MASAÜSTÜ VE MOBİL BİLGİSAYARLARI DESTEKLEYEN BİLGİ TABANLI YENİ BİR KİMLİK DOĞRULAMA YÖNTEMİNİN TASARLANMASI, GELİŞTİRİLMESİ VE DEĞERLENDİRİLMESİ

Uğur ÇİL

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AĞUSTOS 2013
ANKARA

Fen Bilimleri Enstitü onayı

_____

Prof. Dr. Necip CAMUŞCU
Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

_____

Doç. Dr. Erdoğan DOĞDU
Anabilim Dalı Başkanı

Uğur ÇİL tarafından hazırlanan MASAÜSTÜ VE MOBİL BİLGİSAYARLARI DESTEKLEYEN BİLGİ TABANLI YENİ BİR KİMLİK DOĞRULAMA YÖNTEMİNİN TASARLANMASI, GELİŞTİRİLMESİ VE DEĞERLENDİRİLMESİ adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

_____

Doç. Dr. Kemal BIÇAKCI
Tez Danışmanı

Tez Jüri Üyeleri

Başkan : Yrd. Doç. Dr. Ahmet Murat ÖZBAYOĞLU _____

Üye : Doç. Dr. Kemal BIÇAKCI _____

Üye : Doç. Dr. Bülent TAVLI _____

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.

Uğur ÇİL

Üniversite : **TOBB Ekonomi ve Teknoloji Üniversitesi**
Enstitü : **Fen Bilimleri Enstitüsü**
Ana Bilim Dalı : **Bilgisayar Mühendisliği**
Tez Danışmanı : **Doç. Dr. Kemal BIÇAKCI**
Tez Turu ve Tarihi : **Yüksek Lisans Tezi – Ağustos 2013**

Uğur ÇİL

MASAÜSTÜ VE MOBİL BİLGİSAYARLARI DESTEKLEYEN BİLGİ TABANLI YENİ BİR KİMLİK DOĞRULAMA YÖNTEMİNİN TASARLANMASI, GELİŞTİRİLMESİ VE DEĞERLENDİRİLMESİ

ÖZET

Günümüz dünyasında İnternete erişim olanakları hızlı bir şekilde gelişmekte ve çoğalmaktadır. Bu eğilimin bir neticesi olarak da akıllı telefonlar, tablet bilgisayarlar ve diğer tür mobil cihazlar yaygın olarak kullanılmaya başlanmıştır. İnternet üzerinde varlığını sürdürmekte olan birçok sistem ve/veya servis kullanıcılarından öncelikle kendilerini tanıtmalarını istemektedir. Bu isteğin sonucu olarak bahsi geçen cihazlardan metin tabanlı parolaların girişi son kullanıcılar açısından oldukça sıkıntılı bir süreç olabilmektedir. Büyük boyutlu fiziksel bir klavyeye sahip olmayan bu tür cihazlarda metin tabanlı parolaları girmek hem hata yapmaya daha yatkındır, hem de daha uzun zaman gerektirmektedir. Bu dezavantajlara çözüm bulabilmek amacı ile önerdiğimiz gridWordX yöntemi klasik metin tabanlı parola girişi ile grafik parola yaklaşımın aynı anda kullanılmasına olanak sağlayan ve masaüstü cihazlar ile mobil cihazlarda aynı anda kullanılabilen melez bir bilgi tabanlı kimlik doğrulama yöntemidir. Bu tez kapsamında gridWordX için çeşitli kullanıcı çalışmaları gerçekleştirilmiş ve bu çalışmaların sonucunda katılımcıların mobil cihazlarda gridWordX'i kullanarak sisteme giriş yapmalarının metin tabanlı parolaları kullanarak giriş yapmalarından daha kısa sürdüğü gözlenmiştir.

Anahtar Kelimeler: Kimlik Doğrulama, Kullanışlı Güvenlik, Mobil Cihazlar, Grafik Parolalar

University : TOBB University of Economics and Technology
Institute : Institute of Natural and Applied Sciences
Science Programme : Computer Engineering
Supervisor : Associate Professor Dr. Kemal BIÇAKCI
Degree Awarded and Date : M.Sc. – August 2013

Uğur ÇİL

DESING, IMPLEMENTATION, AND USABILITY EVALUATION OF A NOVEL KNOWLEDGE-BASED AUTHENTICATION SCHEME SUPPORTING BOTH DESKTOPS AND MOBILE DEVICES

ABSTRACT

In today's world, the number and opportunities of Internet access possibilities are rapidly increasing and developing. As a result of this situation, smart-phones and other mobile devices began to be commonly used in day-to-day life. Moreover, most of the online services want their users to authenticate themselves firstly. However, because of less friendly input methods, using traditional text-based passwords becomes even more tedious on these devices. To cope with these drawbacks on mobile devices and provide a scheme supporting both desktop and mobile devices, we propose a hybrid knowledge-based authentication scheme, gridWordX, which combines text and graphical elements. We conduct lab and web studies to compare usability of gridWordX with text-based passwords. The results show that gridWordX has significantly shorter login times on a mobile device and maintains comparable login times on a desktop machine.

Keywords: Authentication, Usable Security, Mobil Devices, Graphical Passwords

TEŞEKKÜR

Değerli tez danışmanım Doç. Dr. Kemal BIÇAKCI'ya yüksek lisans eğitimin boyunca bana karşı göstermiş oldu sabır ve içtenlikten dolayı,

Tez savunmama katılmayı kabul eden hocalarım Doç. Dr. Bülent TAVLI ve Yrd. Doç. Dr. Ahmet Murat ÖZBAYOĞLU'na,

Ve bütün eğitim hayatım boyunca bana karşı desteklerini esirgemeyen değerli aileme

En içten duygularımla teşekkür ederim.

