RESİM ŞİFRE TEKNİKLERİ:
DENEYSEL KARŞILAŞTIRMA VE SAHA ÇALIŞMASI

MUHAMMED RAŞİT YILDIZ

YÜKSEK LİSANS TEZİ
ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AĞUSTOS 2010
ANKARA

Fen Bilimleri Enstitü onayı

_____

Prof. Dr. Ünver KAYNAK

Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

_____

Doç. Dr. Kahraman Güçlü KÖPRÜLÜ

Anabilim Dalı Başkanı

Muhammed Raşit YILDIZ tarafından hazırlanan RESİM ŞİFRE TEKNİKLERİ: DENEYSEL KARŞILAŞTIRMA VE SAHA ÇALIŞMASI adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

_____

Doç. Dr. Kemal BIÇAKCI

Tez Danışmanı

Tez Jüri Üyeleri

Başkan : Doç. Dr. Kemal BIÇAKCI _____

Üye : Doç. Dr. Bülent TAVLI _____

Üye : Yrd. Doç. Dr. Tolga GİRİCİ _____

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

(İmza)

(Adı Soyadı)

Muhammed Raşit YILDIZ

Üniversitesi : **TOBB Ekonomi ve Teknoloji Üniversitesi**
Enstitüsü : **Fen Bilimleri**
Anabilim Dalı : **Elektrik ve Elektronik Mühendisliği**
Tez Danışmanı : **Doç. Dr. Kemal BIÇAKCI**
Tez Türü ve Tarihi : **Yüksek Lisans – Ağustos 2010**

Muhammed Raşit YILDIZ

RESİM ŞİFRE TEKNİKLERİ: DENEYSEL KARŞILAŞTIRMA VE SAHA ÇALIŞMASI

ÖZET

Bilgi güvenliğinde kimlik doğrulamak amacıyla en yaygın kullanılan teknik hatırlamaya dayalı şifre (parola) teknikleridir. Kullanıcılar şifrelerinin kolay hatırlanabilir olmasını isterler fakat bu tercih başkaları tarafından kolay tahmin edilebilir şifrelerin seçilmesine sebep olmaktadır. Söz konusu bu kullanışlılık/güvenlik açmazının çözümü için önerilmiş yöntemlerden birisi insanların resim hafızasının daha güçlü olmasından hareketle ortaya atılmış resim-şifre teknikleridir.

Bu tez çalışmasında literatürdeki tanıma tabanlı resim şifre tekniklerinin kullanışlılık ve güvenliğini karşılaştırma amacıyla yürütmüş olduğumuz deneysel çalışmanın sonuçları tartışılmaktadır. Ayrıca resim-şifre teknikleri ile tasarlanmış bir şifre yönetici programının kullanımı ile ilgili bir saha çalışması yürütülmüştür. Çalışmamızda bu saha çalışmasının sonuçları da paylaşılmaktadır.

Anahtar Kelimeler: Resim Şifre, Kimlik Doğrulama, Kullanılabilirlik, Saha Çalışması

University : **TOBB Economics and Technology University**
Institute : **Institute of Natural and Applied Sciences**
Science Programme : **Electrical and Electronics Engineering**
Supervisor : **Associate Professor Dr. Kemal Bıçakcı**
Degree Awarded and Date : **M.Sc. – August 2010**

Muhammed Raşit YILDIZ

GRAPHICAL PASSWORD:
EXPERIMENTAL COMPARING AND FIELD STUDY

ABSTRACT

The most common computer security authentication is recall-based authentication. Users want passwords to be easy to remember, however this preference causes that selected passwords can be easily guessed by others. To address this problem, some researchers have developed authentication methods that use pictures as passwords, because of the human ability to accurately recognize and recall images.

In this thesis, we discussed our study results to compare the usability and security of recognition-based graphical password techniques. Moreover, we conducted field study of graphical password application to examine usability. The results of field study will be shared.

Keywords: Graphical Password, Authentication, Usability, Field Study

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren hocam Doç. Dr. Kemal BIÇAKCI' ya teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

ÇİZELGERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

1.GİRİŞ

1.1. Giriş ve Çalışmanın Amacı

Bilgisayar güvenlik sistemlerinde, güvenlik uzmanları, en zayıf halkanın insan olduğunu söylerler [1]. Buna karşın, güvenli bir sistem tasarımında, insan davranışlarını saf dışı bırakmak sistemin çökmesini neden olur. Geliştirilen sistemler ne kadar iyi olursa olsun; yine de insanlar tarafından kimlik doğrulanmasını gerektirir ve bu kimlik doğrulaması, kullanışlı ve güvenli olmalıdır [2]. Kimlik doğrulama metotlarını; işaretçi tabanlı, biyometrik tabanlı ve bilgiye dayalı kimlik doğrulamalar olarak üçe ayırabiliriz.

İşaretçi tabanlı kimlik doğrulama tekniklerine örnek olarak, banka kartlarını ve akıllı kartları verebiliriz. İşaretçi tabanlı kimlik doğrulamalar, güvenliği arttırmak için bilgiye dayalı kimlik doğrulamayı da kullanırlar. Aynen banka kartlarının çalışması için şifre gereksinimi olduğu gibi.

Biyometrik tabanlı kimlik doğrulamalar için yüz tanıma, parmak izi tanıma ve iris tanımayı örnek verebiliriz. Biyometrik tabanlı kimlik doğrulamalar, bilgiye dayalı kimlik doğrulamalara alternatif olarak kullanılmaya başlanmıştır [3]. Ancak biyometrik tabanlı kimlik doğrulamaların pahalı olmaları, yavaş çalışmaları ve kendilerine özgü güvenlik sorunları olması [4], kullanım alanlarında sınır getirmiştir.

Bilgiye dayalı kimlik doğrulamalar en yaygın kullanılan tekniklerdir ve temel olarak ikiye ayrılır:

- Metin tabanlı
- Resim (Grafik) tabanlı

Metin tabanlı kimlik doğrulama, bilgiye dayalı kimlik doğrulamanın en çok bilinen ve kullanılan tekniğidir. Bu tekniğin zayıf noktası herkes tarafından çok iyi bilinir. Metin tabanlı tekniklerde, en büyük problem hatırlama olduğundan genellikle

kullanıcılar, başkaları tarafından kolay tahmin edilebilen şifreler ya da kısa şifreler seçerler [5]. Daha güvenli olan şifreler (başkaları tarafından tahmin edilmeleri zor ve uzun) hatırlaması zor olur. Bu durumda kullanışlılık ve güvenliğin aynı anda yükseltilemediğini, biri için diğerinden vazgeçildiğini gösterir.

Resim şifre tabanlı kimlik doğrulamalar, metin tabanlı kimlik doğrulamalara göre daha hatırlanabilir ve de diğerine göre daha güvenlidir. Hatırlanabilir ve güvenilebilir olması, insan beyninin resimleri seçme, algılama ve tanıma yeteneğinin daha fazla olmasından kaynaklıdır [6,7]. Resim tabanlı kimlik doğrulamayı, tanıma tabanlı ve hatırlama tabanlı olarak ikiye ayırabiliriz. Tanıma tabanlı teknikte kullanıcılar, şifre belirleme esnasında var olan resimler içerisinden bir resmi ve ya noktayı tanır ve tanımlarlar. Hatırlama tabanlı teknikte ise kullanıcılar, şifre belirleme esnasında kendilerinin oluşturduğu ya da seçtiği bir resmi hatırlarlar. Bölüm 1.2'de örneklerle açıklanacaktır.

Kimlik doğrulamada kullanılışlığı ve güvenliği arttırmak için, kısıtlı kullanım alanlarına sahip ve pahalı olan biyometrik tabanlı kimlik doğrulamaların yerine, daha ucuz ve daha çok kullanım alanına sahip bilgiye dayalı kimlik doğrulamanın geliştirilmesi daha uygundur. Metin tabanlı kimlik doğrulamalarda yapılan bazı geliştirmeler (passphrases [8] ve ya mnemonic [9]) kullanılabilirlik ve güvenebilirliğe istenilen katkıyı sağlamamıştır. Resim şifre tekniği, son yıllarda hatırlanabilirliği geliştirilebilir olmasından dolayı önerilen bir tekniktir [10,11].

Biz bu tezde, geliştirilen ikon tabanlı resim şifre uygulamasının [12,13] kimlik doğrulamadaki kolaylıklarını ve zorluklarını, yapacağımız laboratuar ve saha çalışmalarıyla inceleyeceğiz.

1.2. Resim Şifre ve Sınıflandırılması

Uzun yıllar boyunca psikoloji uzmanları, insan beyninin görsel nesneleri tanımaları ve hatırlamaları üzerine çalışmalar yapmışlardır. Resimlerin karakterlerden daha

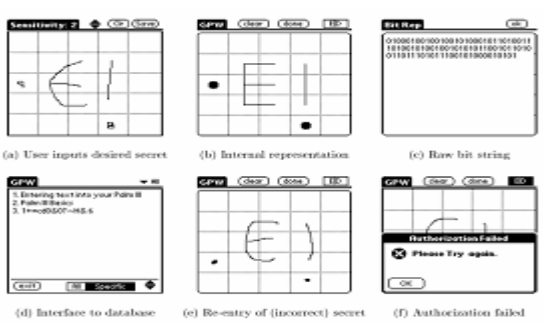
rahat hatırlanır olduğunu söylemişlerdir [6,7]. Bu sebepten insan için resim şifreler ile daha kullanışlı ve güvenli (daha uzun ve karmaşık) şifreler oluşturulabilir.

