Türk Kullanıcıların Parola Seçimindeki Eğilimleri

İlker Korkmaz[1] Mehmet Emin Dalkılıç[2]

[1]Bilgisayar Mühendisliği Bölümü, İzmir Ekonomi Üniversitesi, İzmir
[2]Uluslararası Bilgisayar Enstitüsü, Ege Üniversitesi, İzmir

[1]e-posta: ilker.korkmaz@ieu.edu.tr [2] e-posta: mehmet.emin.dalkilic@ege.edu.tr

Özetçe

Bilgisayar sistemlerinin güvenliği ele alındığında, kullanıcı doğrulama ve yetkilendirme amacıyla, birçok sistemde ilk denetleme noktası olarak ilgili parola kontrolleri mevcuttur. Parolaların sadece gizli değil aynı zamanda sahibi dışındaki kişiler tarafından kolayca tahmin edilemeyecek şekilde seçilmesi ve sürekli korunması güvenlik açısından uygun görülmektedir. Bu noktada, bilhassa kritik sistemlere erişim esnasındaki kullanıcı doğrulama mekanizmalarında girilen parolalar için, güçlü görülebilecek nitelikte uygun parolaların seçimi, güvenlik için önem kazanmaktadır. Bu bildiri parolaların seçiminde uygun olan ve olmayan biçimleri belirlemek üzere gerçek kullanıcı parolalarının şifrelenip daha sonra kırılmaya çalışılması ile elde edilen bulguları ve bu bulgular üzerinde yapılan istatistiksel çalışmaları sunmaktadır. Deneyler, Türk kullanıcıların sistemlerinde kullanmak üzere kısıtsız bir şekilde seçtikleri parolalar üzerinde gerçekleştirilerek, parola seçimindeki genel eğilimler ortaya konmuş ve değerlendirilmiştir.

Anahtar Kelimeler: zayıf parola, parola kırma, parola denetimi, parola seçim eğilimi.

1. Giriş

Bilgisayar sistemlerinde güvenliğin ilk ve genellikle en önemli adımı kullanıcı parolalarıdır. "Parola" kavramı "şifre" kavramı olarak da geçebilmektedir. Parola, sisteme bağlanan kullanıcının kimliğinin doğrulanması amacı ile kullanılan ve bu kullanım amacı açısından gizli olan bir anahtardır. Parola seçiminde, kendi haline bırakılan kullanıcıların doğal olarak hatırlanması kolay ve kısa parolalar seçtikleri bilinmektedir. Bu tür parolalar bilgisayar korsanları için kolay hedefler teşkil etmekte ve tek bir "zayıf" kullanıcı parolası bile tüm sistemin güvenliğini tehlikeye düşürebilmektedir [1].

Parola güvenliğinde amaç kullanıcıları yönlendirerek "zayıf" parolaların kullanımını engellemek ve sistem güvenliğini arttırmaktır. Bu yolda öncül parola denetimi mekanizmaları aracılığıyla, kullanıcıların parola seçimi anında zayıf görülen bir parolayı seçmesi kabul edilmeyip kullanıcılar daha güçlü bir seçime yönlendirilebilir [2, 3, 4]. Öncül parola denetim yazılımları temel olarak bir "zayıf parola" modeli oluşturur ve aday parolaları bu modele uygunluk açısından değerlendirerek modele uyan parolaları "zayıf" olarak işaretleyip, o parolaların sisteme girişine seçim anında engel olur.

İyi bir "zayıf parola modeli" oluşturabilmek ancak kullanıcıların ne tür zayıf parolalar seçmeye eğilimi olduğunu bilmekten geçer. Üretilen bir zayıf parola modeli ile denetlenen parola adayları, bilinen bu eğilimler ışığında değerlendirilebilir. Ayrıca, bilinen bu eğilimler, bir zayıf parola modelinin oluşturulmasında da kullanılabilir. Bu doğrultuda, kullanıcı eğilimlerini en doğru şekilde anlayabilmek için gerçek kullanıcıların, bilgisayar sistemlerinde aktif olarak kullandığı gerçek parolaların incelenmesi yararlı olacaktır.

