YÖNETİM BİLİŞİM SİSTEMLERİ DERGİSİ
http://dergipark.ulakbim.gov.tr/ybs/

Yayın Geliş Tarihi: 30.05.2016
Yayına Kabul Tarihi: 15.08.2016
Online Yayın Tarihi: 05.10.2016

Cilt:1, Sayı:3, Yıl:2016, Sayfa 192-201
ISSN: 2148-3752

BİREYLERİN ŞİFRE YAPILARINA YÖNELİK BİR ARAŞTIRMA VE ŞİFRE ÖNERİ SİSTEMİ

Onur DOĞAN

Hakan AŞAN

Özet

Her ne kadar parmak okuma, retina tarama, ses algılama vb. yeni kimlik doğrulama teknikleri olsa da, kullanıcı adı ve şifre ile ulaşılan hesaplar özellikle internet ortamında oldukça yaygındır. Kişiler sanal dünyadaki eylemlerinin çoğunlukla şifre girilmesi zorunlu alanlarda gerçekleştirmektedirler. Şifreler aynı zamanda cep telefonu, bilgisayar, vb. aletler için kullanılmaktadır. Şifreler ile korunan bu alanlardaki içeriğin kötü amaçlı kişilerin eline geçmesinin kişiye maddi ve madeni zararlar verebileceği açıktır. Bu nedenle bireysel şifrelerin güvenliği oldukça önemlidir.

Bu çalışmada ele alınan bir örneklemin şifreleri; uzunluk, farklı kategorilerden karakter kullanımı, tahmin edilme zorluğu gibi konular üzerinden ele alınmıştır. İncelenen şifrelerin uzunlukları makul düzeyde olsa da, şifrelerin genellikle tahmin edilebilir kişisel bilgilerden oluşan ve az sayıda karakter grubu ile oluşturulan şifreler olduğu tespit edilmiştir. Güvenlik düzeyi düşük şifre tercihi yapan kullanıcılar için herhangi birini şifre olarak belirleyebilecekleri daha güvenli şifreler üreten şifre öneri sistemi tanıtılmıştır.

Anahtar Kelimeler: Bilgi Güvenliği, Şifre Gücü, Şifre Davranışı

A RESEARCH ON PEOPLE'S PASSWORDS STRUCTURES AND PASSWORD SUGGESTION SYSTEM

Abstract

Although there are some new authentication techniques such as; fingerprint confirmation, retinal scan, voice recognition, etc. accounts could be accessed by using a user name and password is still common especially on the internet. People have been performing most of the virtual activities on password required platforms. Passwords also have been using for accessing mobile phones, computers, and so on. The content of such fields that protected by passwords could damage both financial and emotional in case of handled by vicious people. Therefore, it is very important to the safety of individual passwords.

In this study, the passwords analysed according to their length, complexity and predictability. Results show that the lengths of the passwords are acceptable. However most of the passwords are predictable and have low complexity level, and also constituted by using personal information. In the present study also; Password Suggestion System has been introduced which could create more secure passwords for the people which have unsecure passwords.

Keywords: Information Security, Password Strength, Password Behavior

GİRİŞ

İnternet teknolojilerinin hızlı bir şekilde yaygınlaşması, sanal bir dünyanın ve bu dünyada bireysel alanların oluşmasına neden olmuştur. Özellikle sosyal ağ siteleri, kişisel bloglar gibi alanlarda insanlar düşüncelerini, özel hayatlarını paylaştıkları gibi bu alanlarda kişiye ait çok fazla miktarda bilgi de bulunmaktadır. Sanal ortamdaki bu kişisel alanların yaygınlaşması ile birlikte bu alanların korunmasını önemli hale gelmiştir. Bu nedenden dolayı bu tür sitelere üyelik işlemleri sırasında seçilecek olan şifrelerin güvenilir yapıda olması, gelecekte bu özel hesapların çalınmaması açısından çok önemlidir. İnternet alanlarının yanı sıra günlük hayatta kullandığımız teknolojik cihazlar, kredi kartları, vb.lerine de kişisel şifreler ile ulaşmaktayız. Bu tip şifreleri, gerçek hayattaki ev kapı kilidimize benzetebiliriz. Kapımızın kilidi güvenlik açısından ne kadar önemliyse, bu şifreler de o kadar önemli olduğu benzetmesi yapılabilir.