Resim şifreler, şifre hatırlama için gerekli bilişsel faaliyetler bakımından üç temel sınıfa ayrılabilir [14,15]. Bunlar, hatırlama (recall), tanıma (recognition) ve ipucuyla hatırlama (cued- recall) dır. Bu bölümde her birine birer örnek vererek açıklanacaktır. Resim şifreler için yayınlanmış anketler mevcuttur [10,11] ve bu anketlerde bugüne kadar mevcut bütün resim şifre uygulamalarının detaylı olarak kullanabilirlik ve güvenlik çizelgeleri verilmiştir.

1.2.1. Hatırlama (Recall) Tabanlı Teknik

Bu teknik de, genel olarak giriş bölümünde de bahsettiğimiz gibi kullanıcının sistemden hiçbir yardım ve ipucu almadan şifrelerini hatırlaması ve üretmesi gerekir. Bu yönüyle metin tabanlı şifrelere benzerler ve zor bir hafıza görevidir [16].

Kullanıcıların iki boyutlu bir kareli alan üzerinde fare ile basit bir resim çizmesini isteyen Draw_A-Secret (DAS) [17] bu tekniğe bir örnektir. Şekil 1.1'de bu uygulamayı görebilirsiniz. Kullanıcı, kimlik doğrulama esnasında; şifre oluştururken çizimini yaptığı karelerin sırası ile aynı sırada çizimi gerçekleştirir ise, sisteme girmiş olduğu şifre doğrulanmış olur. Kullanıcıların, bu teknikte şifre hatırlama oranları çok düşük çıkmıştır [17]. Yinede metin tabanlı sistemlere bir alternatiftir. Passdoodle [18] ve Pass-Go [19] diğer hatırlama tabanlı uygulamalardır.

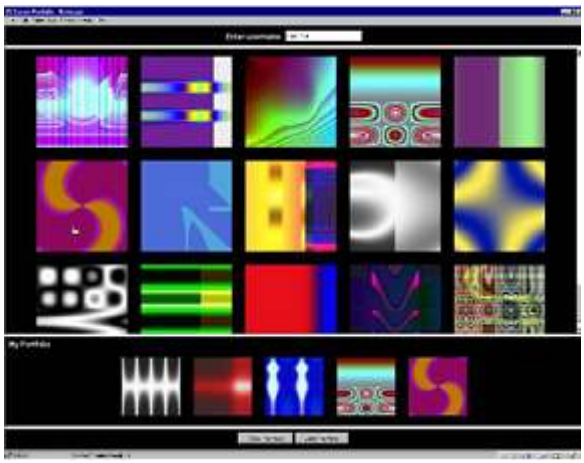


Şekil 1.1. Draw-A-Secret [17]

1.2.2. Tanıma (Recognation) Tabanlı Teknik

Hatırlama ile tanıma tekniklerinin, hafızaya geri çağrımlarda aralarında benzer teknikler olup olmadıkları ile ilgili birkaç çalışma vardır [20], ama genel kanı tanıma tekniğinin hatırlama tekniğinden daha kolay bir hafıza görevi olduğudur [21]. Tanıma tekniğinde genel olarak kullanıcılar, şifre oluşturma esnasında onlara verilen bir grup resim içerisinden bazılarını seçerler ve hafızaya alırlar. Kimlik doğrulama esnasında ise seçtikleri resimleri tanımaları ve hatırlamaları gerekmektedir.

Şekil 1.2'de gösterilen Déja Vu [22] ismindeki uygulama tanıma tekniğine bir örnektir. Bu uygulamada kullanıcılar, kendilerine verilen büyük bir grup resim içerisinden belli sayıdaki resimleri seçerek şifrelerini oluştururlar. Kullanıcılar, kimlik doğrulanması için bu seçtikleri resimleri, yine kendilerine verilen büyük bir grup resim içerisinden seçmelidir. Çalışmayı yapan araştırmacılar, kimlik doğrulama sırasında metin tabanlı uygulama ile Déja Vu yu karşılaştırdıklarında, kendi tekniklerinin % 90, metin tekniğinin ise % 70 başarılı olduğunu belirtmişlerdir [22]. Ancak şifre giriş sürelerinde metin tabanlı tekniklere göre daha yavaştırlar [22]. Yinede metin tabanlı şifrelerin yerine kullanılabilecek bir uygulamadır.



Şekil 1.2. Déja Vu Resim Şifre Uygulaması [22]

En çok bilinen ve günümüzde ticari amaçlı olarak kullanılan Passface [14,23,24] bir diğer tanıma tabanlı tekniktir ve Şekil 1.3'de gösterilmektedir. Bu uygulama 2.

bölüm de ikonlu resim şifre uygulaması ile karşılaştırması yapılmıştır. Passface uygulamasında da kullanıcılar, Déja Vu da olduğu gibi resimler seçmektedirler. Seçilen resimler, insan yüzleridir. Bu resimler veri bankasından seçilir ve şifreyi oluşturur. Şifre seçme ve hatırlama işlemi sırasında, 4 tur aynı işlemlerin yapılması gerekmekte ve şifreler 9 adet resimden oluşmaktadır. Her turda, farklı paneller oluşmakta ve bu panellerde kullanıcıların, kendi şifrelerini oluşturmaları ve kimlik doğrulanmasında hatırlamaları istenmektedir. Çalışmayı yapanlar, bu sistemi insan yüzlerinin diğer resimlerden daha rahat hatırlandığı varsayımı üzerine yapmışlardır. Bu uygulama için yapılan deneylerde, şifre hatırlama oranı metin tabanlı uygulamaya göre çok daha yüksek olmasına rağmen; şifre giriş süreleri tam tersi çıkmıştır [25,26]. Bu sebepten dolayı kullanıcıların, Passface kullanma istekleri çok azalmıştır.

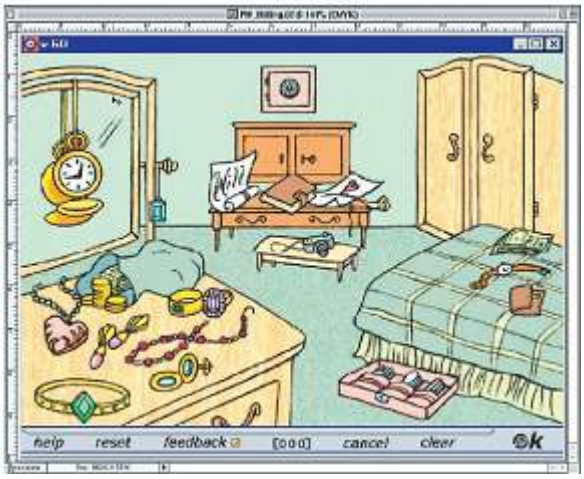
Şekil 1.3. Passface Uygulaması İçin Bir Örnek [23]

Story [14], Weinshall [27], Jansen (mobil uygulamalar için) [28] gibi uygulamaları diğer tanıma tabanlı resim şifre tekniklerine örnek olarak verebiliriz.

1.2.3. İpucuyla Hatırlama (Cued-recall) Tabanlı Teknik

Bu sistemde, kullanıcının, şifresini hatırlamasını sağlamak amacı ile sistem bazı ipuçları verir ve böylece hafıza yükü azaltılmaya çalışılır. Bu ipucu sadece kullanıcıya yardım etmek içindir. Bu teknikte, hatırlama (recall), tekniğinden farklı olarak, kullanıcıların, resmin tamamını değil sadece resimler içerisinden belirli bir alanı hatırlaması istenmektedir.

Blonder [29]; kullanıcıların, bir resim içerisinden belirli yerleri tıklayarak şifre oluşturabilecekleri bir resim şifre uygulaması geliştirdi. Kimlik doğrulamada esnasında, seçilen yerlere yakın alanların da tıklanması kabul ediliyordu. Blonder, ayrıca tıklama tabanlı resim şifreyi ilk geliştirendir. Ancak bu çalışma ile ilgili her hangi bir sonuç açıklamamıştır. Bu teknik üzerine geliştirilen Passlogix [30] de kullanıcılar, resim üzerinde çeşitli nesneleri tıklayarak şifre oluşturur ve kimlik doğrulama da aynı sırada bu nesneleri tıklanmaları ile olur. (Şekil 1.4)



Şekil 1.4. Passlogix İçin Bir Örnek [11,31]

Şekil 1.5'de gösterilen PassPoints [32–34], Blonder uygulamasının geliştirilmiş şeklidir. Kullanıcılar, şifre oluşturma esnasında, verilen resim içinden sıralı şekilde 5 tıklama noktası seçerler. Kimlik doğrulamada ise, şifrelerini aynı sırada aynı noktalara tıklayarak yaparlar. Tıklanan noktaların, tamamen aynı nokta olması gerekmez, bir tolerans içerisinde tıklanmak istenen noktanın etrafı olabilir. Yapılan çalışmalarda, kullanıcıların; şifre oluşturma sırasında 64 saniye, öğrenmede 171 saniye ve şifre doğrulamada ise 9 ile 19 saniye süre kullandıklarını gösterir. Kimlik doğrulama başarısı ise % 55–90 olarak veriliyor [33,34].

Şekil 1.5. PassPoint Tekniğinde Kullanılan Bir Resim [32]

1.3. İkonlar İle Resim Şifre (GPI)

1.2 bölümünde anlattığımız gibi resim şifre tekniklerindeki kullanılabilirlik ve güvenlik yönünden iyileştirme yapabilmek amacı ile ikonlar ile resim şifre geliştirildi [12,13] . Bölüm 2 ve 3'de detaylı bir şekilde hem uygulama anlatılacak hem de kimlik doğrulama için laboratuar ve saha çalışmalarının sonuçları gösterilecektir. Bu teknik, Şekil 1.6'da gösterilmiştir. Uygulamada şifre, kullanıcılar tarafından seçilebilir ya da kullanıcılar sistemden şifre ürettirebilir. İkinci durum, çok fazla talep edilen, ikonların seçimini elimine edebilir. İkonlar, kategorilere ayrıldığı için hatırlanmalarında önemli bir artış olacağını düşünmekteyiz. Bu uygulamada şifre alanı 2^{43}'dür.