Bu çalışmada, [1] içeriğinde incelenen konular dahilinde gerçekleştirilen ilgili araştırmalar aktarılarak, parola seçiminde güvenlik arttırıcı bir durum da teşkil edebilmesi amacıyla, Türk kullanıcıların gerçek parolaları ile yapılan deneyler ve bu deneyler aracılığıyla ne tür niteliklerin zayıf olarak belirlendiği sunulmaktadır. Ayrıca, Türk kullanıcı parolaları içeriğindeki karakterleri baz alan istatistiksel çalışmaların bulguları sunulup Türk kullanıcıların parola seçim eğilimleri değerlendirilmektedir.

Bildirinin 2. bölümünde parola seçimlerinin belirlenmesinde kullanılan yöntem açıklanıp 3. bölümde Türk kullanıcıların parolalarında belirlenebilen özellikler sunulmuş ve son bölümde de gerçekleştirilen deneyler ile ilgili sonuçlar aktarılmıştır.

2. Parola Seçimlerinin Belirlenmesinde Kullanılan Yöntem

Parola seçimlerindeki eğilimlerin belirlenmesi için, temel olarak, çok sayıda parola üzerinde çeşitli karakteristik özellikler sorgulanmaktadır. Bu bağlamda, literatürde ilk olarak Klein [5] en geniş çaplı kesime ulaşıp en fazla sayıda gerçek veri olarak (yaklaşık 14000 adet) şifreli parolaları elde edip kırmaya çalışmış ve kırılabilen parolaların karakteristik özelliklerine ait bulguları paylaşmıştır. Klein [5], çok sayıda sistem sorumlusundan yönettikleri sistemlerde bulunan parolaları şifreli halde alıp gerçekleştirdiği testler ile 1 hafta içinde parolaların yaklaşık % 20'sinin, 1 yıl sonunda da toplam % 25'inin kırılabildiğini ortaya koymuştur.

Gerçek parolaların açık olarak elde edilmesi için, ilgili sistemlerde kullanılan parolaların, sistemlerde şifrelenmeden saklanıyor olması veya ilgili bir dosyada açık halde saklanıyor olması ve bu dosyanın elde edilebilmesi ihtiyaçtır ki bunlar karşılanması zor koşullardır. Buna karşın, ilgili sistemlerde şifrelenmiş olarak saklanan parolaların elde edilmesi sonucu, sözlük atağı gibi yöntemler kullanılarak parolaların açık halleri elde edilebilmektedir.

Bizim çalışmamızda, güvenilir kaynaklardan elde edilen, bir sistemde kullanılmakta olan ve kısıtsız olarak seçilmiş olan gerçek Türkçe parolalar (2564 adet) kullanılmıştır. Bu parolaların öncelikle şifrelenip sonrasında kırılmaya çalışılması yanı sıra, şifrelenmemiş haldeki tüm açık Türkçe

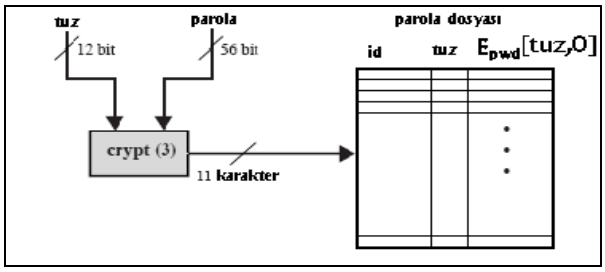
parolaları, şifrelendikten sonra kırılabilenleri ve kırılamayanları 3 farklı grup halinde tutulup bu gruplardaki parolaların karakteristik özellikleri incelenmiştir. Açık parolalar üzerinde incelemeler ilk başta tüm grup için de yapılabilirdi fakat o durumda karakteristik özelliklerine göre gruplanacak olan parolaların hangilerinin ne tür bir değerlendirme sonucunda zayıf olarak algılandığı tutarlı olmayabilirdi. Böyle bir görecelilik yerine, karakteristikleri belirlemek üzere 3 gruptaki parolalar üzerinde ayrı ayrı yapılan aynı sorgulamalar ve karşılaştırmalar sonucunda, kırılabilmiş parola grubu içinde yer alan parolaların zayıf olduğu düşüncesine dayanarak, kullanıcı eğilimleri belirlenmeye çalışılmıştır. Kullanıcı eğilimleri hakkında yaptığımız değerlendirmeler ve yorumlar bu istatistiklere dayalı olduğu üzere ve incelenen parolalar gerçek olduğu üzere, yöntem tutarlı ve anlamlı görülmektedir.