Bireylerin oluşturdukları şifrelerin daha güvenli hale getirilmesi için sistemler tarafından belli bir karakter uzunluğu veya karakter grubu alt sınırı konulmaktadır. Bunun yanı sıra şifre belirleme esnasında şifrenin güvenlik düzeyinin zayıf, orta, güçlü gibi ifadelerle kullanıcıya belirtilerek kullanıcının uyarılması ve daha güvenli şifreler oluşturmaya teşvik edilmesi de karşılaşılan uygulamalardandır. Ayrıca sistemler tarafından oluşturulan şifreleri kullanıcıya kullandırılması gibi uygulamalar da bulunmaktadır. Bu şekilde şifrelerin oluşturulması, şifre unutmak gibi sonuçları beraberinde getirebildiği gibi şifrelerin unutulmaması için aynı şifreyi farklı platformlarda kullanmak veya şifreyi bir yere not etmek de başka güvenlik açıklarına yol açabilir.

Bu çalışma, kullanıcıların güvenilir şekilde şifre belirleyip belirlemediklerini ölçmenin yanı sıra daha güvenli şifreler için tasarlanan şifre öneri sistemini tanıtmayı amaçlamaktadır. Kullanıcıların şifre belirleme alışkanlıklarını belirlemek için bir web uygulaması yazılmıştır. Bu web uygulaması üzerinden kullanıcıların şifre belirlemeleri istenmektedir. Yazılan web uygulamasında öncelikle kullanıcılardan temel bir form doldurmalarını istemektedir. Bu form da kullanıcıların bazı kişisel bilgileri alınmaktadır. Ayrıca sistem için kullanıcı adı ve şifre oluşturmaları istenmektedir. Bu bilgiler şifre oluşturma alışkanlıklarını keşfedebilmek ve şifre önerileri oluşturabilmek için kullanılacaktır.

Bu çalışmada ele alınan iki temel araştırma amacı aşağıdaki gibi özetlenebilir;

Amaç$_1$: Deney grubunun şifre güçlerinin ve alışkanlıklarının tespit edilmesi

Amaç$_2$: Şifre öneri sisteminin tanıtılması

Çalışmada öncelikle farklı şifre çalışmalarına ilişkin literatür taraması verilecektir. Bunun ardından, birinci çalışma amacına istinaden bireylerin şifre tercihlerine ilişkin istatistiksel analiz sonuçları verilecek ve ikinci amaca istinaden şifre öneri sistemi tanıtılacaktır.

TEORİK ÇERÇEVE VE LİTERATÜR TARAMASI

Kullanıcılar tarafından oluşturulan şifrelerin daha güvenli bir yapıda olması konusunda tavsiye ve uyarı niteliğinde çok sayıda akademik yazın ve tavsiye niteliğinde makaleler mevcuttur. Örneğin, Microsoft güçlü bir şifre oluşturmak için önerilerini aşağıdaki gibi sıralamıştır(Tips for creating a strong password, 2016):

- En az sekiz karakter uzunluğunda olmalıdır.
- Şifreniz kullanıcı adınız, gerçek adınız veya şirket adınız gibi adları içermemelidir.
- Tam bir kelimeyi içermemelidir.
- Diğer şifrelerinizden anlamlı düzeyde farklı olmalıdır
- Büyük harf, küçük harf, sayı ve özel karakter olmak üzere 4 kategoriden de karakter içermelidir.

US-CERT (United States Computer Emergency Readiness Team, 2013), şifre seçimi ve güvenliği konusundaki tavsiyeleri aşağıdaki gibi sıralanmıştır:

- Kolay ulaşılabilir ya da tahmin edilebilir kişisel bilgilerinizi şifre olarak kullanmayınız.
- Herhangi bir dilin sözlüğünde bulunan bir kelimeyi şifre olarak kullanmayınız.
- Karmaşık şifreleri hatırlamak için bir hatırlatıcı geliştiriniz.
- Hem büyük hem küçük karakter kullanınız.
- Şifrenizi hem özel karakter hem de sayılardan oluşturunuz.
- Mümkünse şifre hatırlatıcı kullanınız.
- Farklı sistemlerde farklı şifreler kullanınız.

Tari vd. (2006) bir şifre için akılda kalıcı olması, en fazla 1 yıllığına kullanılması, herhangi bir yere yazılmaması gibi özelliklere dikkat çekmişlerdir. Ancak aynı çalışmada bu tip özelliklere dikkat ederek şifre oluşturmanın aynı zamanda kullanıcılar için uygulama esnasında zorluklar doğurduğu ve üretkenliği düşürdüğünü belirtmişlerdir.