Şekil 1.6. İkonlar İle Resim Şifreleme

2. PASSFACES VE GPI KARŞILAŞTIRMALARI İÇİN LABORATUAR ÇALIŞMASI

Bazı resim şifre çalışmaları resimleri tanıma ve ya bunları sırayla geri hatırlamayı dayanır. Çoğunlukla ise tanımaya dayanır. Bunun en çok bilineni ise Passface [24] dır. Bu uygulama, resim şifre uygulamalarının nasıl çalıştığını tipik olarak gösterir. GPI (İkonlar ile Resim Şifre Uygulaması) ise bu uygulamadan daha yeni geliştirilen bir uygulamadır. Bu yüzden GPI tabanlı resim şifre uygulamasını, Passface ile kullanabilirlik üzerine karşılaştırmak istedik.

2.1. Yöntem

Çalışma öncesi, bütün katılımcıların eşit şartlara maruz kalması için bir oda hazırlandı. Her iki uygulamada, bir diz üstü bilgisayarına yüklendi. Seçilen katılımcılara, çalışma öncesi gönüllü katılım formu imzalatıldı. Katılımcılara istedikleri her an çalışmadan ayrılabilecekleri söylendi.

Çalışma iki aşama olarak planlandı. 1. aşama, şifre öğrenme ve hatırlama; 2.aşama ise şifre hatırlama şeklindedir. Bu iki aşama arasına 15 günlük bir süre aralığı konmuştur. Her katılımcı, çalışmalarını arka arkaya uygulamaları kullanarak tamamlamıştır. Katılımcıların uygulamaları kullanma sırası, bir önceki katılımcının tersi şeklinde olmuştur (önceki kullanıcı ikon-yüz olarak çalışmasını tamamlamış ise sonraki kullanıcı yüz-ikon şeklide çalışma yapmıştır) ve her iki sırada çalışma yapanların eşit sayıda olmasına dikkat edilmiştir. 15 gün sonra hatırlama evresinde, katılımcılara ilk aşamadaki sıra ile çalışma yaptırılmıştır.

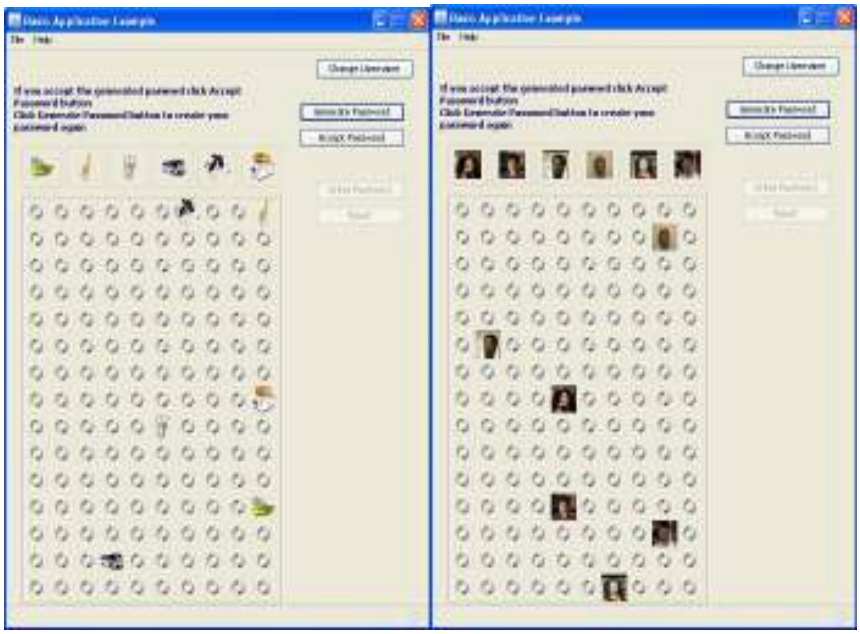
Çalışma öncesi katılımcılara uygulamaların nasıl çalıştığını anlatan bir yazılı doküman verilmiş ve okumaları istenmiştir. Çalışma sonrasında ise katılımcıların görüş ve yorumlarını almak için bir anket yapılmış ve veriler toplanmıştır.

2.2. Amaç

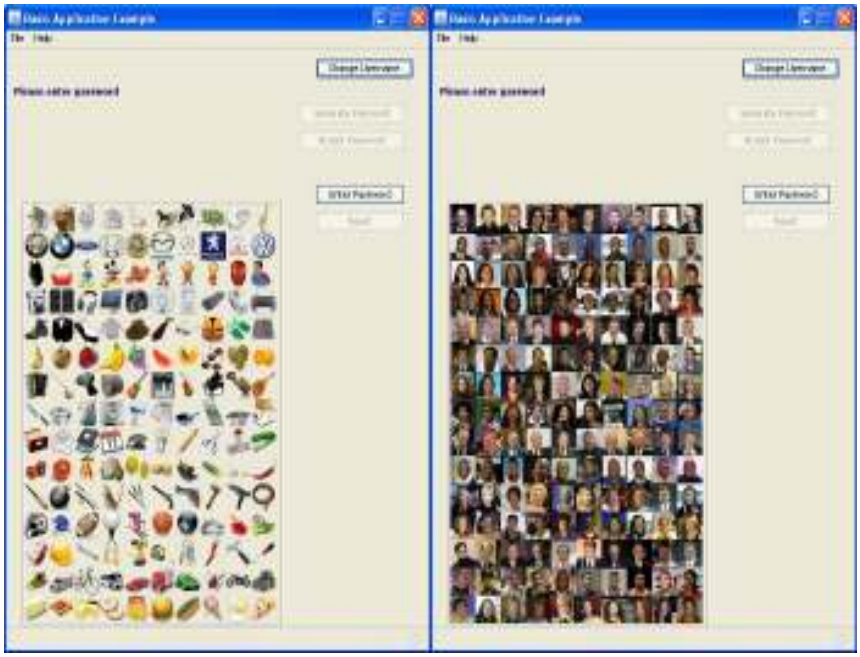
GPI uygulamasının kuvvetli ve zayıf yönlerini anlamak için ilk önce laboratuar çalışması yapılması planlandı. Bu çalışmada katılımcıların, 6 adet ikon ve yüzden oluşan bir şifreyi öğrenmeleri ve hatırlamaları beklendi. Katılımcıların temel olarak yapmaları amaçlanan işlemler:

- Şifre Oluşturma: Bu aşamada kullanıcıların kullanıcı isimlerini girmeleri ve sistemden bir 6 haneli şifre ürettirmeleri ve kabul etmeleri (Şekil 2.1 ve Şekil 2.2).
- Şifre Öğrenme: Bu aşamada, kabul edilen şifrenin akabinde gelen pencerede şifrelerini öğrenerek doğru sırada girmeleri (Şekil 2.2 ve Şekil 2.3).
- Şifre hatırlama: Öğrenilen şifrenin hem birinci hem de ikinci aşamada doğru sırada doğru olarak hatırlamaları (Şekil 2.3).

Şekil 2.1. Kullanıcı İsmin Girilmesi



Şekil 2.2. Şifre Üretilmesi ve Öğrenmesi



Şekil 2.3. Şifre Hatırlanması

Birinci aşamada, katılımcıların şifre öğrenmeleri, hatırlamaları ve ikon-yüz tıklama süreleri; ikinci aşmada ise şifre hatırlamaları ve yine ikon-yüz tıklama süreleri ölçülmüştür.

2.3. Katılımcılar

Katılımcılar, Orta Doğu teknik Üniversitesinden 21 (13 kadın, 8 erkek) kişi olarak seçilmiştir. Bu katılımcıların 11'i doktora, 10'u yüksek lisans öğrencisidir ve bağlı oldukları fakültelerde araştırma görevlisi olarak çalışmaktadırlar. Yaş ortalamaları 29,1'dir. Katılımcıların hiç biri daha önce resim şifre ile ilgili bir çalışmaya katılmamıştır.

2.4. Sonuçlar

Burada kullanıcıların, öğrenme ve hatırlama durumlarındaki başarı oranlarını ve sürelerini vereceğiz. Hiçbir şekilde kullanıcıların isimleri verilmeyecektir.