3. Parola Kırma

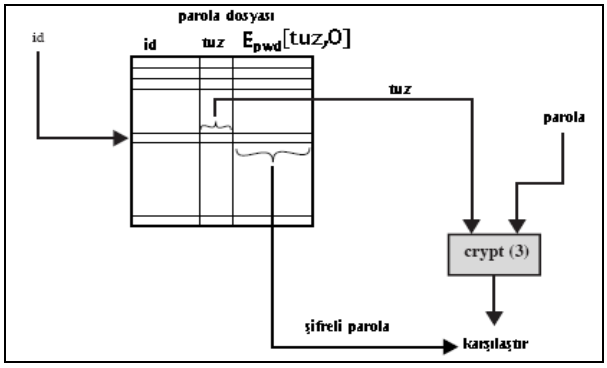
Bu bölümde, parola kırma konusuyla ilgili olan çalışmalara değinilerek gerçekleştirilen parola kırma deneyi, genel sonuçları ile birlikte sunulmuştur.

3.1. Parola Mekanizması

Çok kullanıcılı sistemlerde, her kullanıcının hesabına yönelik belirleyici bir isim ve bu isimle ilişkilendirilen bir parola söz konusudur. Ayrıca, her kullanıcının kendi hesabındaki veri kendisine aittir ve bu verinin gizli tutulabilme imkanı sistem desteği ile sunulmaktadır. Temel olarak kullanıcı doğrulanması esnasında kullanılan parolaların saklanma biçimleri kullanılan parola yönetim mekanizmasına bağlıdır. UNIX parola yönetim mekanizmasının parola saklama biçimi Şekil 1'de ve parola doğrulama yöntemi Şekil 2'de gösterilmiştir.



Şekil 1: UNIX parola saklama biçimi [3].



Şekil 2: UNIX parola doğrulama biçimi [3].

Kullanıcılar tarafından seçilen, ekrana bastırılabilen en fazla 8 karakterden oluşan parola, her birinin en düşük anlamlı 7-biti alınıp 7-bit ASCII kodlama düşünülerek 56-bit uzunluğunda bir değere dönüştürülür. Şekil 1'de gösterildiği gibi, bu değer, *crypt(3)* [1] olarak bilinen ve DES algoritmasına dayanan şifreleme fonksiyonunda anahtar değeri olarak kullanılacaktır. Anahtar değer ve parola seçim anında üretilen rastgele 12-bit tuz (*salt*) değeri *crypt(3)* fonksiyonuna girildiğinde, çıkış 11 karakterlik şifrelenmiş parolayı işaret eder. Şifrelenmiş parola, tuz değerinin açık hali ile birlikte sistemdeki parola dosyasında ilgili kullanıcının hanesine yüklenir. Tuz değeri sayesinde, aynı parolayı seçen kullanıcıların parolalarının şifreli hallerinin farklı olması sağlanmaktadır.

Bir kullanıcı, UNIX sistemindeki hesabına giriş esnasında kullanıcı adını ve parolasını sunduğunda, işletim sistemi, parola dosyasındaki ilgili kullanıcı adı ile ilişkili hanedeki açık tuz değerini ve şifreli parolayı Şekil 2'de gösterildiği gibi ele alır. Kullanıcının sunduğu açık parola ve dosyadan alınan tuz değeri *crypt(3)* fonksiyonundan geçirildiğinde oluşan sonuç, parola dosyasındaki sonuç ile karşılaştırıldığında aynı ise kullanıcı sisteme kabul edilir [3].