Özellikle e-ticaretin gelişimi ile şifre ile korunan sitelerin sayısı da artmıştır. Forrester Research araştırması, aktif bir web kullanıcısının günde ortalama 15 adet şifre gerektiren bir alanı kullandığını belirtmektedir. Bununla beraber Adam ve Sasse (1999)'a göre kullanıcılar ancak 4 ya da 5 şifreyi etkin olarak kullanmaktadırlar (Ives vd., 2004). Bu durumdan aynı şifrenin farklı platformlarda kullanıldığı sonucu çıkarılabilir. Bir hesap için kullanılan bir şifrenin, başka hesaplarda da kullanılmasının güvenlik yönünden olumsuz sonuçlar doğuracağı açıktır. Ives vd. (2004) bu duruma şifre yeniden kullanımının domino etkisi ifadesiyle dikkat çekmişlerdir. Araştırmacılar iki farklı hesapta aynı şifre kullanıldığı takdirde, hesaplardan biri yüksek güvenlikli diğeri düşük güvenlikli ise yüksek güvenilirlikli hesabın da düşük güvenlikli hesap kadar risk altında olduğunu belirtmişlerdir. Kullanıcılar kolay hatırlamak için uzun ve karmaşık şifreler yerine kısa şifreleri tercih etmektedirler. Kullanıcıların genellikle kısa ve hatırlanabilir şifreler kullandıkları, Adams ve Sasse (1999), Schneier (2006) gibi çalışmalarda gösterilmiştir.

Microsoft şifre hatırlama konusunda verdiği önerilerde, şifrenin kişi için bir anlam ifade eden bir yapıda olması gerektiğini belirtmektedir. Verdikleri örnekte oğlu 12 Aralık 2004 doğumlu olan bir kişinin "My son's birthday is 12 December, 2004" ifadesini "Msbi12/Dec,4" veya "Mi$un's Brthd8iz 12124" biçimlerine dönüştürerek şifre biçiminde kullanılabileceğini, sevdiği spor badminton olan bir kişinin "I love to play badminton" ifadesini "ILuv2PlayB@dm1nt()n" olarak şifre biçimine dönüştürebileceğini belirtmişlerdir.

Uzun ve kompleks şifreler oluşturmanın güvenliği arttırdığının biliniyor olmasına rağmen kullanıcılar tarafından genellikle kullanılmama nedenlerinden biri; kullanıcıların internet üzerinde herhangi bir olumsuz sonuçla karşılaşmayacaklarına olan inançlarıdır. Kullanıcıların bu konudaki iyimserliklerini, Campbell vd. (2007) çalışmalarında ele almışlardır. Ayrıca, kişinin önem vermediği bir hesapta kullandığı şifrenin de güvenlik olarak düşük olan bir şifre olabileceği yorumu yapılabilir.

Bireylerin kullandıkları şifrelerin yapısına yönelik çok sayıda çalışma literatürde yer almış ve yer almaya devam etmektedir. Bu kapsamdaki ilk çalışmalardan biri Morris ve Thompson (1979) tarafından yapılan 3289 şifrenin yapısının analiz edildiği çalışmadır. Araştırmacılar şifrelerin %86'sının kısa şifrelerden ve karakter grupları karmaşık olmayan şifrelerden oluştuğunu tespit etmişlerdir. Riddle vd. (1989) yaptıkları çalışmada katılımcıların %88'inin şifrelerinin 4 veya daha az karakterden oluştuğunu ve bu şifrelerin %44'ünün de bir İngilizce kelimeye denk geldiği ve tahmin etmesi kolay olduğunu belirtmişlerdir. Brown vd. (2004)'nin 218 öğrencinin şifreleri üzerinde yaptığı araştırmaya göre; katılımcıların şifre karakter uzunlukları ortalaması 4,45 olarak bulunmuştur. Schneier (2006), 34,000 adet MySpace sitesine ait kullanıcı adı ve şifresi üzerine yaptığı araştırmada, kullanıcıların %65'nin 8 ya da daha az karakterden oluşan şifrelere sahip olduklarını tespit etmişlerdir. Riley (2006)'in 315 kişilik örneklem üzerinde yaptığı çalışmaya göre ise katılımcıların %85,7'sinin şifrelerinin yalnızca

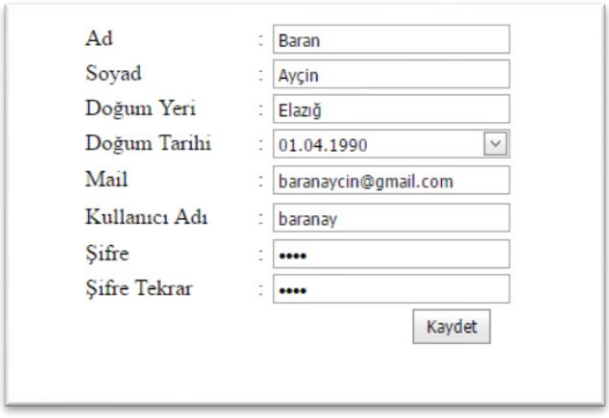
küçük harften oluştuğu belirlenmiştir. Liu, Hong, Pi (2014)'nin Çinli internet kullanıcıları üzerinde yaptıkları çalışmada, kullanıcıların dört farklı sitedeki şifre bilgilerini toplamışlardır. Buna göre kullanıcıların ortalama şifre uzunluklarının 4 site için 7,74 ile 9,45 arasında değiştiği, ayrıca dört sitede de kullanıcılardan şifrelerini yalnızca sayıdan oluşturanların diğer şifre kombinasyonları ile şifre belirleyenlerden daha fazla oldukları tespit edilmiştir. Doğan (2015), çalışmasında bir e ticaret sitesinin kullanıcılarına ait 9997 adet şifreyi incelemiş, şifrelerin ortalama uzunluğunu 7,1 olarak tespit etmiştir. Ayrıca şifrelerin %53'lük kısmının yalnızca bir kategoriden oluşan şifreler olduğu ortaya konmuştur.