İÇİNDEKİLER

ÖZET ..... İİİ

ABSTRACT ..... İV

TEŞEKKÜR V

İÇİNDEKİLER ..... Vİ

ÇİZELGELERİN LİSTESİ ..... Vİİİ

ŞEKİLLERİN LİSTESİ ..... İX

KISALTMALAR X

1 GİRİŞ 1

2 GENEL BİLGİLER 4

2.1 GRAFİK ŞİFRELER 4

2.1.1 Hatırlamaya Dayalı Sistemler 4

2.1.1.1 DRAW-A-SECRET (DAS) 5

2.1.1.2 DİĞER HATIRLAMAYA DAYALI GRAFİK PAROLA YÖNTEMLERİ 6

2.1.2 Tanımaya Dayalı Sistemler 8

2.1.2.1 PASSFACES (FACE) 9

2.1.2.2 DİĞER TANIMAYA DAYALI GRAFİK PAROLA YÖNTEMLERİ 10

2.1.3 İpucu ile Hatırlamaya Dayalı Sistemler 11

2.1.3.1 PASSPOİNTS 11

2.1.3.2 DİĞER İPUCU İLE HATIRLAMAYA DAYALI PAROLA SİSTEMLERİ 12

2.2 MOBİL KİMLİK DOĞRULAMA YÖNTEMLERİ 13

2.2.1 Kişisel Tanımlama Numarası (PIN) 13

2.2.2 Biyometrik Parola Sistemleri 14

2.2.2.1 İVMEÖLÇER ALGILAYICI İLE YÜRÜYÜŞ TANIMA 15

2.2.2.2 TUŞ BASIMI (KEYSTROKE) İLE TANIMA 15

2.3 ÇOK KELİMELİ (MULTİWORD) PAROLALAR 15

3 İLK SÜRÜM (GRİDWORD) 17

3.1 İLK SÜRÜM 17

3.2 ÖNCÜ ÇALIŞMA 18

3.2.1 Laboratuvar Çalışması 18

3.2.1.1 HİPOTEZLER 19
3.2.1.2 ÖNCÜ ÇALIŞMADA KARŞILAŞTIRILAN YÖNTEM PCCP 19
3.2.1.3 METODOLOJİ 22
3.3 ÖNCÜ ÇALIŞMANIN SONUÇLARI 25
4 ÖNERİLEN YÖNTEM (GRİDWORDX) 25
4.1 YENİ SÜRÜM: GRİDWORDX 25
4.1.1 Geliştirme Süreci ve Parametrelendirme 26
4.1.2 Hipotezler 29
4.1.3 Laboratuvar Çalışması 29
4.1.4 Web Çalışması 31
5 KULLANILABİLİRLİK ÇALIŞMASI 33
5.1 TOPLANAN VERİLER 33
5.1.1 Zaman ve Başarım Oranları 33
5.1.2 Parola Değiştirme Sayısı 34
5.1.3 Parola Giriş Yöntemi 34
5.1.4 Anket 34
5.2 VERİLERİN SONUÇLARI 34
5.2.1 Zaman ve Başarım Oranları 34
5.2.2 Parola Değiştirme Sayısı 36
5.2.3 Parola Giriş Yöntemi 38
5.2.4 Kullanıcı Algıları ve Görüşleri 39
5.3 TARTIŞMA 40
5.4 GÜVENLİK ANALİZİ 44
6 SONUÇ 47
7 KAYNAKLAR 48

ÇİZELGELERİN LİSTESİ

ÇİZELGE 5.1 GRİDWORDX VE METİN TABANLI PAROLA BAŞARIM ORANLARI 35
ÇİZELGE 5.2 DEĞİŞTİRME SAYISININ BAŞARIM ÜZERİNDEKİ ETKİSİ 36
ÇİZELGE 5.3 PAROLA GİRİŞ YÖNTEMİ FREKANSLARI 38

ŞEKİLLERİN LİSTESİ

ŞEKİL 2-1 DRAW-A-SECRET [14] 6
ŞEKİL 2-2 PASSFACES [22] 9
ŞEKİL 2-3 PASSPOİNTS [37] 12
ŞEKİL 2-4 CUED CLİCKED-POİNTS (CCP) [36] 13
ŞEKİL 3-1 GRİDWORD' UN PAROLA GİRİŞ EKRANI 17
ŞEKİL 3-2 PCCP PAROLA MİMARİSİ [57] 19
ŞEKİL 3-3 PCCP PAROLA OLUŞTURMA EKRANI 20
ŞEKİL 3-4 PCCP PAROLA ONAYLAMA EKRANI 21
ŞEKİL 3-5 PCCP PAROLA GİRİŞ EKRANI 22
ŞEKİL 4-1 GRİDWORDX PAROLA OLUŞTURMA EKRANI 1 26
ŞEKİL 4-2 GRİDWORDX PAROLA OLUŞTURMA EKRANI 2 27
ŞEKİL 4-3 GRİDWORDX PAROLA GİRİŞ EKRANI 27
ŞEKİL 4-4 GRİDWORDX'İN INTERNET ORTAMINDA ÇALIŞAN VERSİYONU 28
ŞEKİL 5-1 PAROLA OLUŞTURMA VE ONAYLAMA ZAMANLARI 36
ŞEKİL 5-2 PAROLA GİRİŞİ – LABORATUVAR ÇALIŞMASI 37
ŞEKİL 5-3 PAROLA GİRİŞİ – WEB ÇALIŞMASI 37
ŞEKİL 5-4 PAROLA GİRİŞ YÖNTEMİNE GORE ZAMAN PERFORMANSI (LABORATUVAR ÇALIŞMASI) 38
ŞEKİL 5-5 PAROLA GİRİŞ YÖNTEMİNE GORE ZAMAN PERFORMANSI (WEB ÇALIŞMASI) 39
ŞEKİL 5-6 MASAÜSTÜ PAROLA GİRİŞ SÜRELERİ 41
ŞEKİL 5-7 MOBİL CİHAZ PAROLA GİRİŞ SÜRELERİ 42
ŞEKİL 5-8 GRİD ÜZERİNDEKİ HÜCRELERİN SEÇİLME SIKLIKLARI 44
ŞEKİL 5-9 KELİMELERİN SATIR BAZLI DAĞILIMI 45
ŞEKİL 5-10 KELİMELERİN SÜTUN BAZLI DAĞILIMI 46

KISALTMALAR

Kısaltma	Açıklama
TOBB	Türkiye Odalar ve Borsalar Birliği
GPS	Global Positioning System
PDA	Personal Digital Assistant
PIN	Personal Identification Number
MITM	Man in The Middle Attack
KDA	Keystroke Dynamics-Based Authentication
NIST	National Institute of Standards and Technology

1 GİRİŞ

Günümüz İnternet sitelerindeki kimlik doğrulama işlemlerinde yaygın olarak kullanılan yöntem metin parola tabanlı kimlik doğrulama yöntemidir. Metin tabanlı kimlik doğrulama yöntemlerinin bu derece yaygın olarak kullanılmasının altında yatan başlıca nedenler olarak şunları sayabiliriz; kullanışlılık açısından basitliği, düşük kullanım ve gerçekleştirilme maliyeti, birden fazla platformdan erişilebilirlik, kullanıcıların hali hazırda sahip oldukları alışkanlıklarına uyumları, vb. gibi faktörler metin tabanlı parola sistemlerinin diğer sistemlere üstünlük sağlamasına neden olmaktadır. Tabi ki metin tabanlı kimlik doğrulama yöntemleri de tam anlamıyla sorunsuz ve harika sistemler değillerdir. Bu sistemlerinde bilenen ve üzerinde araştırmalar yapılan belli dezavantajları mevcuttur [1]. Kolay tahmin edilebilir parolalar genellikle kullanıcıların ilk seçimleri olurken [2], daha güçlü (daha yüksek entropi) parolaların hatırlanması daha zor olduğu için uygulamada birçok kullanıcı tarafından tercih edilmemektedir [3]. Kullanıcıların bu eğilimlerini göz önüne alan birçok çevrimiçi sistem, kullanıcıların da parola oluşturmaları esnasında uymaları gereken bazı politikalar belirlemektedirler. Örneğin, parolanın en az sekiz karakterden oluşması, en az bir tane rakam ve özel karakter içermesi gibi.

Metin tabanlı parola sistemlerinin yukarıda bahsi gecen sakıncalarına ek olarak İnternete erişiminde kullanılan cihazlarda görülen hızlı gelişmenin sonucu olarak kullanıcılar kimlik doğrulama adımında parolalarını, kullanımı kısıtlı ve zor olan sanal klavyeler yardımı ile girmek gibi yeni bir problemle daha karşı karşıya kalmışlardır [4]. İnternete erişim için kullanılan birçok akıllı telefonda var olmayan fiziksel klavyeler ve küçük ölçekli ekran boyutları kullanıcıların parolalarını doğru bir şekilde girmelerini güçleştirmektedir. Özellikle, sadece standart karakterlerden farklı olarak rakam ve özel karakter içeren parolaları girmek hem fazladan tuş vuruşu istemekte hem de hataya daha eğilimli olmaktadır. Örneğin, "QWERTY" klavye düzenine sahip bir sanal klavyede "a1bc1" parolasını girmek %50 daha fazla tuş vuruşu anlamına gelmektedir, bu da doğrudan kullanıcıların parolalarını girerken hata yapmaları oranının artmasına sebep olmaktadır.