2.4.1. Şifre Öğrenme

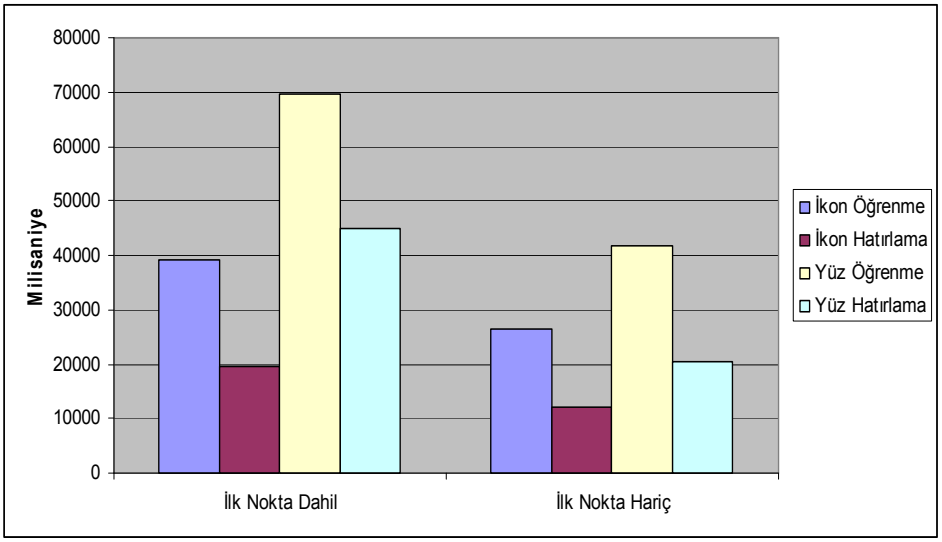
Kullanıcıların, 10'u yüz-ikon, 11'i ikon-yüz sırasıyla uygulamalar ile çalışmışlardır. Kullanıcılar, ikon için ortalama 1,3 kez; yüz için ise ortalama 1,6 kez deneme yapmışlardır. İkon uygulamasında 8, yüz uygulamasında ise 11 olmak üzere toplamda 19 yanlış giriş yapılmıştır. Bununla birlikte ikon uygulamasında, şifre öğrenme süresi ortalama 39,1 saniye olur iken yüz uygulamasında ortamla 69,7 saniyedir. Çizelge 2.1'de bahsedilen öğrenme zamanları ve deneme sayılarını verilmektedir. Yapılan bu denemeler sonucunda katılımcılar, şifrelerini öğrenmişlerdir. Burada beklenen, ikon uygulamasında deneme sayısı bakımından yüz uygulamasına göre daha iyi çıkması idi ancak bu gelişmedi. Burada göze çarpan durumsa şifre giriş sürelerinde ikonun daha iyi olmasıdır.

Çizelge 2.1. Şifre Öğrenme Denemeleri ve Zamanları

	İKON	**YÜZ**
Deneme Sayısı (Ortalama)	1,3	1,6
Yanlış Giriş	8	11
Süre (saniye)	39,1	69,7

2.4.2. Şifre Hatırlama

Çalışmanın birinci aşamasında yer alan hatırlamada aşamasında, kullanıcıların tamamı şifrelerini başarıyla hatırlamışlardır. Bu aşamada ki şifre giriş süreleri öğrenme aşamasına göre önemli ölçüde azalmıştır (Şekil 2.4). Birinci aşamada, öğrenme ve hatırlama seansları arasında 10 dakikalık bir fark vardır.



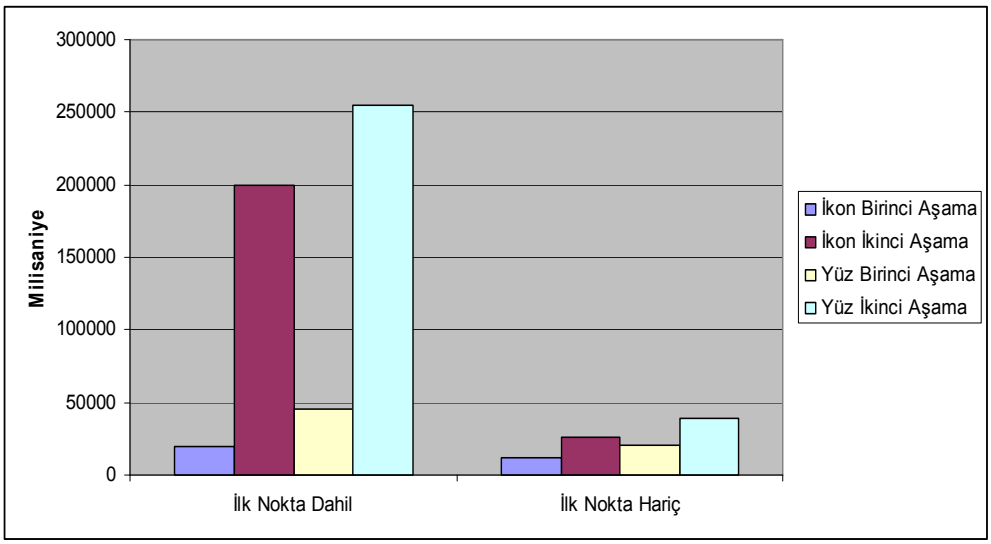
Şekil 2.4. Birinci Aşama Öğrenme ve Hatırlama Süreleri

15 gün sonra yapılan ikinci aşamada (bu aşama sadece hatırlama işlemi vardır), Çizelge 2.2'de gösterildiği gibi deneme sayıları birbirine yakındır ve beklenildiği gibi birinci aşamadan fazladır. Burada beklenilmeyen durum, hatırlama oranlarının düşük ve bir birlerine yakın çıkmasıydı. İkon uygulamasında hatırlama yüzdesinin daha iyi olması bekleniyordu. Her iki uygulamada şifresini hatırlayanların oranı % 28,5'dir.

Çizelge 2.2. Şifre Hatırlama Denemeleri ve Oranları

	İKON	**YÜZ**
Deneme Sayısı (Ortalama)	4,8	5,9
Hatırlama Oranı %	52,4	42,8

Şekil 2.5'de birinci ve ikinci aşamadaki hatırlama süreleri görülüyor. Burada ilk noktaların dahil edildiği durumda ikinci aşamada süreler aşırı yüksek çıkmıştır. Bunun nedeni, iki aşama arasında verilen süreden kaynaklanıyor. Burada kullanıcılar verilen arada hiç bir şekilde uygulamaları incelememişlerdir. Yine her iki durumda da ikon uygulamasındaki şifre giriş süresi, yüz uygulamasına göre daha iyidir.



Şekil 2.5. Birinci ve İkinci Aşamalarda Şifre Hatırlama Süreleri

2.5. Katılımcıların Görüşleri ve Yorumları

Çalışmaya ilk önce yüz uygulaması ile başlayan katılımcıların % 50'si, çalışma sonundaki hatırlama oranlardaki azlığın nedenini yüz uygulamasına fazla yoğunlaşmalarına ve bu yüzden ikon uygulamasına fazla dikkat edemediklerine bağladılar. Katılımcılar şifrelerini hatırlarken ikonlar arasında bir ilişki kurmaya çalışmadıklarını ya da yüzlerin tipik özelliklerini kullanmadıklarını, daha çok yer olarak hafızaya almaya çalıştıklarını söylediler. Çizelge 2.3'de çalışma sonunda sorulan sorular ve kullanıcıların sayısı görülmektedir. Katılımcıların % 85'i, ikon ve yüz uygulamalarının şifre üretmekte ve kullanımda güvenli olduğu görüşünde. Katılımcıların uygulamaların güvenli olduğuna inanmasına rağmen % 47,6'lık kısım uygulamalardan hiçbirini ilerde kullanmayı düşünmediklerini ilettiler. Yine kullanıcıların % 33,3'lük oranı ikon uygulamasını kullanabileceklerini söylüyorlar.

Bunda en büyük payın, ikon uygulamasının şifre oluşturma ve hatırlama kolaylığı yönünden yüz uygulamasına göre daha iyi olduğu görüşüdür.

Çizelge 2.3. Katılımcıların Çalışma Sonundaki Görüşleri

SORULAR	KULLANICI
Kullanılan programlardan (GPI ve Passface) hangisi ile şifrenizin güvende olduğunu düşünüyorsunuz?	
GPI	3 (%14,3)
Passface	7 (%33,3)
İkisi de	8 (%38)
Hiçbiri	3 (%14,3)
Hangi programı kullanırken şifrenizi hatırlamakta zorlandınız?	
GPI	7 (%33,3)
Passface	9 (%42,8)
İkisi de	3 (%14,3)
Hiçbiri	2 (%9,5)
Hangi uygulamada tıklama sayısı 6'dan az olsa şifreyi hatırlamak kolaylaşır?	
GPI	5 (%23,8)
Passface	8 (%38)
İkisi de	5 (%23,8)
Hiçbiri	3 (%14,3)
Hangi programın kullanım ve şifre oluşturma konusunda kolay bir uygulama olduğunu düşünüyorsunuz?	
GPI	13 (%61,9)
Passface	2 (%9,5)
İkisi de	1 (%4,7)
Hiçbiri	5 (%23,8)
Hangi programın daha güvenli olduğunu düşünüyorsunuz?	
GPI	2 (%9,5)
Passface	6 (%28,5)
İkisi de	11 (%52,4)
Hiçbiri	2 (%9,5)
İleride hangi programı kullanmak istersiniz?	
GPI	7 (%33,3)
Passface	3 (%14,3)
İkisi de	1 (%4,7)
Hiçbiri	10 (%47,6)

3. GRAFİK ŞİFRENİN İNTERNET TARAYICI EKLENTİSİ OLARAK SAHA ÇALIŞMASI

Saha çalışmaları günlük yaşam şartlarında kullanılabilirlik ve güvenlik açısından daha doğru bilgiyi verir. Çünkü bu tür çalışmalarda daha fazla zaman ve çaba harcanır ve de daha fazla veri toplanır. Kullanıcıların davranışlarıyla, şifre programının güvenliği ve kullanılabilirliği artırılabilir.

3.1. Yöntem

Günlük yaşam şartlarında kullanılabilirlik ve güvenliği incelemek ve zayıflıklarını anlamak için resim şifre programını internet tarayıcı eklentisi (GPEX) haline getirerek uzun dönem saha çalışması yapılması planlandı. Ayrıca eklenti ile kullanıcıların bu yeni programa alışmaları ve çabuk ulaşmaları sağlandı.