Literatürde kullanıcılara daha güvenli şifreler kullandırmayı amaçlayan şifre önerilerinin yer aldığı çalışmalara da sıklıkla rastlanmaktadır. Kuo, Romanosky ve Cranor (2006) çalışmalarında; kullanıcıların şifrelerini hatırlamaları için bazı karakterleri değiştirerek oluşturulan şifrelerin daha güvenilir olduğunu göstermişlerdir. Yan, Blackwell ve Anderson (2004) çalışmaları da benzer biçimde kullanıcının hatırlaması temeline dayalı şifre öneri modelinin incelendiği bir çalışmadır. Leonhard ve Venkatakrishnan (2007) çalışmaları ise bilgisayar tarafından kullanıcı için şifre oluşturmaya yarayan üç farklı şifre oluşturma modelini ortaya koymuşlar ve her bir modelden türetilen şifreleri analiz etmişlerdir. Forget vd. (2008) ise çalışmalarında kullanıcı şifre girdikten sonra girilen şifrenin güvenliğini arttırmak için şifrenin rastgele bir yerine, yine rastgele seçilen bir karakterin yerleştirilmesi esasına dayanan bir yapı önermişlerdir. Sotirakopoulos (2011) çalışması ise kullanıcı şifre girmeden önce kullanıcının şifresinin güvenlik derecesini gösteren yapıların aksine kullanıcının şifresinin diğer kullanıcıların ne kadarından daha güvenli ya da güvensiz olduğunu belirten bir uyarı sistemini önermiştir. Bu sayede kullanıcıların daha güvenli şifreleri tercih ettiklerini ortaya koymuştur.

BİREYSEL ŞİFRE TERCİHLERİNİN DEĞERLENDİRİLMESİ

Araştırma örneklemi, Dokuz Eylül Üniversitesi İzmir Meslek Yüksekokulu İktisadi ve İdari Programlar bölümlerinde öğrenim gören ve okulun bilgisayarın laboratuvarında dersi olan öğrencilerden oluşmaktadır. Veri toplanması için belirlenen günlerde laboratuvarda bulunan öğrencilere, okulun öğrencilerin notların görmeleri konusunda yeni bir sistem üzerinde çalıştığı bilgisi verilerek, o anki sınıfın bu çalışma için pilot sınıf olarak seçildiği söylenmiştir[1]. Çalışmada 176 öğrenciden veri toplanmıştır. Öğrencilerden pilot uygulama yapılacak olan yeni not sistem için isim, soy isim, doğum tarihi, yaş, kullanıcı adı ve şifre bilgilerini girmeleri istenmiştir. Bu bilgiler bir form vasıtasıyla kullanıcıdan talep edilir (Şekil 1).

Şekil 1. Kullanıcı Bilgi Formu



Kullanıcılara belirleyecekleri şifreler konusunda başlangıçta herhangi bir uzunluk ya da karakter kısıtlaması getirilmemiştir. Kullanıcı 8 karakter uzunluğundan ve 3 kategori çeşidinden az şifre girmiş ise şifrenin güvenli olmadığı, aksi halde güvenli olduğu yönünde sınıflanmasına

[1] Öğrencilerden daha güvenilir sonuçlar almak için böyle bir yol izlenmiştir.

karar verilmiştir. Şifresi güvenli olan kullanıcıların formu kaydedildi uyarısı ile kapanır. Güvensiz bulunan kullanıcılar yeni bir forma yönlendirilir. Bu form farklı özelliklerde 5 farklı şifre seçeneği sunar. Kullanıcı dilerse bu 5 seçenekten birini seçebilir ya da yeni bir şifre belirleyebilir. Sistemin belirlediği seçeneklerden birisini seçerse sistem bu şifreyi kaydeder. Ancak kullanıcı yeni bir şifre belirlerse bu şifre tekrar aynı kontrol mekanizmasından geçirilir. Eğer güvenli bulunursa kaydedilir. Bulunmaması durumunda sistem bu sefer sadece 5 seçenek sunarak kullanıcının bu seçeneklerden birisini seçmesi için zorlar. Yapılan bu yönlendirmeler sırasında kullanıcıya şifrenin neden güvensiz olduğuna dair bir bilgi verilmez. Bunun nedeni ise kullanıcının alışkanlıklarını anlayabilmektir. Sistem tüm bu süreci ve yapılan işlemleri kaydeder. Bu şekilde kullanıcının tüm ilerlemesi ve şifre tercihleri anlaşılabilir.