İnternete erişim için kullandığımız cihazların yetersiz ve kısıtlı giriş yöntemlerine sahip cihazlardan, tam donanımlı fiziksel klavyelere sahip olan geleneksel masaüstü bilgisayarlarına gün içinde sıklıkla değişmektedir [5]. Bununla birlikte akıllı telefonların kendilerine özgü bazı fonksiyonları olan ivmeölçer, GPS ve kullanıcı profilini kullanan yeni kimlik doğrulama metotları masaüstü bilgisayarlar için uygun değillerdir. Bu noktada her iki kullanım şeklini de destekleyen daha güvenilir ve daha kullanışlı bir kimlik doğrulama yönteminin geliştirilmesi yeni bir akademik araştırma konusu olarak ortaya çıkmaktadır. Daha önce çalışılmamış olan bu probleme bir çözüm olarak sunulan metin tabanlı parola girişine ve ekran tabanlı seçimler ile parola girişine aynı anda olanak sağlayan melez bir kimlik doğrulama yöntemi olan gridWord çalışması daha önce sunulmuştur [5]. Bu tez kapsamında gridWord' ün yeni bir sürümü olan ve üzerinde yapılan geliştirilmeler sonucunda en son şeklini alan gridWordX isimli yöntem önerilmektedir. gridWordX'in kullanışlılığını değerlendirmek için yapılan kullanıcı deneylerinin sonuçları ışığında şunu söyleyebiliriz ki gridWordX, hem akıllı telefonlarda hem de masaüstü bilgisayarlarda kimlik doğrulamayı kolay ve güvenli bir şekilde sağlayan yeni ve umut verici bir yaklaşımdır.

Bu tezin kalan kısımları şu şekilde organize edilmiştir. Bölüm 2'de grafik parolalar ve mobile cihazlarda kimlik doğrulama ile ilgili genel bilgilerden bahsedilmiştir. Bölüm 3'de gridWordX'in bir önceki sürümü olan gridWord den ve yapılan pilot çalışmalardan bahsedilmiştir. Bölüm 4'de gridWordX uygulamasından ve yapılan kullanıcı çalışmalarından ve Bölüm 5'de yapılan kullanıcı çalışmalarının sonuçlarında bahsedilmiştir.

1.1 Bu Araştırmanın Temel Amacı

Bu tez kapsamında önerilen yöntem kimlik doğrulama yöntemlerine katkı sağlamak için şu amaçları taşımaktadır:

- Grafik şifreleri ve metin tabanlı şifreli birleştiren yeni bir kimlik doğrulama yöntemi geliştirmek.

- Bu geliştirilen kimlik doğrulama yönteminin geleneksel masaüstü bilgisayarları ve mobil cihazları destekleyebilecek özellikleri barındırması.

- Geliştirilen yeni yöntemin kabul edilebilir bir güvenlik seviyesi sağlamakla beraber, özellikle mobil cihazlarda kimlik doğrulamanın kullanışlılığını artırması.

2 GENEL BİLGİLER

Bu kısım altında grafik parolalar ve mobil cihazlardaki kimlik doğrulama yöntemleriyle alakalı genel bilgiler verilecektir. Bu bilgilerin verilmesindeki temel sebep tez kapsamında geliştirilmiş olan yöntemi anlatırken ve yapılan kullanıcı çalışmalarından bahsedilirken okuyucunun konu hakkındaki temel bilgilere sahip olmasını sağlamaktır böylelikle okuyucu daha verimli ve rahat bir şekilde konuları takip edebilecektir.

2.1 Grafik Şifreler

Geleneksel metin tabanlı parolalara alternatif olarak geliştirilen bir parola yöntemidir. Grafik parolaların doğumu doksanlı yılların sonlarına dayanmaktadır. Metin tabanlı parolalara alternatif, kullanıcılar tarafından daha kolay hatırlanabilen ve bunun sonucu olarak daha kullanışlı olan aynı zamanda tahmin etme (guessing attacks) saldırılarına karşı daha güvenli bir parola yöntemi oluşturmak motivasyonu ile ortaya çıkmışlardır [6]. Grafiksel parolalar da, selefleri olan metin tabanlı parolalar gibi bilgi tabanlı (knowledge-based) parola yöntemleridir. Bilgi tabanlı parola yöntemlerinde ortak bir giz kimlik doğrulama için kullanılır. Bu giz kullanıcı ve kimliğin doğrulanmak istenildiği sistem arasında ortak olarak bilinen bir gizdir. Grafiksel parolaların, metin tabanlı parolalardan farkı ise bu gizin alfabetik karakterlerden, sayılardan veya özel karakterlerden oluşmak yerine görsel öğelerden oluşmasıdır. Böyle bir yaklaşımın altında yatan bir numaralı bilimsel gerçek insanların görsel bilgileri sözel bilgilere göre daha kolay hatırlayabilmeleri ve anımsamalarıdır [7-10].

Grafik parolalar hatırlama ve parolayı girme yöntemlerine göre 3 ayrılırlar; hatırlamaya dayalı (recall based), tanımaya dayalı (recognition based) ve ipucu ile hatırlamaya dayalı (cued-recall based).

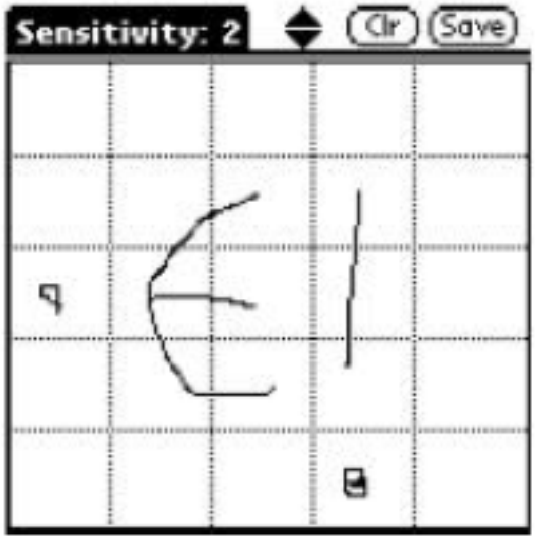
2.1.1 Hatırlamaya Dayalı Sistemler

Hatırlamaya dayalı sistemlerde kullanıcılar daha önceden oluşturdukları veya sistem tarafından kendilerine atanmış olan grafik parolalarını hatırlamak ve boş bir tuval

veya ızgara üzerine yeniden çizmek zorundadırlar. Bir ipucu olmaksızın bir şeyi hatırlamak zor bir durumdur [11]. Standart metin tabanlı parolaları da hatırlamaya dayalı parola sistemleri olarak sınıflandırabiliriz. Her ne kadar kullanıcılar metin tabanlı parolalarında sistem isimlerini parolalarına birer ipucu olarak kullansalar da bundan kullanıcı dışında kimsenin haberi olmamaktadır [12-13]. Birçok hatırlamaya dayalı parola sisteminde kullanıcılar kendi parolalarını kendileri seçmektedirler (sistem tarafında atanmamaktadır), bu tip bir sisteme karşı yapılacak kişilere özgü ataklar genel ataklardan daha başarılı olabilir. Hali hazırda var olan bir kaç tane standart hatırlamaya dayalı parola sistemine örnek vermek gerekirse;

2.1.1.1 Draw-A-Secret (DAS)

Önerilen ilk hatırlamaya dayalı grafiksel parola sistemidir [14]. Bu sistem de kullanıcı fare veya dokunmatik kalem yardımıyla iki boyutlu tuval üzerine bir çizim yapmalıdır ve daha sonra kendisini sisteme tanıtmak istediğinde bu çizimi tekrarlamak zorundadır. Kullanıcılar parolalarını çizdiklerinde sistem bu parolaları tuval üzerindeki hücrelerin ardışık koordinatları olarak tutmaktadır. Bu sistem üzerine yapılan çalışmalar sonucunda kullanıcıların iki boyutlu tuval üzerinde genellikle simetrik şekilleri parola olarak seçmeye eğilim gösterdikleri ortaya çıkmıştır. Teorik parola uzayı, 5x5 boyutlarında bir tuval ve en fazla 12 uzunluğundaki bir parola için 2^{58} olacaktır [14]. Fakat burada belirtilen teorik parola uzayıdır yani gerçekte kullanıcıların eğilimlerine göre pratikte ortaya çıkacak olan parola uzayı daha düşük seviyelerdedirler.