3.2. Parola Kırma Yöntemleri

Parolaları açık tutmamak amacıyla kullanılan şifreleme veya öz alma algoritmalarının gücü, parolaların kırılamamasının gücünü vermektedir. İdeal bir algoritma ile geri dönüşü olmayan bir şifreleme veya öz alma işlemi yapılsa bile, bu prosedürde kullanılan ilk anahtar girişi bulunabilirse, işlemden çıkan veri, olası bir parolanın şifrelenmiş hali olacaktır. Bu durumda iki alternatif ortaya çıkmaktadır: Çıkışın doğruluğunu kontrol edebilmek amacıyla, parola dosyasının ele geçirilmesiyle karşılaştırma yapılması veya parola dosyasına ihtiyaç duymadan, sisteme bağlı iken deneme yanılma yönteminin kullanılması. Bu çalışmada, ilk alternatif denenip eldeki tüm açık parolalar Linux sistemde ilişkili kullanıcı hesapları oluşturularak saklanmış ve sistemdeki ilgili şifreli parola dosyası elde edilip kırılmaya çalışılmıştır.

Parola kırma işleminde temelde yapılan, olası açık parola adaylarının şifrelenerek, şifrelenmiş gerçek parola metinleri ile karşılaştırılmasıdır. Bu doğrultuda, olası parola adayları çeşitli yöntemlerle oluşturulabilir. Kaba kuvvet atağıyla, parolalarda kullanılan tüm karakter uzayını tarayarak olası en fazla 8 karakterli parolaları taramak ilk akla gelen yöntemdir. Fakat bu durumda zaman sorunu doğmaktadır. Bunların yerine sözlük atağı yöntemi seçilerek, tahmin edilebilecek olası parola aday sözcüklerinin de yer aldığı istenen her aday parolanın eklendiği bir sözlük oluşturulup içeriğindeki her sözcük otomatik olarak şifrelenerek karşılaştırma denenebilir. Ayrıca sözlük içindeki parola adayı sözcükler, büyük ve küçük harf değişimi, kelimelerin tersinin alınması, kelime sonlarına nümerik karakter eklenmesi gibi çeşitli karakter dizgisi işlemlerinden geçirilerek, sözlük içeriği genişletilebilir ve dolayısıyla otomatik olarak denenecek aday parola sayısı arttırılabilir [6].

[1] http://www.belgeler.org/man/man3/man3-crypt.html, 29.10.2009 tarihinde erişilmiştir.

3.3. Parola Kırıcı Araçlar

Parola kırıcı yazılım araçları, genel olarak iki amaçla kullanılmaktadır. İlk amaç, bilgisayar korsanları tarafından ele geçirilen parola dosyasındaki gizli parolaların açığa çıkarılmasıdır. Diğer bir amaç da, sistem yöneticileri tarafından, ardıl parola denetlemesi yapmak üzere zayıf parolaları ortaya çıkarmak için parola dosyalarındaki parolaların taranmasıdır. Bilhassa ardıl parola denetimi amacıyla sistemdeki zayıf parolaların belirlenmesi için kullanılan parola kırıcı araçları İnternet ortamında birçok yerde indirilebilir halde bulmak mümkündür. Parola kırıcı araçlardan en yaygın kullanılanları, *John the Ripper* [2] ve *Crack* [3] yazılımlarıdır. Bu çalışmada, şifreli haldeki gerçek kullanıcı parolalarını kırmak amacıyla yapılan deneylerde, *John the Ripper 1.7.0.2* sürümü kullanılmıştır.

3.4. Parola Kırma Deney Sonuçları

Güvenilir kaynaklardan elde edilen parola dosyalarında yer alan açık parolalar ve bunların ilişkilendirildiği kullanıcılara ait bilgiler, mahremiyet kavramı etik olarak düşünülerek, araştırma kapsamı dışında kesinlikle kullanılmamıştır. Bu elde edilen parola dosyaları, Klein [5] deneyine benzer bir şekilde kırılmaya çalışılmıştır. Fakat, Klein [5] deneyinde sadece şifreli parolalar mevcut iken, bizim çalışmamızda eldeki açık parolalar şifrelenerek benzer şifreli parola dosyaları oluşturulmuştur. Ayrıca, bizim deneyimizdeki parola miktarımız Klein deneyindekinin % 20'si civarındadır.