Kullanıcılar için oluşturulan şifre önerilerinin oluşturulma mantığı aşağıdaki gibidir;

Öneri 1:

- Kullanıcının adının veya soyadının baş harfi (B veya A)
- Doğum yerinin plaka numarası (23)
- Bir tane karakter (!,*,-,+)
- Doğum tarihi (1990)
- Örnek : **A23!1990**

Öneri 2:

- Şifre kullanıcının adının veya soyadının harflerini alır. (BARAN veya AYCIN)
- İlk ve son harflerini büyük, diğer harfleri küçük hale getirir. (BaraN veya Aycin)
- Oluşturulan kelime ile doğum tarihini sıralı şekilde yerleştirir.
- Örnek: **B1a9r9a0N**

Öneri 3:

- Bir karakter seçilir. (!,*,-,+)
- Doğum tarihinin ay veya günü seçilir. (01 veya 04)
- Kullanıcı adının yarısı alınır. İkiye bölünmüyorsa bir fazlası alınır. (BARA)
- Doğrum tarihindeki ay veya günden başta seçilmeyen alınır. (01 veya 04)
- Kullanıcı adının kalan kısmı alınır. Küçük harfe çevrilir. (nay)
- Örnek: **!04BARA01nay**

Öneri 4:

- Doğum tarihi iki ayrılır ve birinci kısmı alınır.(19)
- Ad veya soyad alınır. Sesli harfleri silinir. İlk ve son harfi büyük diğerleri küçük hale getirilir.
- Doğum tarihinin ikinci kısmı eklenir.(90)
- Bir tane karakter eklenir. (!,*,-,+)
- Örnek: **19YcN90+**

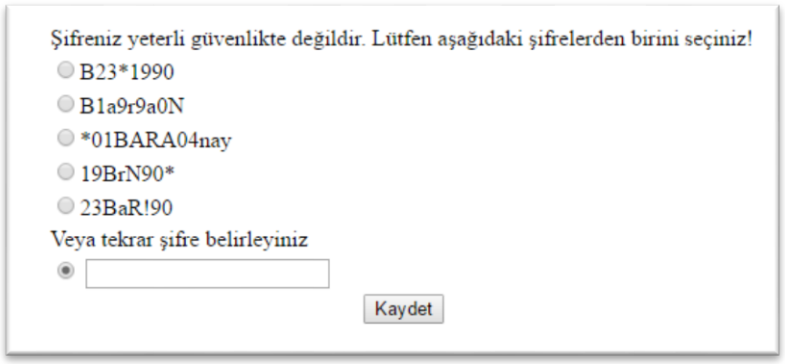
Öneri 5:

- Doğum yerinin plaka kodu alınır. (23)
- İsmin ilk üç harfi alınır. İlk ve son harfleri büyük diğer harfleri küçük hale getirilir. (Bar)
- Bir karakter alınır. (!,*,-,+)
- Doğum tarihinin son iki hanesi alınır.(90)
- Örnek: **23Bar*90**

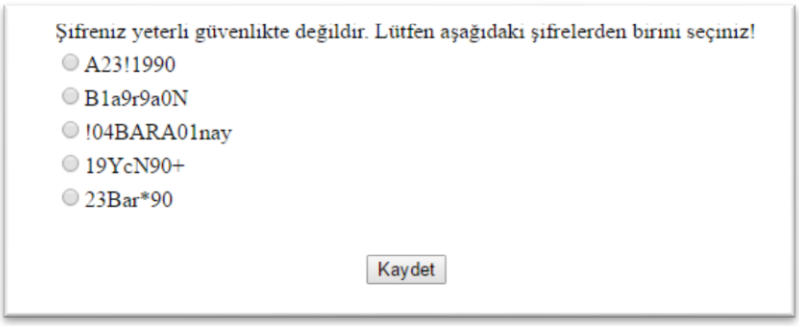
Şifre öneri oluşturulurken, şifrelerin en az sekiz haneli olması gerekliliğinden dolayı, sistem sekiz haneden küçük olan şifrelerin başlarına ve sonlarına rasgele karakterler eklemektedir.