Şekil 2-1 Draw-A-Secret [14]

Sonuç olarak, DAS metin tabanlı parola yöntemleriyle karşılaştırıldığı zaman yeteri kadar teorik büyüklükte bir parola uzayı sağlamaktadır. Fakat daha önce de söylendiği gibi burada önemli olan kullanıcıların davranışlarıdır. Kullanıcıların, yapılan çalışmalarda görüldüğü gibi, simetrik şekilleri tercih etmesi DAS'nin pratikteki etkinliğini azaltacağı ortadadır.

2.1.1.2 Diğer Hatırlamaya Dayalı Grafik Parola Yöntemleri

BDAS (Background Draw-A-Secret) [15], DAS'nin geliştirilmiş bir sürümüdür. DAS'ye ek olarak arka plana koyulan bir resim yardımıyla kullanıcıların simetrik çizimlerden kaçınmaları ve daha uzun çizimleri parola olarak seçmeleri sağlanmıştır. Fakat kullanıcıların resimler üzerindeki belli noktaları ve/veya modelleri izleyip izlemediği konusunda ek çalışmalar mevcut değildir.

Gao ve diğerleri tarafından önerilen YAGP (Yet Another Graphical Password) de DAS'nin geliştirilmiş bir modelidir. Daha hassas tuval kullanmak için farklı bir yakınsama algoritması kullanılmıştır (Levenshtein mesafesi). Fakat bu sistemdeki sorun girilen parolanın karşılaştırılma yapılmak için sistem tarafından erişilebilen bir yerde kriptografik bir hash fonksiyonu uygulanmadan saklanmak zorunda olmasıdır.

Passdoodle [16-17] diğer hatırlama tabanlı grafik parola sistemleri gibi tuval üzerine yapılan çizimleri kullanmaktadır. DAS'ye ek olarak tuvali belli bölgelere ayıran görünür çizgiler yoktur ve daha karmaşık eşleşme algoritmaları kullanmaktadır. Bu sistem üzerine yapılmış üç ayrı kullanıcı çalışması mevcuttur. Kullanıcıların kendi yaptıkları karalamalarını hatırlamaları ve tekrar yapabilmeleri üzerine yoğunlaşmışlardır. Bu çalışmaların sonuçları belirgin bir şekilde rapor edilmemiş olsa da eşleştirme algoritmalarının kullanılmadan önce, eğitim sürecine ve veri kümelerine ihtiyaç duyduğu anlaşılmıştır.

Pass-Go [18], Tao ve Adams tarafından önerilen bir sistemdir. Adını eski bir oyun olan Go'dan almaktadır. Bu sistemin arkasında yatan motivasyon DAS'nin yaşamış olduğu bazı problemlere çözüm getirerek daha kullanışlı ve güvenli bir grafik parola yöntemi sunmaktır. Bu sistemi kullananlar parolalarını oluşturmak için tuval üzerinde bulunan yatay ve dikey çizgilerin kesişim noktalarını kullanmaktadırlar. Buna ek olarak çizimlerinin rengini değiştirerek parolalarını daha da kişiselleştirebilmektedirler. Ve çapraz çizimlere de izin verilmektedir. Bu özellikleri sayesinde Pass-Go'nun teorik parola uzayında artış yakalamıştır. Ve sistem kullanışlılığının test edilmesi için alan çalışması yapılan tek hatırlama tabanlı grafik parola yöntemidir. Rapor edilen sonuçlara göre kullanıcıların %78 başarılı bir şekilde sisteme giriş yapmışlardır.

Ticari bir kimlik doğrulama yöntemi olan GrIDsure [19] kullanıcılarından 5x5 boyutlarındaki bir tuval üzerinde yerleştirilmiş olan yirmi beş tane sayıdan bir model seçmelerini ve bu modeli ezberlemelerini istemektedir. Daha sonra kullanıcılar sisteme giriş yapmak istediklerinde bu yirmi beş rakam karşılarına rastgele dizilmiş bir şekilde çıkmakta ve kullanıcılardan ezberledikleri modellerini klavye yardımı ile metin tabanlı parolalar gibi girmeleri istenmektedir. Diğer sistemler gibi GrIDsure da parolaları açık bir şekilde tutmaktadır. Bu sistemin PDA'lar üzerinde yapılan bir kullanıcı deneyi sonucunda, katılımcıların parolalarını ilk seferde doğru olarak girmelerinin oranı %84 olmuştur. Aynı katılımcıların 2 yıl sonra parolalarını tekrar girmeleri istenildiğinde %12'lik bir başarı oranı gözlemlenmiştir.

2.1.2 Tanımaya Dayalı Sistemler

Hatırlamaya dayalı sistemler genellikle kullanıcılarından bir kaç resimden oluşan bir portföyü ezberlemelerini ve sisteme girişleri sırasında daha önce ezberlenen resimleri de içeren birçok resim arasından bu portföyü tanımalarını istemektedir. İnsanların bilişsel özellikleri üzerinde yapılan çalışmalara göre, daha önce açık bir şekilde görülen resimlerin daha kolay olarak tanınabilmesi beklenmektedir [20-21]. Tanımaya dayalı sistemleri güvenlik açısından değerlendirecek olursak yeterince güvenli olduklarını söyleyemeyiz. Güvenlik seviyeleri 4-5 rakamdan oluşan PIN güvenlik seviyesi ile aynı düzeydedir. Kullanıcıların tanıması beklenen resimler ikonlar, yüz resimleri, günlük nesnelerin resimleri gibi farklı resimlerden oluşabilmektedir.

Oltalama (Phishing) saldırılarına karşı tanımaya dayalı sistemler daha fazla direnç göstermektedirler. Çünkü kullanıcıya özel olan resim kümesini ki bu küme kullanıcının portföyünü de içermek zorundadır sunması gerekeceği için ve resim kümesinin de kullanıcıya özgü olmasından böyle bir saldırı gerçekleştirilmesi oldukça güçleşmektedir. Fakat MITM ile birleştirilen bir oltalama saldırısı ise oldukça etkili olabilir. Kullanıcı ismini aldıktan sonra bu bilgiyi gerçek sisteme gönderen ve buradan gelen resim kümesini de kendi üzerinden kullanıcıya sunabilen bir oltalama sitesi kullanıcının portföyüne kolaylıkla ulaşabilecektir.

Gözetleme saldırılarına (ShoulderSurfing) karşı tanımaya dayalı sistemlerin eğer belirli önlemler alınmazsa zafiyetleri mevcut. Çünkü kullanıcıların ekranları gözetlenebiliyorsa her kullanıcıya ait resim kümesi kolayca belirlenebilir ve kullanıcıların seçtikleri portföyleri küçük olmasından bu portföyler de kolayca gözetlenebilirler. Tanımaya dayalı sistemlerin bu zafiyetlerini mümkün oldukça azaltabilmek adına alınan belli başlı önlemler bulunmaktadır. Mesela, portföy resimlerinin yerini her giriş sırasında değiştirmek saldırganlar için ekstra gözetleme yapmak anlamına gelecektir. Bu kapsamda geliştirilmiş olan sistemlerden birkaçını aşağıda bulabilirsiniz.

