşı Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, İstanbul / Alternatif Bilişim Derneği
melihk76@gmail.com

Özet
Bilgisayar ortamında bilgi güvenliğinin en önemli unsurlarından biri parola güvenliğidir. Parola kullanımı bilgisayar sistemlerinde genellikle birinci basamak kimlik doğrulama aracı olarak kullanılır. Hassas uygulamalarda ikinci basamak olarak akıllı kart ve parmak izi gibi biyometrik kimlik doğrulama işlemleri de kullanılmasına rağmen bunlar parola yerine geçen değil, onu tamamlayan araçlardır. Bu yazıda güvenli parola kullanma pratikleri ve dikkat edilmesi gereken özellikler tartışılacaktır. Bu kapsamda uzun parolalar seçilmesi ve sadece küçük veya büyük harf değil bunlarla beraber rakam ve özel karakterlerin de kullanılma gereği sebepleriyle birlikte irdelenecektir.

Anahtar Sözcükler: Bilgi Güvenliği, Bilgisayar Güvenliği, Parola Güvenliği.

Abstract
One of the most important aspects of information security in the computer environment is password security. Password is usually used as a first step authentication tool in computer systems. Although tools such as smart cards and fingerprint may be also used as second step authentication in sensitive applications, they complement rather than replace password authentication. This article will discuss secure implementation practices of passwords and points to consider thereby. In this context, the necessity for choosing long passwords and using numbers and special characters along with uppercase and lowercase letters will be investigated.

1. Giriş

Parola kelimesi birçok anlam içermesine rağmen bu yazıda bilgisayar ortamındaki "password" karşılığı olarak kullanılacaktır.

Parola bilgisayar güvenliği için en yaygın olarak kullanılan kimlik doğrulama (authentication) aracıdır. Hassas uygulamalarda kimlik doğrulama amacıyla parolaya ek olarak biyometrik veriler (göz-iris tarama, parmak izi, vb.) veya parola içeren fiziksel araçlar da (akıllı kart vb.) kullanılır. Ancak bu kimlik doğrulama araçlarının kullanımı yaygın olmayıp parola hassas olanlar da dahil olmak üzere bilgisayar sistemlerinin tamamında kullanılır.

Parola ilgisiz kişiler tarafından ele geçirildikten sonra bilgisayar ortamında bilgi güvenliği için alınan diğer tedbirlerin çoğu anlamsızlaşır. Bu nitelikleriyle parolalar "birinci adım bilgi güvenliği araçları" olarak tanımlanırlar. Bu yazıda asıl olarak işletim sistemlerine giriş parolaları irdelenecektir. Bu parolaların disk üzerinde saklanma yöntemleriyle birlikte neden uzun ve karmaşık olma gereklilikleri örneklerle birlikte araştırılacaktır.

2. İşletim Sistemi Parolalarının Disk Üzerinde Saklanması

Parolalar bilgisayar ortamında gerçek halleriyle saklanmazlar; belli algoritmalar aracılığıyla değiştirilerek özütleri (hash) saklanır. Teorik olarak parolanın aslından özüte gitmek kolay, bunun tersi ise imkansıza yakın derecede zordur. (Bilgisayar ortamında özütten parolaya gitmeyi algoritmik yönden imkansızlaştırmak amacıyla parola özütleri de "tuzlama-salting" denilen bir işlemden geçirilerek diske yazılır, ancak basitlik amacıyla bu yazıda bu konuya girilmeyecektir.) MD5, SHA1, SHA256, SHA512, LM, NTLM gibi birçok özüt vardır.

Bir dosyanın veya disk bölümünün (partition/volume) özütü alınabildiği gibi bir metin parçasının da özütü alınabilir. Özüt boyutları asıl kaynaktan bağımsız olarak sabittir. Asıl kaynaktaki en küçük bir değişiklik özütün tamamen değişmesine neden olur. Tablo 1'de bazı metin parçalarının özütleri gösterilmektedir:

Özüt haline getirilmiş parolalar işletim sistemleri tarafından belli dizinlerde saklanır. Örneğin, Windows 7 işletim sistemi özütü c:\windows\system32\config\sam isimli dosyada saklar. Bu dosya normal hallerde kullanıcının kendisi tarafından görülemez. Görmek için çeşitli yöntemler kullanılabilir. Bunlardan biri bilgisayarı TAILS gibi bir Linux sürümü tarafından çalıştırıp Windows'un bulunduğu dizine erişmektir.