GPEX firefox eklentisi olarak tasarlandı. Kullanıcıların rahat bir şekilde eklentiyi her an ve her yerde kullanılabilmeleri için taşınabilir firefox 2 Gb.'lık usb bellekler içine yüklenerek dağıtıldı. Başarılı bir şekilde çalışmayı bitirenlere bu usb bellekler ödül olarak verileceği katılımcılara bildirildi. Çalışma öncesi bütün kullanıcılara gönüllü katılım formu imzalatıldı. Bu çalışmanın süresi 45 gün (1,5 ay) olarak belirlendi. Kullanıcıların, bu süre içerisinde istenilen herhangi bir zamanda çalışmadan ayrılabilecekleri kendilerine belirtildi.

Çalışmaya başlamadan önce her katılımcıya internet kullanımı ve şifre oluşturma alışkanlıkları ile ilgili bir anket yapıldı ve eklentinin nasıl çalıştığı hakkında 3 dakikalık bir video izletildi (bu video deney sorumlusu tarafından hazırlanmıştır). İlk şifre oluşturma işlemi deney sorumlusu gözetiminde yapıldı. Çalışma süresince katılımcılara, karşılaştıkları her türlü sorunda deney sorumlusu ile irtibata geçebilecekleri bildirildi ancak deney sorumlusu bu süre zarfında katılımcılardan bir istek gelmediği müddetçe katılımcıyla irtibat kurmadı. Bunun nedeni kullanıcıların,

uygulamayı kendi standartlarına göre kullanmasını sağlamak içindir. Çalışma sonrası ise kullandıkları eklenti hakkında görüşlerini ve yorumlarını almak için ikinci bir anket yapıldı ve verilerin hepsi toplandı.

3.2. Amaç

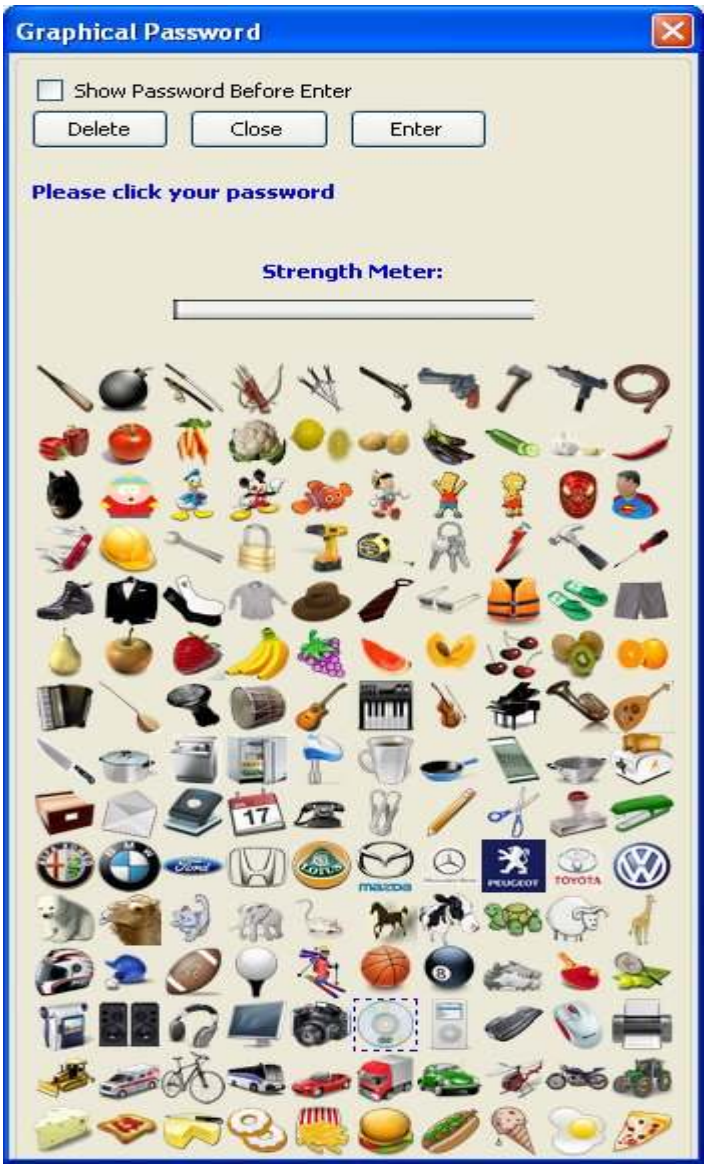
Bu saha çalışmasında katılımcılardan, geliştirilen resim şifre eklentisinin 45 gün boyunca düzenli bir şekilde kullanılması beklendi. Katılımcılardan çalışma sırasında 3 den az olmamak üzere istedikleri kadar şifre gerektiren internet sitelerine giriş yapmalarını istendi. Katılımcılar 2 ayrı gruba ayrıldı. 1. grubun, eklentinin şifre önerme butonunu kullanması zorunlu tutuldu. 2. grubun ise kendi şifresini oluşturulması istendi. Katılımcılar seçtikleri sitelerde bir adet 6 ikondan oluşan ana şifre kullanılması istendi. Böylece resim şifre eklentisinde ikon tıklama süreleri ölçülecek, hangi ikonların seçildiği ve kullanıcıların hatırlama oranları incelenecektir. Çalışmanın sonunda ortaya çıkan sonuçlarla resim şifre eklentisinin kullanılabilirliği ve güvenliği ölçülecektir.

3.3. Katılımcılar

Katılımcılar, TOBB Ekonomi ve Teknoloji Üniversitesinden 1 doktora, 12 yüksek lisans ve 7 lisans öğrencisi olmak üzere 20 kişi olarak belirlenmiştir ve kullanıcıların hiçbiri daha önce resim şifre ile ilgili bir deneye katılmamışlardır. Bu kullanıcıların 3’ ü kadın, 17’si erkektir. Yaş ortalamaları 24,5’dir. Çalışmanın başlamasının 25. günü bir kullanıcı usb belleğini kaybettiğini birdirdi. Bu durumda çalışmaya en baştan başlayacağı için çalışmaya devam etmek istemedi. Çalışmanın 35. gününde farklı bir kullanıcı kişisel sorunları yüzünden çalışmaya devam etmek istemediğini birdirdi. İki kullanıcının ayrılmasından sonra yerlerine yeni kullanıcılar bulunmadı ve çalışmaları iptal edildi. 20 olan katılımcı sayısı 18 düşürülerek çalışmaya devam edildi. Çalışmadan ayrılan 2 kullanıcıda erkek idi ve biri lisan diğeri ise yüksek lisans öğrencisiydi.

3.4. Eklenti Tanıtımı (GPEX)

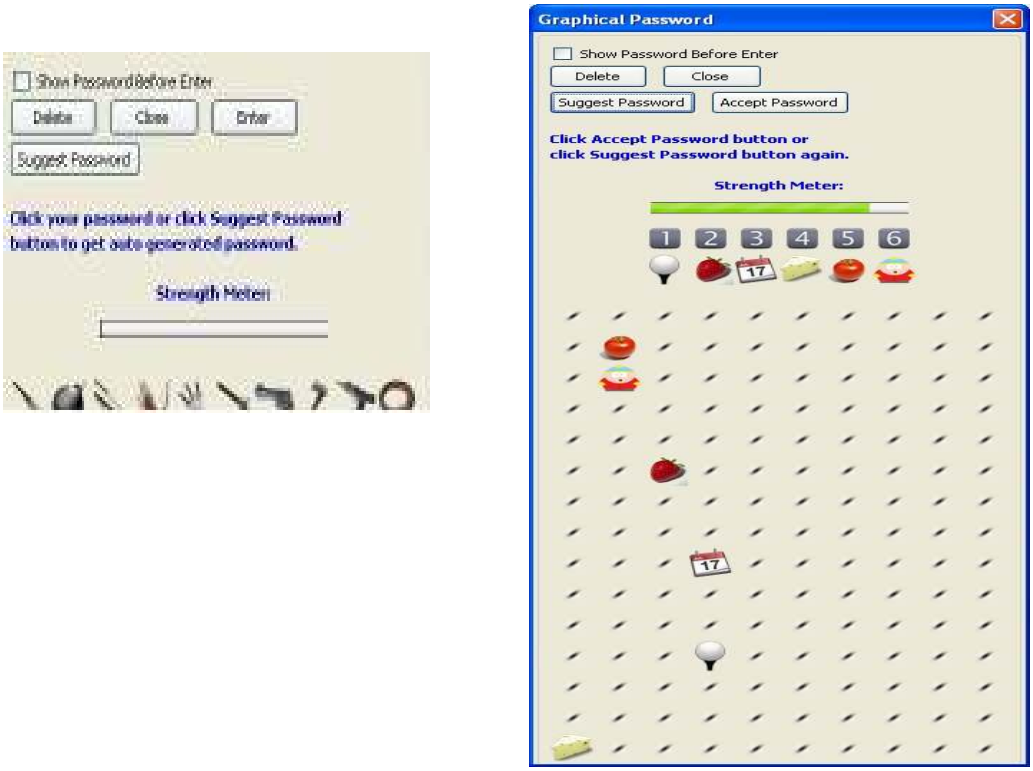
Eklenti 15x10 olarak 150 adet ikondan oluşmaktadır ve her bir satır bir kategoriyi oluşturmaktadır. Kategoriler silahlar, sebzeler, çizgi karakterler, alet edevat, giysiler, meyveler, müzik aletleri, mutfak aletleri, ofis malzemeleri, araba markaları, hayvanlar, spor malzemeleri, elektronik eşyalar, araçlar, hazır yiyecekler olarak ayrılmıştır. GPEX Şekil 3.1'de gösterilmiştir.