2.1.2.1 Passfaces (Face)

Bugüne kadar üzerinde en çok çalışılmış olan tanımaya dayalı grafik parola sistemi Passfaces'dir [22]. Bu sistemde kullanıcılardan kendilerine ait bir resim kümesi oluşturmaları istenilmektedir. Resimler insan yüzlerinden oluşan profil resimleri olacaktır. Daha sonra sisteme giriş yapmak isteyen kullanıcı farklı birçok resim arasından kendi resim kümesine ait olan yüzleri seçmek zorundadır ve bu işlem farklı resim kümeleri ile birçok kez tekrarlanarak sistemin güvenlinin artırılması hedeflenmektedir. Orijinal sistemde n = 4 kere tekrar ve her tekrar için M = 9 adet profil resminden oluşmaktadır. Her panelde sadece bir resim kullanıcının gerçek resim kümesine ait olmaktadır. Bu durumda sistemin güvenlik düzeyi M^n olacaktır bu da 9^4 olarak yaklaşık 2^{13} olmaktadır.

Şekil 2-2 Passfaces [22]

Valentine [23] gerçekleştirdiği kullanıcı deneylerinin sonucuna göre 5 aylık aralarda yapılan deneylere rağmen kullanıcıların %72'si ilk ve %100'ü de en fazla üçüncü denemelerinde sisteme giriş yapabilmektedirler. Bu sistem üzerinde gerçekleştirilen birçok akademik çalışmanın sonucu olarak farklı veri elde edilmiştir. Brostoff ve Sasse'nin [24] çalışmalarına kullanıcılar Passfaces parolalarını metin tabanlı parolalara oranla daha yavaş şekilde girmektedirler. Davis ve diğerlerinin [25]

çalışmalarında vardıkları sonuç ise kullanıcıların kolay tahmin edilebilir parolalar seçtikleri olmuştur. Mesela kullanıcıların kendi ırklarına benzer profil resimlerini veya kendi cinsiyetlerinin profil resimlerini seçmeye eğilim gösterdiklerini ortaya çıkarmışlardır. Bahsi geçen problemleri aşmak için ticari Passfaces uygulaması parola olarak seçilen profil resimlerini kullanıcının seçimine bırakmak yerine sistem tarafından rastgele bir şekilde atamaktadır. Akademik olarak yapılan çalışmalarda parola oluşturma sürelerinden hiç bahsedilmemesine rağmen The Passfaces şirketinin internet sitesinde yer alan bilgilere göre parola oluşturma suresi 9 profil resimli ve 5 tekrarlı bir sistemde 3 ile 5 dakika arasındadır [22].

2.1.2.2 Diğer Tanımaya Dayalı Grafik Parola Yöntemleri

Story [25], Passfaces'e benzer bir sistemdir. Bu sistemde kullanıcılardan bir resim kümesi içinden kendilerine ait başka bir alt küme oluşturmaları istenmektedir ve bu kümeyi tanımalarını kolaylaştırmak için bir hikâye oluşturmaları tavsiye edilmektedir. Kullanıcılar 9 resim içinden kendilerine ait 4 adet resim belirleyecekleri için sistemin güvenlik seviyesi 9*8*7*6 = 3024 yani yaklaşık olarak 2^{12} olmaktadır. Yapılan çalışmalarda kullanıcıların Story parolalarını tanımaları Passfaces parolalarını tanımalarından daha zor olduğu ortaya koyulmuştur.

Déjà Vu [26] Passfaces ve Story'nin farklı bir uygulamasıdır. Déjà Vu'nun farkı resim kümesi olarak günlük nesnelerin resimleri veya profil fotoğrafları yerine rastgele üretilmiş sanat resimleri kullanmasıdır. Bu sistemin teorik parola uzayı 25 resimden oluşan 5 turluk bir sistem girişi için yaklaşık olarak 2^{16} denilebilir.

GPI ve GPIS [27] bir diğer tanımaya dayalı grafik parola sistemleridir. İki sistem arasındaki tek fark ise GPIS de parolanın sistem tarafından öneriliyor olmasıdır. Her iki sisteminde güvenlik seviyeleri birçok ipucu ile hatırlamaya dayalı sistem ile baş başadır, 2^{43}.

2.1.3 İpucu ile Hatırlamaya Dayalı Sistemler

Bu tip sistemlerde kullanıcılardan genellikle bir resim üzerinde belli nokta veya noktaları hatırlaması istenilmektedir. Burada arka plan resimleri kullanıcıların işini kolaylaştırmak için birer ipucu olarak kullanılmaktadır. Daha önce yapılan çalışmalarda [28] insanların resimlerde dikkat ettikleri bazı parçaları veya kısımları daha rahat hatırlayabildikleri anlaşılmıştır. Şu ana kadar geliştirilmiş olan ipucu ile hatırlamaya dayalı grafik parola sistemlerine bir göz atalım.

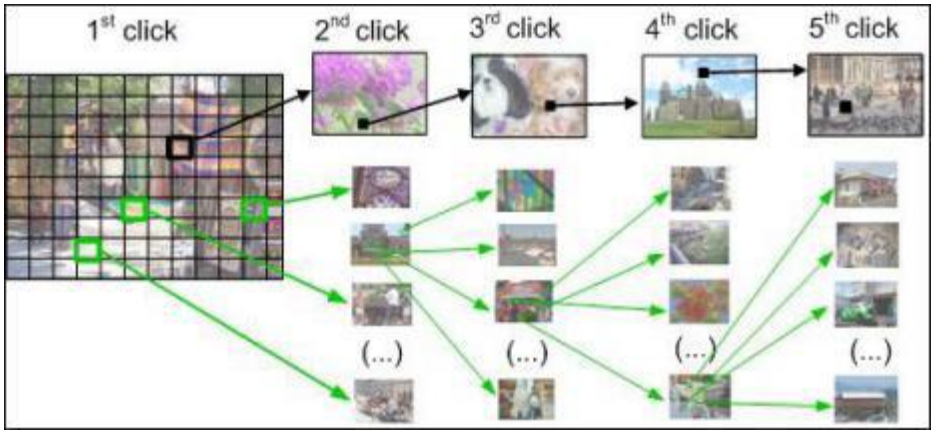
2.1.3.1 PassPoints

Bu alanda üzerinde en çok araştırma yapılan ve ileri çıkan parola yöntemi PassPoints'dir [29-31]. Kullanıcılarından aynı resim üzerinde 5 nokta seçmeleri istenilmekte ve sistem girişi sırasında seçtikleri noktaları ayni sıra ile tekrar girmeleri beklenmektedir. Daha önce seçilen bir noktayı birebir olarak tutturmak kullanışlılık açısından uygun olmadığı için tıklamaların belli bir yanılma payı ile yapılması kabul edilmektedir. Burada dikkat edilmesi gereken bir husus da şudur ki 5 ayrı nokta için sadece bir resim kullanmak tam anlamıyla ipucu ile hatırlamak manasına gelmemektedir. Wiedenbeck ve diğerlerinin [29-31] yapmış olduğu kullanıcı çalışmalarına göre kullanıcıların parolalarını oluşturmaları 64 saniye sürerken, sisteme giriş yapabilmeleri için geçen ortalama süre 9 ile 19 saniye arasında değişmektedir. Ve bu çalışmalar sonucunda resimler üzerindeki noktalar için gereken tolerans alanın en az 14x14 piksel olması gerektiği önerilmektedir. Bu çalışmaya ek olarak Chiasson ve diğerleri [37] tarafından yapılan başka bir çalışmada arka plan resminin sistemin kullanışlılığını etkilediği ortaya koyulmuştur. Ayrıca sıcak nokta (Hotspots) problemi olarak bilinen resimlerin belli noktalarında öbekleşmenin meydana gelmesi gibi problemler de daha sonraki deneylerde ortaya çıkmıştır [32-35].