3. Parola kırma saldırıları

Parola kırma saldırıları genellikle parolanın kendisi değil, özütü üzerinden yapılır. Saldırgan parolanın kendisiyle (yukardaki tabloda birinci kolon) özüt (üçüncü kolon) arasındaki tek yönlü ilişkiyi kullanır.

Bilgisayar parolalarını kırmanın başlıca iki yolu vardır: Kaba kuvvet (brute force) ve sözlük (dictionary) saldırıları. Kaba kuvvet saldırısında -genellikle- bir karakter uzunluğundaki paroladan başlanarak mümkün olan her kombinasyon denenir. Sözlük saldırılarında ise kişi ve eşya isimleri ile birlikte sıkça kullanılan parolalar birbiri ardından denenir. Bunun için genellikle Internet üzerinde mevcut olan ve saldırıyı sistemli hale getiren "rainbow-gökkuşağı" tabloları kullanılır [1], [2].
Sözlük saldırılarından kaçınmak için günlük hayatta sıkça kullanılan sözcükleri parola olarak kullanmamak gerekir. Bunların genellikle kısa olmaları (2-8 karakter) kaba kuvvet saldırılarılarına

açık olmaları sonucunu doğurur. Örneğin, kişi ismi, doğum yılı, gibi kolayca tahmin edilebilecek harf dizileriyle birlikte Türkçe, İngilizce veya başka dillerde kullanılan kelimeleri yalın halleriyle parola olarak kullanmamak gerekir. Zira bunların toplam sayısı birkaç milyonu geçmediği için aşağıda anlatılacağı gibi sözlük saldırıları vasıtasıyla kolayca kırılabilirler.

Parolalarda Türkçe karakterlerin (ı,İ,ğ,Ğ,ş,Ş,ç,Ç,ü,Ü,ö,Ö) kullanılması önerilmez. Zira bu karakterler farklı sistemlerde farklı şekilde işlenebilirler.

Tablo1: Bazı metin parçalarının özütleri

Metin	**Tür**	**Özüt**
a	MD5	0cc175b9c0f1b6a831c399e269772661
bilgisayar	MD5	bb45cc31d4b20c15f2c5e0a805c23a86
Bilgisayar	MD5	d9f5977f1ca30012510bf30569957723
Bilgisayar kullanmak eğlencelidir.	MD5	35272b8ebf1328167c5e47792d44f99a
a	SHA1	86f7e437faa5a7fce15d1ddcb9eaeaea377667b8
bilgisayar	SHA1	9e087f57c36fa83fdc9a43008f1f31c6f4c81e7c
Bilgisayar	SHA1	8fafd5fda22422f3754d92a65d815bdf735bfe7b
Bilgisayar kullanmak eğlencelidir.	SHA1	d27c00e35cfe828e738274e0e374b6e8fe64472f
a	SHA256	ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb
bilgisayar	SHA256	0734326bf69f65d0071300c274c0f0ddc1a343b5161519597d2bf2854b8455a1
Bilgisayar	SHA256	06e44c77accf6db4b944092b65ae8e7a173287ff569d95e72ffda7f30e7b5186
Bilgisayar kullanmak eğlencelidir.	SHA256	58f6cf84c6c32c8902ea65ce68fc76afefa73fcbeaef8e6acd7ffe136df02093

4. "Güçlü" parola oluşturulması

Parolalarda küçük ve büyük harflerle birlikte rakamların ve özel karakterlerin de kullanılması gerekir. Bunların toplam sayıları yaklaşık olarak tablo2 de gösterilmektedir:

Tablo 2: Güçlü parola oluşturulması

		Toplam karakter
Rakam	0123456789	10
Küçük harf	ab ... yz	26
Büyük harf	AB … YZ	26
Özel karakter (sadece bazıları)	"!'^+%&/()=?-_*#$${:;}[.,]~	26
Toplam		88