Açık olarak elde edilmiş olan 2564 parola şifrelendikten sonra, parolaların sahiplerinin bilgilerinin yer aldığı ve yer almadığı iki ayrı dosya oluşturulup iki ayrı Linux makinede kırılmaya çalışılmıştır. Deneyin ilk 1 aylık sürecinde parolaların toplam 777 adedinin (% 30) tahmin edilebildiği gözlenmiştir. Daha sonra deney sürdürüldüyse de sonraki 1 ay içinde herhangi bir parola kırılamadığı için deney sonlandırılmıştır. Her iki makinede de aynı şekilde kırılmak üzere denenen parolaların yaklaşık % 5'i ilk 15 dakika içinde, % 10'una yakını da ilk gün içinde tahmin edilebilmiştir. Deney sonunda her iki makinede de ortak olarak tahmin edilen 712 parola gözlenmiştir. Kullanıcı bilgilerinin de yer aldığı dosyanın kırılmaya çalışıldığı makinede ek olarak 65 parola daha program tarafından kırılabilmiştir. Buna göre, kırılan parolalar içinden en az 65 adedinin (yaklaşık % 9) kullanıcı ismi ve bilgilerine has veriler olduğu anlaşılmaktadır. Kullanıcıların hesap bilgilerinde sundukları veriler ile ilişkili parola seçmiş olmaları, kullanıcılar için ortak bir olumsuz seçim eğilimidir.

Deney sonuçlarına göre, kırılabilen parolalar arasında bazı ilginç özellikler hemen farkedilmiştir. Mesela, kırılan 777 parolanın 564 adedi, sadece nümerik karakter içermektedir. Buradan anlaşıldığı üzere, sadece rakam dışında hiçbir karakter kullanmadan parola seçen kullanıcı sayısı azımsanmayacak orandadır. Ayrıca, kırılan parolaların büyük oranının sadece rakamlardan oluşması, bu tür parolaların zayıf olarak nitelenebileceğini göstermektedir ki sadece rakam barındıran parola seçimi, zayıf bir parola seçim eğilimi olarak değerlendirilmektedir.

Türk kullanıcıların parola seçim eğilimlerine ışık tutabilmesi amacıyla aktarılabilecek bir gözlem de, kırılan parolalar arasında sadece 32 parolanın en az bir Türkçe alfabeye has karakter içerdiğidir. 2564 Türk kullanıcısı içinde % 98'den daha fazlasının parola seçiminde Türkçe karakter tercih etmeyişi, muhtemelen Türkçe karakterlerin sistemlerde sorun oluşturabileceği şüphesinden kaynaklanmaktadır. Aslında, bu sadece Türk kullanıcılara has bir özellik olarak görülmeyip tüm dünyada farklı milletlerin de parola seçiminde İngilizce alfabe dışı karakterleri tercih etmediği düşünülmektedir.

Deney sonuçlarına genel bakıldığında, kırılan parolaların arasında kullanıcı ismi ile ilişkili olan, kullanıcı bilgileri ile ilişkili olan, sadece sayılardan oluşan, sadece büyük harf karakterlerinden oluşan, sadece küçük harf karakterlerinden oluşan, karışık karakterlerden oluşan, isim ve soyadı gibi görülebilen, kelime sonlarına sayı eklenerek oluşturulan, farklı kullanıcılar tarafından aynı şekilde seçilen çeşitli parolaların yer aldığı görülmüştür.