Şekil 2-3 PassPoints [37]

2.1.3.2 Diğer İpucu ile Hatırlamaya Dayalı Parola Sistemleri

PassPoints'in dışında en çok bilinen yöntemlerden birisi de Cued Click-Points (CCP) [36] yöntemidir. PassPoints de bahsi geçen gerçek manada bir ipucu ile hatırlamaya dayalı grafik parola yöntemi olmaması sorununa CCP 5 resim üzerinden toplamda 5 ayrı nokta seçerek çözüm getirmiştir. Bu sayede her nokta için üzerinde bulunduğu resim bir ipucu görevini görmektedir. Kullanıcının resim üzerindeki tıklamasından sonra gelecek olan diğer resim seçilen noktaya göre değişmektedir bu da kullanıcıya doğru noktaya tıklayıp tıklamadığı konusunda bir geri bilgi akışı sağlamaktadır. Bu bilgi meşru kullanıcıdan başka kimseye bir anlam ifade etmemektedir çünkü doğru resmi sadece meşru kullanıcılar bilmektedir. Yapılan kullanıcı deneylerinde CCP ile alakalı olarak şu sonuçlar gözlemlenmiştir: kullanıcıların %96'sı parolalarını ilk seferde doğru olarak girmişlerdir. Parola oluşturma süreleri 25 saniye civarında olurken, sisteme giriş süresi ise ortalamada 7 saniye olmuştur.



Şekil 2-4 Cued Clicked-Points (CCP) [36]

Persuasive Cued Click-Points (PCCP) [2], CCP'nin geliştirilmiş bir versiyonudur. CCP de karşılaşılan sıcak nokta problemine çözüm bulmak için önerilen görüntü kapısı (Viewport) yöntemiyle kullanışlılığı negatif olarak en az seviyede etkileyerek kullanıcıları bilinen sıcak noktalardan uzak tutamak amaçlanmaktadır. Görüntü kapısı sayesinde kullanıcılar resmin sadece bir kısmından (75x75 piksel büyüklüğünde ki bir kısmından) noktalarını seçebilmektedirler. Görüntü kapısının yeri sistem tarafından rastgele olarak seçilmektedir eğer kullanıcı görüntü kapısının yerinde memnun olmazsa istediği kadar yerini değiştirebilmektedir. Her değiştirme isteğinin sonucunda görüntü kapısının yeri tekrar sistem tarafından rastgele olarak belirlenmektedir. Yapılan çalışmalar [2] sonucunda görüntü kapısının başarılı bir şekilde sıcak nokta probleminin üstesinden geldiği görülmüştür.

2.2 Mobil Kimlik Doğrulama Yöntemleri

Mobil cihazlarda kullanılan veya şu ana kadar önerilmiş olan kimlik doğrulama yöntemlerine genel bir bakış yapılacaktır. İlk olarak yaygın bir şekilde kullanılan PIN'ler üzerinde durulacaktır, daha sonra biyometrik kimlik doğrulama yöntemleri ele alınacak ve en son olarak da çok kelimeli parolalara değinilecektir.

2.2.1 Kişisel Tanımlama Numarası (PIN)

Hali hazırda akıllı telefonlar ve PDA'lar için yaygın bir şekilde kullanılan bir kimlik doğrulama yöntemidir [38]. 4 veya 8 haneli rakamlardan oluşan bir paroladır. Birinci

derecede tercih edilmesinin temel sebepleri arasında kullanım kolaylığı ve yıllardır bu alanda var olmasının sonucunda kullanıcılar üzerinde sahip oldu pozitif etkilerdir. Üreticiler tarafından bakıldığında ise gerçekleştirilebilmesinin kolaylığı ve ekstra donanım gerektirmemesi başlıca nedenler olmaktadır [39]. Diğer parolalara göre daha yaygın olarak kullanılmasına rağmen, yapılan bir araştırma sonucunda kullanıcıların sadece %66'sının PIN kullandığına rastlanılmıştır [40]. PIN'lerin dezavantajları arasında düşük güvenlik seviyesine sahip olmaları birinci sırada yer almaktadır. Dört haneli bir PIN için yaklaşık olarak 2^{10} (10^4) derecesinde bir güvenlik seviyesi vardır bu da oldukça düşük bir değer sayılabilir. Buna ek olarak kullanıcıların kolay tahmin edilebilir parolaları seçmeleri de başka bir sorundur (doğum tarihi, plaka numarası vb.). Yapılan bir araştırma sonucunda 204,508 PIN'in %15'i en yaygın 10 PIN'den biri olduğu ortaya çıkarılmıştır [41].

2.2.2 Biyometrik Parola Sistemleri

Biyometrik sistemler kullanıcıların fizyolojik veya davranışsal karakteristiğini temel alan bir kimlik doğruluma yöntemidir. Biyometrik kimlik doğrulama kullanıcının parmak izine, sesine, el veya yüz geometrisine, el yazısına, klavye kullanımına (tuşlara basma hızı vb.), yürüyüş biçimine gibi birçok karakteristiğine bakarak yapılabilmektedir. Kullanıcının fiziksel veya davranışsal karakteristiğinin Biyometrik kimlik doğrulama kullanılabilmesi için bazı koşulları sağlaması gerekmektedir. Bu koşullar, (i) Genellik; herkes istenilen karakteristiğe sahip olmalıdır, (ii) Benzersizlik; karakteristik özelliği birbirine benzeyen iki kullanıcı var olmamalıdır, (iii) Kalıcılık; karakteristik zaman ile değişime uğramamalıdır, (vi) Sayısallaştırma; yani karakteristikler sayısal olarak ölçülebilir olmalıdır [42]. Biyometrik parola sistemlerinin en büyük avantajlarından birisi kullanıcılarının ekstra bir aygıt taşımak zorunda kalmamaları veya herhangi bir parolayı ezberlemek zorunda olmamalarıdır. Parolaları her zaman beraberlerindedir. Fakat biyometrik parolalardan bahsettiğimiz zaman düşünülmesi gereken önemli bir konu vardır ki o da mahremiyet konusudur. [43-45]. Örneğin, kullanıcının parmak izinden tanına bilmesi için aynı verilerin sistem tarafından da saklanıyor olması gerekmektedir. Böyle bir durumda eğer sistemde saklanan veriler üçüncü kişi veya kurumların eline geçecek olursa

kullanıcının mahremiyeti çiğnenmiş olacaktır. Önerilmiş olan birkaç sisteme yakından bakalım.

2.2.2.1 İvmeölçer Algılayıcı ile Yürüyüş Tanıma

İvmeölçer algılayıcı ile yürüyüşe dayalı tanımada (Boimetric Gait Recognition), mobil cihazın donanımları arasında yer alan bir algılayıcı kullanıcısının yürüyüş stilini kimlik tanıma aracı olarak kullanmaktadır. Tıp [46], Psikoloji [47], Biyometrik [48-49] alanında yapılmış temel çalışmalarda insan yürüyüşünün kişilere özgü karakteristikleri olduğu ortaya koyulmuştur. Derawi ve diğerlerin önermiş oldukları sistemde başarım oranı önceki çalışmalara göre %50 oranında artmış ve %20,1'e çıkmıştır [50]. Burada dikkate alınması gereken noktalardan biride mobile cihazların ivmeölçerlerinin düşük seviyede örnekleme yapmış olmalarıdır ve bu deneyinde yürüyüş tanıma sistemini akıllı telefonlarda deneyen ilk çalışma olmasıdır.