Yukardaki tabloya göre beş küçük harften oluşan bir parolayı kaba kuvvet yoluyla çözmek için yapılması gereken toplam işlem sayısı şöyledir (çözüm büyük ihtimalle işlemlerin tamamını bitirmeden gerçekleşecektir):

1 karakter uzunluğu: 261 = 26
2 karakter uzunluğu: 262 = 676
3 karakter uzunluğu: 263 = 17,576
4 karakter uzunluğu: 264 = 456,976
5 karakter uzunluğu: 265 = 11,881,376

Yukarda belirtildiği gibi kaba kuvvet yönteminde bir karakterden başlayarak tümkombinasyonların denenmesi gerekmektedir. Ancak ilk dört satırdaki rakamlar son satıra göre ihmal edilebilir derecede küçük olduğu için hesaplamaya dahil edilmeyebilirler (bu durum aşağıdaki hesaplamalar için de geçerlidir). Dolayısıyla beş karakter uzunluğunda ve sadece küçük harflerden oluşan bir parolayı çözebilmek için en fazla 12 milyon civarında işlem yapmak gerekir. Parolanın denemelerin ortasında çözülebileceği önkabuluyle gerçek hayatta yapılması gereken işlem sayısı yaklaşık 6 milyondur.

Eğer küçük ve büyük harflerle birlikte sayıları ve özel karakterleri içeren bir parola kullanılırsa (toplam 88 karakter) uzunluğu beş karaktere kadar olan parolalar için gereken yaklaşık işlem sayıları aşağıdadır:

1 karakter uzunluğu:
881 = 88 /2 = 44

2 karakter uzunluğu:
882 = 7,744 /2 = 3872

3 karakter uzunluğu:
883 = 681,472 /2 = 340,736

4 karakter uzunluğu:
884 = 59,969,536 /2 = 29,984,768

5 karakter uzunluğu:
885 = 5,277,319,168 /2 = 2,638,659,584

Görüldüğü gibi sadece küçük harflerden oluşan beş karakterlik parolada yapılması gereken işlem sayısı 6 milyon iken küçük ve büyük harflerle birlikte sayıları ve özel karakterleri içeren parolada bu rakam yaklaşık olarak 5.2 milyarın yarısı olan 2.6 milyara çıkmaktadır.

Edward Snowden'a göre NSA'nın süper bilgisayarları kaba kuvvet yöntemiyle parola çözmek için saniyede

bir trilyon (1012) işlem yapabilmektedir. Yani bu bilgisayarlar beş karakterlik bir parolayı saniyenin küçük bir kesri kadar zamanda çözebilirler. Ancak uzunluk arttıkça gereken süre dramatik bir şekilde yükselmektedir. Aşağıda çeşitli uzunluktaki parolalar için bu kapasitedeki bir bilgisayarın yaklaşık olarak çalışması gereken zamanlar gösterilmektedir:

5 karakter uzunluğu:
885 = 5,2*109 /2 = 2.6*109 işlem
→ 0.0026 saniye

6 karakter uzunluğu:
886 = 4.6*1011 /2 = 2.3*1011 işlem
→ 0.23 saniye

7 karakter uzunluğu:
887 = 4.1*1013 /2 = 2*1013 işlem
→ 20.4 saniye

8 karakter uzunluğu:
888 = 3.6*1015 /2 = 1.8*1015 işlem
→ 1,798 saniye → yarım saat

9 karakter uzunluğu:
889 = 3.2*1017 /2 = 1.6*1017 işlem
→ 316,478 saniye → 88 saat

10 karakter uzunluğu:
8810 = 2.8*1019 /2 = 1.4*1019 işlem
→ 1.4*107 saniye → 161 gün

11 karakter uzunluğu:
8811 = 2.4*1021 /2 = 1.2*1021 işlem
→ 1.2*109 saniye → 39 yıl

12 karakter uzunluğu:
8812 = 2.2*1023 /2 = 1.1*1023 işlem
→ 1.1*1011 saniye → 3,419 yıl

13 karakter uzunluğu:
8813 = 1.9*1025 /2 = 9.5*1024 işlem → 9.5*1012 saniye → 300,911 yıl