Klein deneyinde ve Türk kullanıcılar için benzer yapıda olan bizim deneyimizde gerçek parolalar kullanılmıştır. Parola karakteristiklerini inceleme konusunda, literatürde benzer amaçlarla farklı yöntemlere de rastlanmaktadır. Yan v.d. [7] parolaların hatırlanabilirliğini incelemek amacıyla, 388 katılımcı ile kontrollü deneme yöntemi uygulayarak bir deney düzenlemiştir. Katılımcıların gruplandırılarak, farklı gruplara farklı uyarılar ve yönlendirmeler yapılması yoluyla, katılımcılardan kendilerine has parola seçmeleri istenmiş ve daha sonra bu parolalar şifrelenip kırılmaya çalışılmıştır. Deneyin bir sonucu olarak, kolay hatırlanabilecek şekilde seçilen parolaların aynı zamanda tahmin edilmesi veya kırılması zor olabilmesi, yani güçlü parolalar sınıfında olabilmesi için, kullanıcıların kendilerine has anımsatıcı *(mnemonic)* parolaları seçmeleri önerilmiştir [7]. Anımsatıcı ifadesi ile kastedilen, birkaç sözcükten oluşan kullanıcının kendisine has anlamlı bir cümledeki kelimelerin ilk harflerini, o cümleyi anımsatacak şekilde parola olarak seçmesidir. Mesela, bir anımsatıcı olarak, "Ben 3 yıldır Mühendislik eğitimi alıyorum, memnunum" cümlesinden yararlanarak oluşturulan "B3yMea,m" parolası örnek verilebilir.

4. Türk Kullanıcılarının Parolalarının Genel Özellikleri

Bizim çalışmamızda, Klein [5] ve Yan v.d. [7] tarafından yapılan deneylerden farklı olarak, ayrıca gerçek kullanıcılardan elde edilen açık parolalar da özellikleri açısından incelenmiştir. Sadece kırılan parolaların incelenmesi ile zayıf parola özellikleri belirlenebildiği gibi, kırılamayan parolaların da incelenmesiyle birlikte zayıf ve güçlü parola arasındaki çizgi daha belirgin hale getirilmeye çalışılmıştır. Buradan yola çıkılarak, mevcut tüm açık parolaların karakteristik özelliklerini gruplamak amacıyla, istatistiksel olarak parola seçim eğilimi belirleme çalışmaları yapılmıştır.

Tüm parolaların incelenerek, zayıf parolalara ait olan ve güçlü parolalara ait olan ortak özelliklerin belirlenmesi amacıyla

---

[2] http://www.openwall.com/john/, 29.10.2009 tarihinde erişilmiştir.

[3] ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/crack, 29.10.2009 tarihinde erişilmiştir.

düşünülen yöntem, Perl yazılımı yardımıyla parolaların karakterlerinin incelenmesi ve karakterlere has istatistik verilerinin belirlenmesidir. Bu veriler, zayıf veya güçlü gruba ait parolalar hakkında özellikleri sunarken, istatistik çalışmaları sonucunda yüksek oranda karşılaşılan ortak özelliklerin, kullanıcıların parola seçimindeki eğilimlerini yansıtacağı düşünülmüştür. Yapılan istatistik incelemelerinin sonuçları Çizelge 1'de, Çizelge 2'de ve Çizelge 3'te sunulmuştur.

Çizelge 1: Parolaların uzunluk istatistikleri.

Uzunluk	Kırılabilen		Kırılamayan		Tümü	
	#	%	#	%	#	%
2	1	%100	0	%0	1	%0
3	26	%100	0	%0	26	%1
4	485	%96	21	%4	506	%20
5	98	%42	130	%58	228	%9
6	136	%31	300	%69	436	%17
7	10	%4	208	%96	218	%8
8	21	%2	1128	%98	1149	%45
Toplam	**777**	**%30**	**1787**	**%70**	**2564**	**%100**
Ortalama	**4,58**		**7,28**		**6,46**	