2.2.2.2 Tuş Basımı (Keystroke) İle Tanıma

Tuş basımı ile tanıma kullanıcıların fiziksel veya sanal klavyeler ile yazma karakteristiklerini temel alarak çalışan bir sistemdir. Burada iki şekilde ölçüm yapılarak kullanıcılar ayırt edilebilmektedir. Birincisi, iki tuş basımı arasındaki gecikmeyi ölçerek kullanıcı bazlı bir karakteristiğin ortaya çıkartılmasıdır. Bu tip bir ölçüm ile sayısal veri girişleri sınıflandırılabilir [51]. İkincisi ise bir tuşa basıldığı zaman bu tuşun basılı tutulma sürecidir bu tip bir ölçümle de alfabetik veri girişi sınıflandırılabilir, mesela bir metin yazmak [51]. Yapılan çalışmalara göre iki tuş basımı arasındaki gecikmenin ölçülmesiyle varılan sonuçların daha tutarlı olduğu anlaşılmıştır [52-54]. Hwang ve diğerleri [55] tarafından önerilen KDA sisteminde kullanıcılardan sisteme girişleri sırasında sadece parolalarını girmeleri istenilmiştir fakat kimlik doğrulama yapılırken ise sadece parolanın doğru girilip girilmediği değil aynı zamanda tuş basımını dinamiklerini de dikkate alınmaktadır.

2.3 Çok Kelimeli (Multiword) Parolalar

Parolaları anlamlı birçok kelimeden oluşturmak aslında oldukça eski bir yaklaşımdır. Temelleri 1980'lerin başlarına dayanan bir öneridir [5]. Fastword [56] adlı çalışma

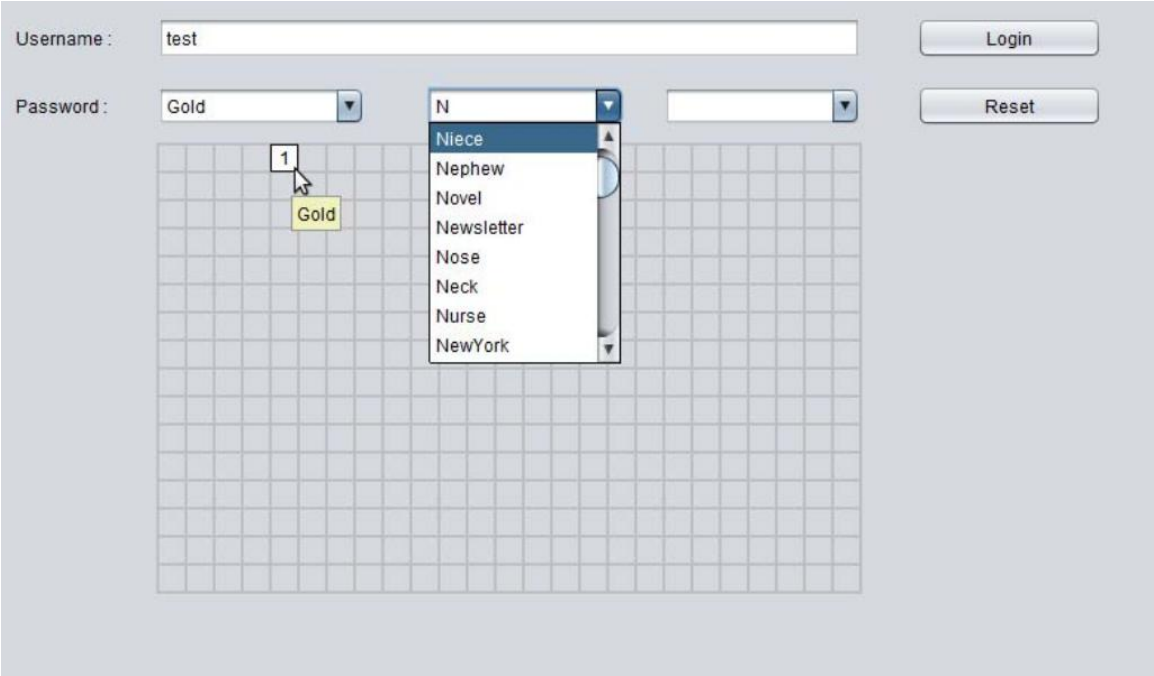
bu olguyu parola girişi kısıtlı olan cihazlar için (dokunmatik ekranlı akıllı cihazlar gibi) tekrar ele almıştır. Hata düzeltme ve otomatik tamamlama gibi özellikleri Fastword'ü küçük ekranlı akıllı telefonlarda kullanıma uygun hale getirmiştir. Yapılan çalışmalar sonucunda Fastword'ün klasik metin tabanlı parolalar üzerindeki 3 avantajından bahsedilmiştir. Birincisi, parola girişindeki hız artışıdır. İkincisi, artırılmış güvenlik seviyesi ve son olaraktan daha yüksek hatırlama oranları Fastword'ün metin tabanlı parolalar üzerindeki avantajları olduğu iddia edilmektedir [56]. Ayrıca Fastword yönteminde kullanıcıların ses ile parolalarını girmeleri de mümkündür.

3 İLK SÜRÜM (gridWord)

Bu kısımda tez kapsamında geliştirmiş olduğumuz yöntem olan gridWordX'in önceki sürümü olan gridWord'den ve bu sistem ile gerçekleştirilen ilk çalışmalardan söz edilecektir.

3.1 İlk Sürüm

gridWord'ün temellerinde yatan fikir, kullanıcılara, iki boyutlu bir tuval üzerinde somut kelimeler (tren, gemi, vb.) ile eşleştirilmiş hücrelere sahip, diğer grafik parolalara alternatif daha kullanışlı bir yöntem önermekti.



Şekil 3-1 gridWord' un Parola Giriş Ekranı

Şekil 3.1 de gridWord'ün parola giriş ekranı görülmektedir. Ekranın üst kısmında 3 adet açılır kutu (combo box) bulunmaktadır. Bu kutulara kullanıcı isterse parolasını klasik yöntemler ile klavyeden girebilir. Bu açılan kutular otomatik tamamlama özelliğine sahiptir bu şekilde kullanıcı parolasının tamamını yazmak zorunda kalmadan, otomatik olarak seçenekler girdi karakterlere göre karşısına çıkacaktır.

Bu açıdan bakıldığında çok kelimeli diğer bir sistem olan Fastword [56] ile arasında önemli bir fark vardır: Açılır kutuların alt kısmında iki boyutlu bir tuval üzerinde birçok hücreden oluşan bir kısım bulunmaktadır. Bu hücrelerin her birisi somut bir kelime ile durağan bir şekilde bire bir olarak eşleştirilmişlerdir. Kullanıcı eğer imleç ile bu hücreler üzerinde gezer ise her hücreye karşılık gelen kelime araç ipucu olarak ekranda görünecektir. Ayrıca kullanıcı her hangi bir hücreye tıkladığı zaman tıklanan hücreye karşılık gelen somut kelime üst kısımdaki ilgili açılır kutuda belirmektedir. Bu durumun tersi olarak da eğer kullanıcı açılır kutuya bir kelimeyi yazdıysa bu kelime ile eşleştirilmiş olan hücre otomatik olarak seçili hale gelmektedir.

PCCP [57] den esinlenerek gridWord de parolalar sistem tarafından rastgele olarak atanmaktadır. Fakat kullanıcı kendisine verilen paroladan memnun değil ise tekrar bir parola isteğinde bulunabilmektedir ve bu işlemi isteği kadar tekrarlayabilir. Parolaların sistem tarafından atanmasında ki temel sebeplerden birisi sıcak nokta (Hotspots) problemindir.

gridWord' un ilk sürümü bağımsız olarak çalışan bir masaüstü Java uygulaması olarak geliştirilmiştir. Bu uygulamada iki boyutlu bir tuval üzerinde 16 satir ve 25 sütun seklinde 400 adet hücre bulunmaktadır. Ve her bir hücrenin boyutu 19x19 piksel büyüklüğündedir. Bu büyüklüğün seçilmesindeki temel sebep PCCP [57] ile tutarlı değerlere sahip olabilmektir. Bu şekilde gridWord deki tuval boyutu PCCP'nin arka plan resmine bire bir oranında benzerlik gösterebilecektir. Ve PCCP deki hassasiyet ölçüleri ile gridWord'ün hücre boyutları aynı olacaktır.