14 karakter uzunluğu:
8814 = 1.7*1027 /2 = 8.4*1026 işlem → 8.4*1014 saniye → 26,480,172 yıl

Görüldüğü gibi özellikle 10 karakterin üzerindeki küçük ve büyük harflerle rakamları ve özel karakterleri içeren parolaları kaba kuvvet yöntemiyle kırmak günümüzün en gelişkin bilgisayarları ile bile imkansız hale gelmektedir. Bununla birlikte aşağıdakileri de gözönünde tutmak gereklidir:

- Bu rakamlar saniyede bir trilyon işlem yapabilen süper bilgisayarlar içindir. Bu
bilgisayarlara erişim ise çok kısıtlıdır. Dolayısıyla parola çözmek amaçlı saldırılarda
kullanılan diğer bilgisayarların çok daha fazla yavaş olduğu düşünülebilir. Ancak bilgisayar hızlarının dramatik şekilde arttığı günümüzde bu konuda da ihtiyatlı olmak gerekir. Örneğin, 2012 tarihli bir raporda parola kırmak için kullanılan sıradan bir kişisel bilgisayarın saniyede 8.2 milyar işlem yapabildiği raporlanmaktadır [3].

- Yukarda da belirtildiği gibi kaba kuvvet yönteminde aranan değerin "yarı yolda" bulunacağı farzedilmiştir. Diğer bir deyişle örneğin toplam bin değer araştırılırken beş yüzüncü değerin aranılan değer olduğu kabul edilmiştir. Ancak gerçek hayattta aranılan değer üçüncü de, dokuz yüzüncü de olabilir. Dolayısıyla kullanılan algoritmaya -ve şansa- bağlı olarak parola ne kadar uzun olursa olsun kısa sürede kırılması ihtimali mevcuttur.

- Halen araştırma aşamasında olan kuantum bilgisayarlarının günümüz teknolojisiyle üretilen bilgisayarlardan binlerce kat daha hızlı çalışacağı öngörülmektedir. Bu teknoloji -belki 20-30 sene sonra- kullanılmaya başlandığında günümüzde hız engeline takılan birçok işlem yapılabilir hale gelecektir.

- Aşağıda [4] numaralı kaynakta belirtilen site günümüzde kullanılan sıradan bir bilgisayar ile çeşitli parolaların kırılma zamanları hakkında bir fikir vermektedir. Ancak bilgisayar hızları arasında çok büyük farkların olduğunu gözden kaçırmamak gerekir.

- Parola ne kadar uzun ve "kuvvetli" olursa olsun "keylogger" denilen programlar vasıtasıyla kaydedilip saldırganlar tarafından kullanılabilir. Keylogger programlarının e-posta vasıtasıyla gönderilip kullanıcı parolalarının ele geçirilmesi Türkiye'de sıkça görülmektedir. Bu ve diğer zararlı yazılımların tamamına yakını ticari bir ürün olan Microsoft'un Windows işletim sistemi üzerinde çalışmaktadır. Bu nedenle Windows yerine Linux sürümlerinden birinin kullanılması önerilir. (Linux özgür yazılım felsefesi ile imece usulu geliştirilip ücretsiz olarak kullanıma sunulan bir işletim sistemidir.) Ayrıca parola girerken klavye kullanmaktan kaçınılması da keylogger yazılımını etkisiz hale getirecektir. Nitekim elektronik bankacılık uygulamalarında parolanın klavye yerine ekrandan girilmesiyle banka hesaplarının kötü niyetle ele geçirilmesi büyük oranda engellenmektedir. Linux ortamında "florence" gibi yazılımlar kullanıcıya bu imkanı sunar.

- Parola uzunluğu arttıkça hatırlama sorunu büyümektedir. Bunun için parolanın bazı kısımları akılda tutması kolay kelimelerle oluşturulabilir (passphrase). Bu durumda kelimelerin bazı kısımlarını "bozmak" gerekebilir. Örneğin: 3rH&9=.#d?guVNli}bir,ParOla.

- Aynı parolayı asla birden fazla yerde kullanmamak gerekir. Çok fazla parolanın hatırlanmasının gerekli olduğu durumlarda bu amaç için Linux ortamında geliştirilmiş birçok programdan birisi kullanılabilir.