Şekil 3 ve Şekil 4' de iki aşamalı öneri sisteminin ekran görüntülerini göstermektedir.

Şekil 3. Birinci Aşama Şifre Tercihi



Şekil 4. İkinci Aşama Şifre Tercihi



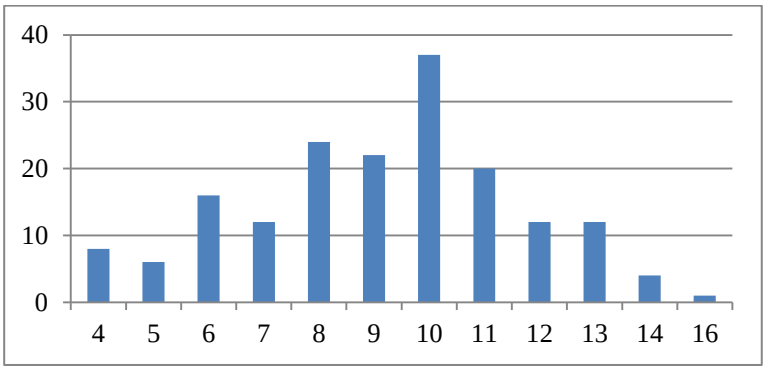
Kullanıcılar tarafından girilen ilk şifrelere ilişkin bazı istatistikler Tablo 1.'de gösterildiği gibidir.

Tablo 1. İlk Şifre Girişlerine Ait İstatistikler

Kullanıcı Sayısı	176
Şifre Uzunluk Ortalaması	9,20
Şifre Karmaşıklık Durumu 1 2 3 4	 76 (%43) 72 (%41) 28 (%16) 0
İlk Girişte Kabul Edilen Şifre Sayısı	28 (%16)

Çalışmada 176 kişiden şifre bilgisi toplanmıştır. Elde edilen şifrelerin uzunlukları 4 karakter ile 16 karakter arasında değişmekte olup şifre uzunluk ortalaması 9,20 olarak tespit edilmiştir. Şifrelerin karakter uzunluklarına dair grafik Şekil 4'te gösterilmiştir.

Şekil 4. Şifrelerin Karakter Uzunlukları



Yalnızca 1 karakter grubu içeren şifrelerin yapılarına ilişkin istatistikler Tablo 2'de gösterildiği gibidir.

Tablo 2. Yalnızca Bir Karakter İçeren Şifrelerin İstatistikleri

Karakter Grubu	N
Sayı	58
Küçük Harf	18
Büyük Harf	0
Özel Karakter	0

Şifresini yalnızca bir karakter grubundan oluşturan kullanıcıların 58 tanesi sayı ile 18 tanesi ise küçük harf kullanarak şifrelerini oluşturmuşlardır. Şifrelerini büyük harf veya özel karakter ile oluşturan kullanıcı bulunmamaktadır. Şifrelerini yalnızca sayı kullanarak oluşturan kullanıcıların şifre yapılarına ilişkin ek istatistikler Tablo 3' te gösterildiği gibidir.

Tablo 3. Kullanıcıların Şifre Yapılarına İlişkin İstatistikler

Sayı	
Telefon numarası	8
Kimlik Numarası	6
Favori Takıma İlişkin	4
Doğum Tarihi Varyasyonları	10
Ardışık Sayılar	8
Okul Numarası	4
Diğer	18

Ayrıca şifrelerini yalnızca harf ile oluşturan kullanıcıların şifrelerinin büyük çoğunluğu isim, soy isim, lakap, favori takım veya ünlü isimlerinin varyasyonlarından oluşmaktadır.

Şifrelerini iki karakter grubundan oluşturan kullanıcıların şifre yapılarına ilişkin istatistikler Tablo 4 'te gösterildiği gibidir.

Tablo 4. İki Karakter Grubundan Oluşturulan Şifre İstatistikleri

Şifre Kombinasyonu	N
Küçük Harf ve Sayı	54
Küçük Harf ve Büyük Harf	0
Sayı ve Büyük Harf	4
Sayı ve Özel Karakter	10
Büyük Harf ve Özel Karakter	0
Küçük Harf ve Özel Karakter	4

İki karakter grubu ile şifre oluşturan kullanıcılar arasından küçük harf ve sayı ile oluşturan kişiler genellikle şifrelerini isim, soy isim ile kendileri için bir anlam ifade eden sayıları (Doğum tarihi, favori takım kuruluş tarihi, vb.) birleştirerek oluşturdukları tespit edilmiştir. Sayı ve özel karakter ile şifre oluşturan kişilerin ise genellikle doğum tarihini şifre olarak kullandıkları sonucuna ulaşılmıştır.