Şekil 3.1. GPEX Ara Yüzü

Eklenti, sitenin şifre alanına bilgisayar faresi ile çift tıklanarak açılır. Şekil 3.2 bu şifre alanını gösterir ve açılan eklenti Şekil 3.1 ile aynıdır. Şifre oluşturma esnasında eklenti, öneri butonunu gösterir. Kullanıcı burada kendi setçiği şifreyi girebilir ya da programdan öneri isteyebilir (Şekil 3.3). Belirlenen şifreler fare ile tıklanarak girilir.

Şekil 3.2. Şifre Alanı



Şekil 3.3. Öneri Butonu

Şekil 3.3'de kullanıcı tarafından öneri butonuna basıldığı zaman rastgele üretilen ikonları görebiliriz. Eklenti üzerinde, oluşturulan şifrenin güvenli olup olamadığını bildiren ölçü barı vardır (Şekil 3.4). Bu, şifrenin güvenliğini belirtirken ikonların yan yana, aşağıdan yukarı aynı sırada, çaprazlama vb. gibi olmaları dikkate alınarak kullanıcıya şifrenin güvenli olup olmadığı bildirilir.

Şekil 3.4. Güvenlik Ölçü Barı

Genellikle siteler güvenlik açısından 8 -16 haneli şifre oluşturulmasını isterler. Şifre, sitenin şifre kurallarına uygun uzunlukta ve site kurallarına uygun olarak üretilir. Site kuralları eklenti için önceden tanımlanmamışsa 14 haneli sembol, harf ve rakam içeren şifre üretilir. Aynı ikonlar aynı sırayla tıklansa bile her site için farklı şifre üretilir. Kullanıcı isterse bu üretilen şifreyi görebilir (Şekil 3.5). Eklentide sahip olunan bir ana şifre için her farklı sitede farklı bir şifre üretilmektedir.

Şekil 3.5. Herhangi Bir Site İçin Üretilen Şifre

3.5. Sonuçlar

3.5.1. İnternet ve Şifre Alışkanlıkları

Çalışmaya başlamadan önce katılımcıların internet ve şifre alışkanlıklarını öğrenmek için doldurtmuş olduğumuz anket, Çizelge 3.1'de gösterilmiştir. Katılımcıların 14'ü

(%66,6) bilgisayar bilgileri bakımından kendilerine 5 üzerinden 4 puan veriyorlar. Diğer 3'ü (%16,6) 3 puan ve yine 3'ü (%16,6) 5 puan veriyor.

Çizelge 3.1. Katılımcıların İnternet ve Şifre Alışkanlıkları

SORULAR	KULLANICI
En Sık Kullanılan Web Tarayıcısı	
Internet Explorer	1 (%5,5)
Firefox	14 (%77,7)
Diğer	3 (%16,6)
Bilgisayar Sahibiyim	18 (%100)
İnternet Kullanımı	
Tatiller dahil her gün	16 (%88,9)
Tatiller hariç her gün	2 (%11,1)
Aynı şifreyi birden fazla web sitesi için kullanıyorum	14 (%77,8)
Şifrelerim güvenli	10 (%55,5)
Şifrenin Uzunluğu	
6–7 Karakter	1 (%5,5)
8–9 Karakter	8 (%44,4)
10 Karakterden uzun	9 (%50)
Şifreleri Seçerken Nelere Dikkat Edersiniz?	
Kolay hatırlanmasını	13 (%72,2)
Başkaları tarafından tahmin edilmemesini	14 (%77,8)
Sistem tarafından verilen şifreleri kullanırım	0
Diğer şifrelerimle aynı şifreyi kullanırım	10 (%55,6)
Şifrelerinizi Hangi Karakter Kümesi İçinde Oluşturursunuz?	
Harf ve sayılar (36 karakter)	8 (%44,4)
Büyük ve küçük harfler ve sayılar (64 karakter)	3 (%16,7)
Bütün klavye karakterleri (94 karakter)	7 (%38,9)

Katılımcıların 18'i kendi bilgisayarlarına sahip ve 14'ü internet tarayıcısı olarak firefox kullanıyor. % 77,8'i aynı şifreyi birden fazla sitede kullanıyor. Şifre oluşturmalarda katılımcıların hiçbiri sitemlerin atadığı şifreleri kullanmıyor. Genellikle şifrelerin kolay hatırlanması ve başkaları tarafından hatırlanmaması kullanıcılar tarafından önemsenen konudur. Buna karşılık birden fazla sitede aynı şifreyi kullanma oranı % 55,6'dır.

3.5.2. Kullanılabilirlik

Çalışmanın 1. gününde 6 kişi kullandıkları bir mail sitesinde şifrelerini değiştiremediklerini bildirdi. Bunun sebebinin sitenin şifre oluşturmada bazı karakterleri kabul etmesinden kaynaklandığı anlaşıldı. Eklenti, bir sunucuda tutulan ve her site için şifre politikalarının tanımlanabileceği bir xml dosyasından üreteceği şifrenin özelliklerini belirler. Şifre kabul etmeyen site bu dosyada tanımlanarak siteye uygun şifre üretilmesi sağlandı (Şekil 3.6). Aynı gün 5 kullanıcı kullandıkları bir mail sitesine giremediklerini bildirdi. Bunun sebebinin de girmeye çalıştıkları sitenin otomatik olarak girişe (eklentide şifre girilmesinden sonra giriş butonuna basılınca siteye otomatik olarak girilmesi) izin vermemesinden kaynaklandığı anlaşıldı. Bu durumda eklentinin özelliklerinden otomatik giriş iptal edilerek sorun çözüldü. Çalışma sırasında genellikle en büyük şikâyet programın yavaş çalışması idi. Ancak bu sorun programın yavaş çalıştığından değil taşınabilir firefox kullanımından kaynaklanıyor olmasıydı. Bilgisayarın, usb den okuması yavaşlık nedeniydi. Bu katılımcılara açıklandı ve kabul gördü. Bu iki sorunun dışında kullanımda başka bir sorunla karşılaşılmadı.

Rules

Domain/Subdomain	Minimum Password Length	Maximum Password Length	Symbols	Numeric	Start With Letter	Forbidden Characters
» etu.edu.tr	12	16	Not Allowed	Allowed	Allowed	
» mail.etu.edu.tr	12	16	Not Allowed	Allowed	Allowed	
» google.com	12	16	Allowed	Must	Allowed	
» abc.google.com	12	16	Allowed	Allowed	Allowed	
» kariyer.net	12	16	Not Allowed	Allowed	Allowed	
» mynet.com	12	16	Not Allowed	Allowed	Allowed	
Not in this list	12	16	Allowed	Allowed	Allowed	

Şekil 3.6 Eklenti Site Kural Dosyası

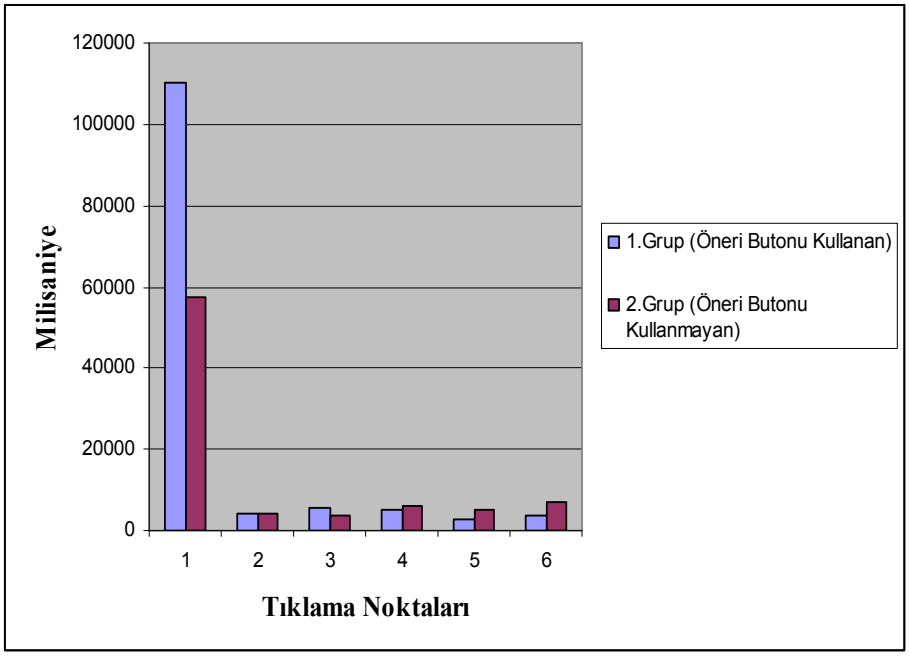
3.5.3. İnternet Sitelerine Giriş Başarı Oranı

Çalışmamız sırasında katılımcılar, 1. grup 988 kez, 2. grup 900 kez olmak üzere toplamda 1888 kez resim şifre eklentisi ile sitelere giriş yapmışlardır. Şifre oluşturma esnasında girişler bu veriye dahil edilmemiştir. Katılımcılar ortalama 3,3 site olmak üzere 22 farklı siteye (google, yahoo, hotmail, etumail, facebook, twitter, myopenid, gittigidiyor, zekirdek, ankarabasket, mybilet, donanımhaber, markofoni, ntvspor, hürriyet, fotokiritik, wikipedia, warnerblade, aol, vatanbilgisayar, ankaramander, zekirdek) giriş yapmıştır. Kullanıcıların hiçbiri sitelere girişleri sırasında şifrelerini yanlış girmemişlerdir.

Katılımcılara çalışmamızın başında şifrelerini bir yere not edebilecekleri iletilmişti ve katılımcıların 14'ü hiçbir şekilde şifrelerini bir kâğıda not etmediklerini, 3 katılımcı şifrelerini kâğıda not aldıklarını ve üç gün sonra bakmayı bıraktıklarını, 1 katılımcı ise not aldığını ancak hiçbir zaman bakmadığını söyledi. Bir kâğıda not alan katılımcıların hepsi 1. gruba (öneri butonunu kullanan) ait kullanıcılardır.