Çizelge 1'de hesaplanabileceği gibi, kırılamayan 7 karakterli parolalar tüm 7 karakterli parolaların % 96'sını oluşturmaktadır. 7 karakterden daha az uzunluktaki parolalar için bu özellik açısından böyle yüksek bir seviyeye ulaşılmamıştır. Yine Çizelge 1'de verilen değerlere göre, kırılabilen parolalar arasında 6 karakter veya daha kısa olanların oranı % 96 olarak hesaplanabilmektedir. Bu bulgulara göre, parola uzunluğu için 7 değerinin kritik değer olduğu ve 7'den az uzunluktaki parolaların zayıf görüldüğü vurgulanabilir. Bir parolayı uzunluk açısından zayıf niteliğinden kurtarmak için, en az 7 karakterli seçim uygun olacaktır. Bu durumda, tüm parolaların ortalama uzunluğu olan 6,46 değeri de geçilmiş olacaktır. Bunun yanı sıra, kullanılan 8 karakterli parolaların tüm parolalar içindeki oranı % 45 seviyelerindedir ki bu, kullanıcıların 8 karakterli parola seçme yönünde yüksek bir eğilimi olduğunu göstermektedir.

Çizelge 2: Parolaların karakter istatistikleri.

Özellik	Kırılabilen		Kırılamayan		Tümü	
	#	%	#	%	#	%
En az 1 adet nümerik karakter içeren parola	587	%31	1278	%69	1865	%73
En az 1 adet büyük harf içeren parola	199	%20	802	%80	1001	%39
En az 1 adet Türkçe'ye has karakter içeren parola	32	%10	280	%90	312	%12
En az 1 adet harf veya sayı olmayan özel bir karakter içeren parola	2	%8	23	%92	25	%1
İçeriğinin tümü nümerik karakterlerden oluşan parola	564	%37	976	%63	1540	%60
İçeriğinin tümü alfabetik karakterlerden oluşan parola	188	%27	500	%73	688	%26
İçeriğinin tümü özel karakterlerden oluşan parola	0	%0	0	%0	0	%0

Çizelge 2'de, parolaların barındırdığı karakterlerin niteliklerine yönelik istatistikler sunulmuştur. Çizelge 2'deki verilere dayanarak kullanıcı eğilimleri hakkında yapılabilecek yorumların başında, parolaların % 73'ünde gözlenen en az 1 adet nümerik karakter ile, Türk kullanıcıların parolalarında rakam karakteri kullanma eğiliminin fazla olduğudur.

Çizelge 2'ye göre, tüm parolaların içinde, en az 1 büyük harf kullananların oranı % 39 olup, Türk kullanıcılarının parolaları kuvvetlendirme amacıyla büyük harf karakteri seçme eğiliminde oldukları düşünülmektedir.

Çizelge 2'de belirtilen bir başka nicelik ise, tüm kullanıcıların % 12'sinin parolalarında İngilizce alfabede yer almayıp Türkçe alfabede yer alan bir karakter gözlendiği ve bunların % 90'a yakınının kırılamadığıdır. Buna göre, Türk kullanıcıların parolalarında Türkçe alfabeye has olan harfleri seçmelerinin genel anlamda parola kırıcılara karşı bir güç unsuru olacağı düşünülmektedir. Ayrıca, yalnız Türk kullanıcılar için değil herkes için, başka dillerde yer almayıp sadece kendi ana dillerinin alfabesinde yer alan karakterler varsa, parolalarında bu harflerden en az 1 karakter kullanmaları önerilmektedir.

Çizelge 2'deki verilere göre, harf veya sayı olmayan özel bir karakter kullanılarak seçilen parolaların kırılma oranının % 8 olarak hesaplanması sonucu, bu türdeki parola seçim eğilimi, parola gücü açısından olumlu görülmüştür. Fakat tüm kullanıcılar içinde en az 1 özel karakter kullananlar 25 kişi olarak belirlendiğinden, Türk kullanıcılarının parolalarında özel karakter kullanma eğilimlerinin düşük olduğu anlaşılmaktadır.

Çizelge 3: Parolaların karakter gruplanma istatistikleri.