Üç karakter grubu ile şifre oluşturanlar için de isim, soy isim ve anlam ifade eden bir sayı grubu kombinasyonu sıklıkla yer almaktadır. Bu kombinasyon ile şifre oluşturan

kullanıcılar örneğin ismin baş harfini büyük yazarak veya şifrenin sonuna bir özel karakter ekleyerek şifre karmaşıklık düzeyini üç kategoriye çıkarmışlardır.

Önceki kısımda belirtildiği gibi 3 karakter grubundan ve 8 karakter uzunluğundan az olan şifreler sistem tarafından kabul edilmemekte ve kullanıcı için şifre önerileri ekrana gelmekte veya yeni şifre belirlenmesi istenmektedir. Tablo 5 bu aşamadan sonra oluşan şifrelere ilişkin istatistikleri içermektedir.

Tablo 5. İkinci Aşamadaki Şifre İstatistikleri

Kullanıcı Sayısı	176
Şifre Uzunluk Ortalaması	10,90
Şifre Karmaşıklık Durumu	
1	0
2	32 (%19)
3	144(%81)
4	0
İkinci Aşamada Kabul Edilen Şifre Sayısı	144 (%81)

İkinci aşamada şifreleri tarafımızca belirlenen güvenlik koşullarını sağlayan 144 kişidir. Bu 144 kişiden 28 kişi daha önce belirtildiği gibi ilk oluşturduğu şifreleri kabul edilen kullanıcılar olup, 96 kişi şifre öneri sisteminin sunduğu şifrelerden birini tercih etmiş, 20 kişi ise kendileri oluşturdukları şifreler ile koşulu sağlamışlardır.

İkinci aşama sonrası kalan 32 kişi kendileri yeni şifre oluşturmayıp, şifre öneri sistemi üzerinden önerilen şifreleri tercih etmek durumunda kalmışlardır. Son durumda ortalama şifre uzunluğu 11,30 olarak bulunmuştur.

SONUÇLAR ve TARTIŞMA

Kişiler elektronik postaları, sosyal ağ sitesi hesapları, kurum hesapları gibi çok sayıda hesaba ulaşmanın yanı sıra kredi kartı ile alışveriş, internete erişim, bilgisayar, telefon gibi teknolojik aletlere erişim gibi sayısız farklı şekilde kişisel şifrelerini kullanmaktadırlar. Bireylerin şifrelerini kullandıkları tüm mecraların güvenliğinin önemli olduğu açıktır. Bu nedenle bu hesaplar için belirlenen şifrelerin, (kötü amaçlı kişilerin verebileceği zararlardan ötürü) mümkün olduğunca tahmin edilmesi ya da çeşitli teknolojik yöntemlerle kırılması zor olmalıdır.

Bu çalışmada ilgili örneklemin şifre yapıları belirlenmiş ve şifrelerin daha güvenilir hale gelmesi için oluşturulan şifre öneri sistemi ortaya konulmuştur.

Çalışmada incelenen şifrelerin ortalama uzunluk değerleri 9,20 olarak bulunmuş olup bu değer, incelenen bazı çalışmalarda (Morris ve Thompson, 1979; Riddle vd. 1989; Brown vd. 2004; Schneier, 2006; Doğan, 2015) bulunan ortalama değerlerden fazla, Liu, Hong, Pi (2014) çalışmalarında bulunan ortalama değere ise yakındır. Her ne kadar şifrelerin uzunluk değerleri tatmin edici olmaya yakın olsa da, oluşturulan şifrelerin genellikle; isim, soy isim, doğum tarihi, favori takım kuruluş tarihi, vb. birleştirilerek oluşturulmuş olması şifrelerin güvenliklerinin düşük olduğunu göstermektedir. Öyle ki çalışmadaki en uzun şifre 16 karakterden oluşmakta olup, şifre kimlik numarası ve ismin yazılması ile oluşturulmuştur. Bunun yanında bir şifrenin güvenliğini arttırıcı bir diğer unsur olan şifre karakterlerinin mümkün olduğunca farklı karakter grupları (büyük harf, küçük harf, sayı, özel karakter) ile oluşturulması konusunda örneklemden elde edilen şifreler başarısız kalmıştır. İlk aşamada oluşturulan şifrelerin %84'ü bir veya iki karakter grubundan oluşmaktadır.

Kullanıcılar kendi belirledikleri şifrelerde kendilerince anlamlı sayı ve kelime gruplarını kullandıkları gibi sistemce önerilen şifrelerde de bu tip basit şifrelere yöneldiği gözlenmiştir.