3.5.4. Şifre Giriş Süreleri ve Şifreler

Çalışmanın etkinliğini anlamak için ilk önce katılımcıların şifre oluşturmak için harcadıkları süreleri incelemek gerekir. Genellikle şifre oluşturma süreleri, siteye giriş sürelerinden fazladır. Bunun sebebi şifre oluştururken başlangıçta ikonlara bakıp, hangisine tıklamaya karar vermek zorunda olmalarıdır. 1. grubun şifre oluşturma zamanlarında ilk nokta süreleri, 2. grubun şifre oluşturma zamanlarındaki ilk nokta süresinden çok daha fazladır. Bu da öneri butonun kullanılarak kullanıcını kendisine daha uygun şifre seçmek istemesinden ve seçtikleri şifreyi doğrulama (öğrenme) aşamasının olmasından kaynaklanıyor. 1. gruptaki kullanıcılar her öneri butonuna bastıklarında önce inceliyorlar ve daha sonra şifreyi kabul edip etmemeye karar veriyorlar. Şekil 3.7'de şifre oluşturma süreleri gösterilmektedir. 1. grup ortalama 2,7 kez öneri butonu kullanmıştır.

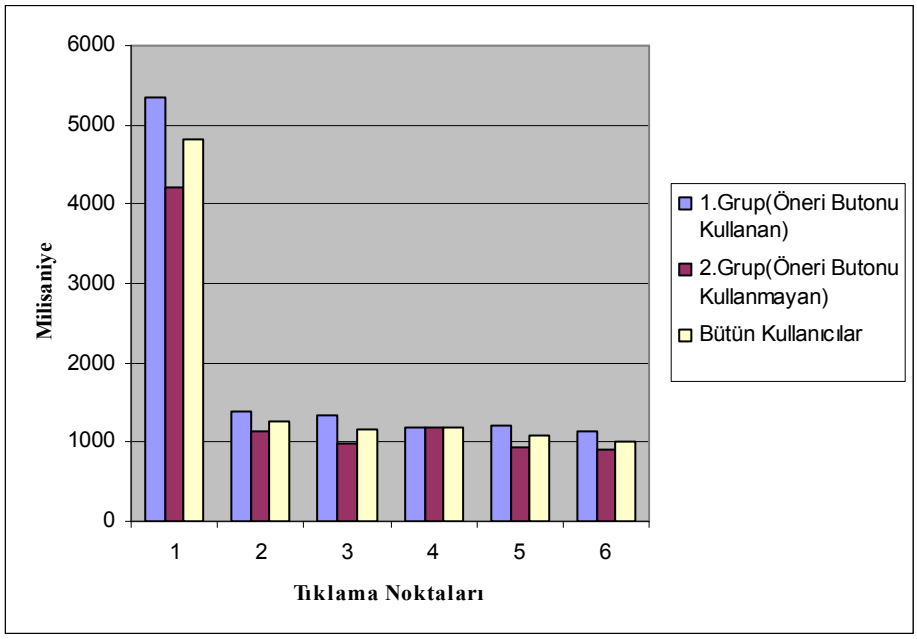


Şekil 3.7. Şifre Oluşturma Süreleri

1. grup ortalama 110,33 saniye ilk nokta tıklama süresi harcamalarına rağmen 2. grup ortalama 57,54 saniye süre harcamışlardır. Bu durumun oluşması beklenen bir durumdur. Diğer noktalarda süreler birbirine yakındır ve 3–6 saniye civarındadır.

Şifre oluşturmadan sonra sürekli olarak internet sitelerine giriş yapmaya başlayan kullanıcıların giriş süreleri Şekil 3.8'de gösterilmiştir. Burada göze çarpan nokta giriş süreleri, şifre oluşturma sürelerine göre çok önemli ölçüde azalma göstermeleridir.

İnternet sitelerine bütün kullanıcılar için giriş süresi ortalama 10,5 saniyedir (1. grupta 11,6saniye, 2.grupta 9,4 saniye). İnternet sitelerine bütün kullanıcılar için ilk nokta giriş süresi 4,8 saniyedir (1. grupta 5,4 saniye, 2.grupta 4,3 saniye). Diğer noktalar 0,9–1,6 saniye arasında değişmektedir. Burada görülen şifre üretirken giriş süreleri ile sonradan giriş süreleri arasındaki fark, şifrelerin daha çok girildikçe sürenin kısalmasıdır. Eklenti kullanıldıkça giriş süreleri daha da hızlanıyor.



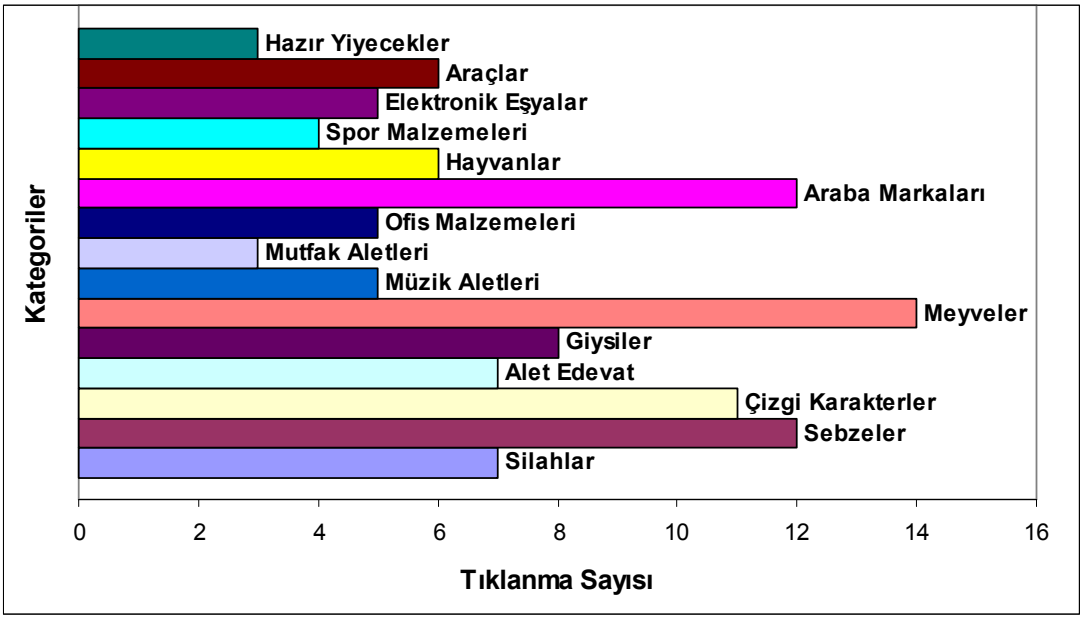
Şekil 3.8. Sitelere Giriş Süreleri

3.5.5 İkon Seçimleri ve Güvenlik

Katılımcılar 2 farklı gruba da ayrılsa şifrelerini belirlerken hangi ikonları beğenirlerse onları seçerler. Burada önemli olan kullanıcıların şifrelerini seçerken hatırlanabilir ve başkaları tarafından kolay tahmin edilemeyen şifreler seçmesidir. Buna duruma da hangi kategorilere ve ikonlara tıklandığına bakarak karar verebiliriz. Şekil 3.9'da kullanıcıların hangi kategorilere ne kadar tıkladığını görebiliriz.

Şekil 3.9'da görüldüğü gibi kategorilerin tıklanması birbirlerine yakın olmuştur. Bu da seçilen kategorilerin doğruluğunu gösterir. Bu verileri daha iyi incelemek için her bir ikonun tıklanma sayısına bakabiliriz. Çizelge 3.2'de bütün ikonların tıklanma sayısı görünmektedir. 1. grubun ve 2. grubun ayrı ayrı tıklama davranışlarını incelersek 2. grubun seçimlerini daha çok eklentinin üst tarafındaki ikonlar yönünde kullandıkları görülüyor. 2. grubun şifre seçimleri daha çok alt alta, bir boşluk bırakarak ya da çaprazlama şeklinde oluşmuştur. Bu da 2. grubun şifrelerinin daha zayıf olduğunu gösteriyor. 1. grubun şifrelerinin çoğunlukla güçlü olmasının nedeni

sistemin genellikle bölüm 3.4'de anlattığımız güvenlik algoritmasına göre şifre üretmesidir. Çizelge 3.3, 1. grubun tıklama davranışını, Çizelge 3.4 ise 2. grubunun tıklama davranışını göstermektedir.