Özellik	Kırılabilen	Kırılamayan	Tümü
P(1a+n)	4	3	7
P(2a+n)	6	34	40
P(3a+n)	4	32	36
P(1n+a)	0	1	1
P(2n+a)	0	5	5
P(3n+a)	0	0	0
P(a+1n)	5	25	30
P(a+2n)	3	87	90
P(a+3n)	5	24	29
P(n+1a)	0	0	0
P(n+2a)	0	13	13
P(n+3a)	0	5	5

Çizelge 3'te, parola içindeki karakterlerin, ardışık nümerik karakterler ve ardışık nümerik olmayan karakterler şeklinde gruplanmış olarak bulunmasına dair istatistikleri sunulmaktadır. Örnek olarak, içeriği ikili nümerik olmayan grup ile başlayıp gerisi tümüyle nümerik karakterden oluşan parolalar *P(2a+n)* şeklinde belirtilmiştir. Çizelge 3'teki verilerde beliren ilk yüksek kullanıcı eğilimi, parolaların içeriğindeki son 2 karakterin rakam olarak seçilmesidir. Çizelge 3'ten çıkarılan bir diğer sonuç da, içeriğinde hem nümerik olan hem de nümerik olmayan karakterler barındıran parolaları seçen kullanıcıların, karakter dizilişleri açısından, rakam karakterleri ile sonlanan parolaları, rakam olmayan karakterlerle sonlanan parolalara göre daha fazla tercih ettikleridir.

5. Sonuç

Bu araştırmada, Türk kullanıcıların gerçek parolalarının şifrelenip kırılması ve tüm açık parolaların çeşitli özelliklerine

göre incelenmesi ele alınarak parolaların zayıf ve güçlü nitelikleri belirlenip bunlar üzerinde yapılan istatistiksel gözlemler sunularak Türk kullanıcıların parola seçimindeki eğilimleri ortaya konmaya çalışılmıştır. Türk kullanıcı parolaları ile çalışıldığı için bulgular Türk kullanıcı eğilimleri olarak belirtilmiş olsa da, sonuçlar incelendiğinde, bu eğilimlerin Türk olmayan kullanıcılar için de genel olarak benzer olduğu düşünülmektedir.

Belirlenen zayıf parola nitelikleri aşağıda sıralanmıştır:

- Parola uzunluğunun 7 karakterden az olması.
- Parolada kullanılan karakterlerin tümünün nümerik olması.
- Parolada kullanılan karakterlerin tümünün alfabetik olması.
- İçeriğinde farklı tipte karakterler kullanılsa da, parolaların, nümerik karakterlerle sonlandırılması.
- Parolanın, uzunluğu 7 karakterden büyük 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.

Belirlenen güçlü parola nitelikleri aşağıda sıralanmıştır:

- 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).

Kullanıcılara, parola seçim eğilimlerini güçlü kriterleri taşıyacak parolaları seçme yönünde geliştirebilecek bilgilerin sunulması yararlı olacaktır. Bu bilgilerin, yukarıda sıralanmış olan kriterleri temel alması yanı sıra bunlara ilişkin bazı zayıf ve güçlü parola adayı örneklerini de içermesi önerilmektedir. Böylece, bu kriterler doğrultusunda, kullanıcıların güçlü parola seçme eğilimleri arttırılabilir.

6. Kaynakça

[1] Korkmaz İ., "Bilgisayar Sistemlerinde Parola Güvenliği Üzerine Bir Araştırma", Ege Üniversitesi Uluslararası Bilgisayar Enstitüsü Yüksek Lisans Tezi, 2006.

[2] Bergadano, F., Crispo, B., Ruflo, G., "High Dictionary Compression for Proactive Password Checking", *ACM Transactions on Information and System Security*, 1(1):3-25, 1998.

[3] Stallings, W., "Cryptography and Network Security, Pearson Education, Inc., New Jersey, 2003.

[4] Blundo C., D'Arco P., De Santis, A., Galdi C., "HYPPOCRATES: a new proactive password checker", *The Journal of Systems and Software,* 71:163-175, 2004.

[5] Klein, D.V., "Foiling the Cracker: A Survey of, and Improvements to, Password Security", Proceedings of the USENIX Workshop on Security (Portland, OR), USENIX Assoc., Berkeley, CA., 1990.

[6] Bishop, M., Klein D.V., "Improving system security via proactive password checking", *Computers & Security*, 14(3):233-249, 1995.

[7] 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.