Şifre öneri sisteminin önerdiği şifreler ile kullanıcı şifreleri daha güvenli bir hale getirilmiştir. Ancak, görece güvenli şifrelerin dezavantajlı unsurlarından biri de hatırlanma

sorunudur. Şifre öneri sistemi vasıtasıyla kullanıcılara sunulan şifrelerin bir başka sefer sisteme giriş kullanılması konusunda hatırlanma oranları araştırılmaya açık bir konudur.

Çalışma olanakların kısıtlılığı nedeniyle 176 kişiden veri toplanabilmiştir. Örneklemdeki kişi sayısının arttırılması ile şifre yapıları ile ilgili daha doğru bilgiler edinmemiz sağlanabilir. Ayrıca çalışmada öğrencilere notlarını görecekleri yeni bir sistem için şifre girmeleri istenmiştir. Söz gelimi kredi kartı, banka hesabı, vb. maddi bir kayıpla sonuçlanma ihtimali olan sitelerde seçtikleri şifrelerin daha güvenilir olup olmadığı da araştırmaya açık alanlar arasındadır. Belirtildiği gibi örneklem belirli bir öğrenci grubunu içermektedir. Farklı bölümlerden öğrencilerin veya daha geniş bir yaş grubunun araştırmaya katılması ile Türkiye'de yaşayan kişilerin şifre davranışları, seçimleri üzerine daha kapsamlı bilgilere sahip olunabilir.

Bazı kısıtlar ve araştırılmaya açık alanlarla beraber bu çalışmanın, şifre yapıları ve daha güvenli kişisel şifrelere sahip olma konusunda katkı yapan bir çalışma olduğu ifade edilebilir.

KAYNAKÇA

Adams, A. ve Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 41-46.

Brown, A.S., Bracken, E., Zoccoli, S. ve Douglas, K. (2004). Generating and Remembering Passwords. *Applied Cognitive Psychology*, 18, 641-651.

Campbell, J., Greenauer, N., Macaluso, K. ve Christian E. (2007). Unrealistic optimism in Internet events. Computers in Human Behavior 23: 1273–1284.

Doğan, O. (2015), Bir E ticaret Sitesi Kullanıcı Hesaplarında Şifre Yapılarının Birliktelik Kuralları ile İncelenilmesi, İnternet Uygulamaları ve Yönetimi Dergisi, 6(2), 49-61

Forget A., Chiasson, S., Oorschot, P.C.V. ve Biddle R. (2008). Improving Text Passwords Through Persuasion, *Symposium on Usable Privacy and Security (SOUPS)* 2008, July 23–25, Pittsburgh, PA USA

Ives B., Walsh, K. R. ve Schneider, H. (2004). "The domino effect of password reuse," Commun. ACM, vol. 47, no. 4, pp. 75–78.

Kuo, C., Romanosky, S., ve Cranor, L.F. (2006). Human Selection of Mnemonic Phrase based Passwords. ACM SOUPS, 67-78.

Leonhard, M.D. ve Venkatakrishnan, V.N. (2007). A Comparative Study of Three Random Password Generators. IEEE EIT 227-232.

Liu, Z., Hong, Y. ve Pi, D. (2014). A Large-Scalestudy of Web Password Habits of Chinese Network Users. *Journal of Software*, 9(2), 293-297.

Microsoft (2015). "Tips for creating a strong password", http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password (Erişim Tarihi: 23.02.2016)

Morris, R. ve Thompson, K. (1979). Password Security: A Case History. *Communications of the ACM*, 22(11), 594-597.

Riddle, B. L., Miron, M. S. & Semo, J. A. (1989). Passwords in Use in A University Time Sharing Environment. *Computer Security*, 8(7), 569-578.

Riley, S. (2006). "Password Security: What Users Know and What They Actually Do". http://psychology.wichita.edu/surl/usabilitynews/81/pdf/Usability%20News%2081%20-%20Riley.pdf (Erişim Tarihi: 11.03.2016)

Schneier, B. (2006). "MySpace Passwords Aren't So Dumb". http://archive.wired.com/politics/security/commentary/securitymatters/2006/12/72300?currentPage=all (Erişim tarihi: 12.03.2016)

Sotirakopoulos, A. (2011) Influencing User Password Choice Through Peer Pressure, Master of Science in THE FACULTY OF GRADUATE STUDIES (Electrical and Computer Engineering) The University Of British Columbia Vancouver.

Tari, F., Ozok, A., ve Holden, S. (2006). A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In: Proceedings of SOUPS 2006 Symposium on Usable Privacy and Security,56–66.

US-CERT (2013). Choosing and Protecting Passwords, https://www.us-cert.gov/ncas/tips/ST04-002 (Erişim tarihi: 12.01.2016)

Yan, J., Blackwell, A., Anderson, R., ve Grant, A. (2004). Password Memorability and Security: Empirical Results. IEEE Security & Privacy Magazine 2, 5, 25-31.