Şekil 3.9. Kategorilerin Tıklanma Sayısı

Çizelge 3.2. Resim Şifre Eklentisindeki Tıklanan İkonların Sayısı

2	2						2	1
1	3	1	1	1		2	1	2
2	2	3	1			1	1	1
1	1	1		2				2
	2			1	1		2	2
2		1	4	2		2	1	2
	1		1			1	1	1
		1				1	1	
			1		1	1	2	
1		1	3		3	3		1
1	1	1					2	1
	1		2			1		
1	1				2	1		
			1		1	1	2	1
					1	1		1

Çizelge 3.3. 1.Grubun (Öneri Butonu Kullanan) Tıklanan İkonların Sayısı

	1								
	1			1		2		1	
2		2	1			1	1		
	1	1							1
					1			2	1
			2			1			1
	1						1		1
		1				1	1		
			1		1	1		1	
1		1	2		3	3			
1		1						1	1
	1		1						
1	1				1	1			
			1		1	1	1	1	
						1			

Çizelge 3.4. 2.Grubun (Öneri Butonu Kullanmayan) Tıklanan İkonların Sayısı

2	1							2	1
1	2	1	1						2
	2	1							1
1				2					1
	2			1					1
2		1	2	2		1	1		1
			1			1			
								1	
			1						1
	1							1	
			1			1			
					1				
							1		
					1				1

3.6. Katılımcıların Görüşleri ve Yorumları

Katılımcıların tamamı resim şifre eklentisinde şifrelerinin güvende olduğunu söylüyor. Buna karşın katılımcıların % 50'si eklentinin kullanması zor bir uygulama olduğu görüşünde. % 77,7 oranındaki katılımcılar şifre hatırlanması kolay bir uygulama olduğunu söyledi ancak yine katılımcıların % 33,3'ü ikonların çok küçük

olduğunu ve bu yüzden hatırlaması zor bir uygulama olduğunu söyledi. İkonların küçük ve çok olması uygulaman kullanılması zor diyen % 50'lik kısmın ana sebebidir. Şifrenin 6 ikondan oluşmasının hatırlamayı zorlaştırdığını katılımcıların % 50'si kabul ediyor. Katılımcıların % 77,7'si şifrelerini hatırlarken kategorilerden yararlandığını söyledi ve katılımcıların tamamı tıklama sayısının gösterilmesinin kullanışlı olduğu görüşünde. Taşınabilir firefox kullanımın deney sırasında faydalı olduğu görüşünde olan kısım % 50'yi buluyor. Diğer kısım ise bunun yavaşlığa neden olduğu görüşünde.

Katılımcıların % 22,2'si eklentiyi kesinlikle kullanacaklarını ilettiler. Katılımcıların % 55,5'i eklentiyi sürekli kullanmakta kararsız olduğunu belirti. Kararsızların % 70'nin kararsızlıkların nedeni uygulamanın yavaş çalışıyor olmasıydı. Eğer bu sorun çözülürse sürekli kullanabileceklerini söylediler. Yine kararsızların % 10'u ise firefox u tarayıcı olarak kullanmadıklarını ama tarayıcı olarak firefox kullanırlarsa eklentiyi sürekli kullanabileceklerini iletiler. Bu da şifre uygulamasının kullanmak isteyenlerin sayısını arttırıyor. Katılımcıların % 22,2'lik kısmı ise kesinlikle uygulamayı kullanmayacaklarını söylediler. Bunun nedeni olarak da fare ile tıklamanın klavyeden girmesinden daha zor olduğunu ve alışkanlıklarını bırakmak istemediklerini belirtmeleriydi. Katılımcıların eklentinin güvenli ve kullanışlı bulmaları bizim istediğimiz bir sonuçtu. Çalışma genel olarak beklentilerimize cevap vermiştir.

4. SONUÇLAR VE TARTIŞMA

Son yıllarda resim şifre teknikleri metin tabanlı tekniklere alternatif olarak kullanılmaya başlamıştır. Bunun ana nedeni ise 1. bölümde bahsettiğimiz gibi, metin tabanlı tekniklerde, kıllanıcılara bağlı olarak, şifrelerde kullanılabilirlik ve güvenliğin aynı anda arttırılamamasıdır. Ayrıca, resimlerin insanlar tarafından daha kolay hatırlanması [6,7] resim şifre tekniklerinin alternatif olma ve gelişmesinin bir başka nedenidir.

Bu tezin 1.2 bölümünde günümüzdeki bazı resim şifre tekniklerinin kullanışlılık ve güvenlik açısından incelenmelerine ve sonuçlarına yer verdik. Bu sonuçlarda şifrelerin, resim şifre tekniklerinde metin tabanlı tekniklere göre daha rahat hatırlandığı, buna karşın şifre giriş süreklerinde bazı uygulamalarda eşit ya da daha uzun olduğu görüldü. Bu sonuçlardan yola çıkarak, kullanabilirliği ve güvenliği biraz daha attırmak için yeni bir resim şifre tekniği geliştirildi [11,12].

Bizim yaptığımız çalışmada, geliştirilen yeni tekniğin 2. bölümde karşılaştırmalı laboratuar çalışmasının ve 3. bölümde ise saha çalışmasının kullanılabilirlik ve güvenlik yönünden incelemeleri ve sonuçları yer alıyor. 2. ve 3. bölümlerde yapılan çalışmaların sonuçlarında kullanıcıların, kimlik doğrulama aşamasında şifrelerini hatırlama oranları yüksek çıkmıştır. Aynı zaman da şifrelerin kimlik doğrulama sırasında giriş süreleri kısa olmuştur. Bunlarla birlikte kullanıcılar, bu programı ileride kullanmak için olumlu görüşler söylemişlerdir.

Bu sonuçlar ile geliştirilen bu yeni tekniğin metin tabanlı tekniklere ve diğer resim şifre tekniklerine iyi bir alternatif olduğunu söyleyebiliriz.

KAYNAKLAR

[1] M. Sasse, S. Brostoff, and D. Weirich. Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3):122–131, July 2001

[2] J. Saltzer and M. Schroeder. The protection of information in computer systems.Proceedings of the IEEE, 63(9):1278–1308, 1975.

[3] K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.

[4] L. Coventry. Usable biometrics. In L. Cranor and S. Garfinkel, editors, Securityand Usability: Designing Secure Systems That People Can Use, chapter 10,pages 175–197. O'Reilly Media, 2005.

[5] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41–46, 1999.

[6] R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156–163, 1967.

[7] B. Kirkpatrick. An experimental study of memory. Psychological Review, 1:602–609, 1894.

[8] M. Keith, B. Shao, and P. Steinbart. The usability of Passphrases for authentication: An empirical field study. International Journal of Human-Computer Studies, 65(1):17–28, 2007.

[9] C. Kuo, S. Romanosky, and L. Cranor. Human selection of Mnemonic Phrase-based Passwords. In 2nd ACM Conference on Symposium on Usable Privacyand Security (SOUPS), July 2006.

[10] F. Monrose and M. Reiter. Graphical passwords. In L. Cranor and S. Garfinkel,editors, Security and Usability: Designing Secure Systems That People Can Use,chapter Chapter 9, pages 157–174. OReilley, 2005.

[11] X. Suo, Y. Zhu, and G. Owen. Graphical passwords: A survey. In Annual Computer Security Applications Conference (ACSAC), December 2005.

[12] K. Bicakci, N. B. Atalay, M. Yuceel, H. Gurbaslar, B. Erdeniz. Towards Usable Solutions to Graphical Password Hotspot Problem. 33rd Annual IEEE International Computer Software and Applications Conference, 2009

[13] K. Bicakci, M. Yuceel, B. Erdeniz, H. Gurbaslar, N. B. Atalay. Graphical Passwords as Browser Extension: Implementation and Usability Study. IFIP Advances in Information and Communication Technology, 2009, Volume 300/2009

[14] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In 13th USENIX Security Symposium, August 2004.

[15] K. Renaud. Evaluating authentication mechanisms. In L. Cranor and S. Garfinkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 6, pages 103–128. O'Reilly Media, 2005.

[16] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle. Multiple password interference in text and click-based graphical passwords. (Manuscript under submission). Technical Report TR-08-20, School of Computer Science,Carleton University, September 2008.

[17] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.
[18] J. Goldberg, J. Hagman, and V. Sazawal. Doodling our way to better uthentication (student poster). In ACM Conference on Human Factors in ComputingSystems (CHI), April 2002.
[19] H. Tao and C. Adams. Pass-Go: A proposal to improve the usability of graphical passwords. International Journal of Network Security, 7(2):273–292, 2008.
[20] J. Anderson and G. Bower. Recognition and retrieval processes in free recall. Psychological Review, 79(2):97–123, March 1972.
[21] W. Kintsch. Models for free recall and recognition. In D. Norman, editor, Models of human memory, chapter Models for free recall and recognition. Academic Press: New York, 1970.
[22] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.
[23] RealUser, "www.realuser.com," last accessed in June 2005.
[24] Brostoff, S. and Sasse, M.A. (2000). Are Passfaces more usable than passwords: A field trial investigation. In McDonald S., et al. (Eds.), People and Computers XIV - Usability or Else, Proceedings of HCI 2000, Springer, pp. 405-424..
[25] T. Valentine. An evaluation of the Passface personal authentic system. Technical report, Goldsmiths College University of London, 1998.
[26] S. Brostoff and M. Sasse. Are Passfaces more usable than passwords? A field trial investigation. In British Human-Computer Interaction Conference (HCI),September 2000.
[27] D. Weinshall. Cognitive authentication schemes safe against spyware (short paper). In IEEE Symposium on Security and Privacy, May 2006.
[28] W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in Data Security, 2004.
[29] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.
[30] Passlogix, "www.passlogix.com," last accessed in June 2005.
[31] L. D. Paulson, "Taking a Graphical Approach to the Password," Computer, vol. 35, pp. 19, 2002.
[32] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Human-Computer Interaction International (HCII 2005). Las Vegas, NV, 2005.
[33] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in Symposium on Usable Privacy and Security (SOUPS). Carnegie-Mellon University, Pittsburgh, 2005.
[34] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human Computer Studies, to appear.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : YILDIZ, Muhammed Raşit
Uyruğu : T.C.
Doğum tarihi ve yeri : 25.05.1982 Yozgat
Medeni hali : Bekar
Telefon : 0 (312) 292 40 75
Faks : 0 (312) 292 40 91
e-mail : myildiz@etu.edu.tr

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Lisans	Selçuk Üniversitesi/Elektrik-Elektronik	2005

İş Deneyimi

Yıl	Yer	Görev
2007-2010	TOBB Ekonomi ve Teknoloji Üniversitesi	Araştırma Görevlisi

Yabancı Dil

İngilizce