3.2 Öncü Çalışma

Öncü çalışmamız laboratuvar tabanlı bir kullanıcı deneyi olarak tasarlandı.

3.2.1 Laboratuvar Çalışması

Bu çalışma kapsamında gridWord, daha önce önerilmiş olan PCCP yöntemi ile klasik masaüstü bilgisayarlarda karşılaştırıldı.

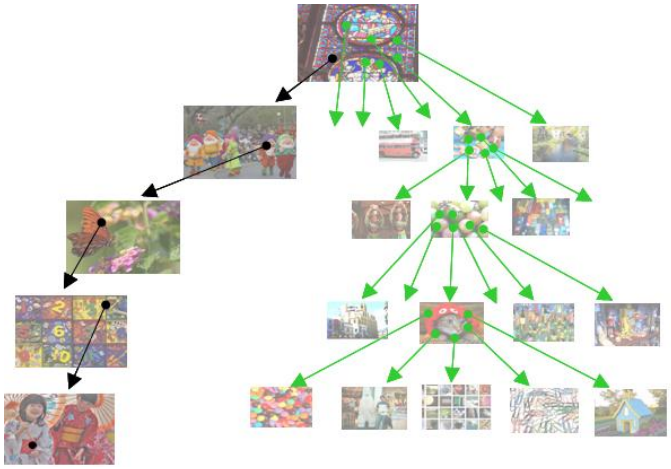
3.2.1.1 Hipotezler

Pilot çalışmada test edilmiş olan hipotezler şunlardır:

- gridWord'ün başarılı şekilde sistem girişi oranları PCCP'nin oranlarından daha yüksektir.
- gridWord'ün sistem giriş süreleri PCCP'nin sistem giriş sürelerinden daha kısadır.
- Kullanıcıların gridWord de sistem tarafından atanan paralarını değiştirme oranları PCCP ile yaklaşık olacaktır.

3.2.1.2 Öncü Çalışmada Karşılaştırılan Yöntem PCCP

PCCP [57], kullanıcının art arda gelen resimler üzerinde bir nokta seçerek parolasını oluşturduğu bir sistemdir.



Şekil 3-2 PCCP Parola Mimarisi [57]

Şekil 3-3'de kullanıcıların parola oluştururken, kullanıcı isimlerini girdikten sonra parolalarını girecekleri için gelecek olan ekran görünmektedir. Kullanıcılar 451x331 piksel büyüklüğündeki resim üzerinde bulunan 75x75 piksel büyüklüğündeki görüntü kapısı (Viewport) içinde kalan kısımdan bir yere tıklayarak parolasının her bir bileşenini oluşturuyorlar. Eğer kullanıcı görüntü kapısının yerinden memnun

değilse “Değiştir” butonuna basarak görüntü kapısının yerini değiştirebilir. Ancak görüntü kapısının yeni konumu tekrar sistem tarafından belirlenecektir ve rastgele olacaktır. Deneyde kullandığımız PCCP uygulamasında kullanıcıların 3 resim üzerinde tıklama yapması gerekmektedir. Eğer kullanıcı daha önceki adımlarda seçmiş olduğu resim ve/veya noktalardan vazgeçmek isterse “Baştan Başla” düğmesine basarak parola oluşturmaya tekrar baştan başlayabilir. Yâda bütün işlemlere tekrar başlamak isterse bunu “Ana Ekrana Dön” düğmesine basarak gerçekleştirebilir.

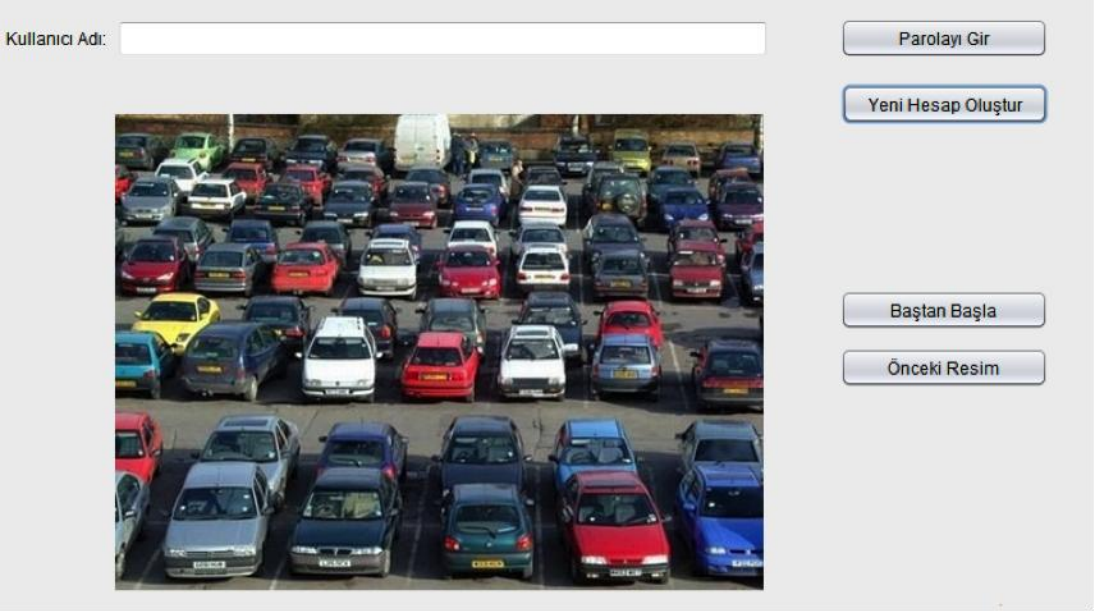
Şekil 3-3 PCCP Parola Oluşturma Ekranı

Parola onaylaması için kullanıcıdan bir önceki adımda oluşturduğu parolasını tekrar girmeleri istenecektir.(Şekil 3-4) Fakat bu sefer resimlerin üzerinde görüntü kapısı olmayacaktır. Kullanıcı parola oluşturma aşamasında belirlediği noktalara tekrar tıklamak zorundadır. Eğer tıkladığı nokta bir önceki adımda parolasını oluştururken tıkladığı noktanın 19x19 piksellik bir tolerans aralığında değil ise bu tıklama yanlış sayılacak ve karşısına parola oluştururken kullandığı resimden farklı bir resim

gelecektir (Şekil **3-2** PCCP Parola Mimarisi [57]). Bu durumda kullanıcının yanlış yere tıkladığını fark etmesi beklenir. Kullanıcı isterse "Önceki Resim" düğmesine basarak bir önceki resme dönebilir ya da "Baştan Başla" düğmesine basarak parolasını doğrulamaya en baştan başlayabilir.

Şekil 3-4 PCCP Parola Onaylama Ekranı

Parolasını başarıyla belirleyip kendisini sisteme kaydedebilen kullanıcılar Şekil 3-5'de gösterilen sayfa üzerinde sisteme giriş yapabileceklerdir. Sistem girişi sayfasında "Kullanıcı Adı" ile istenen kısma kişisel bilgilerini girdiği sırada belirlediği kullanıcı adını yazdığı esnada dinamik olarak şifre belirleme aşamalarında gösterilen birinci resim ekrana gelecektir.



Şekil 3-5 PCCP Parola Giriş Ekranı

451x331 piksel resim boyutu, 19x19 piksel tolerans değeri ve 3 tıklama işlemiyle oluşturulan şifrenin entropi değeri aşağıdaki formülle bulunabilir.

$$[\frac{451x331}{19^2}]^3 \cong 2^{27} \qquad (1)$$

Bu sonuca göre PCCP yönteminden de oluşan şifrenin entropi değeri 27 bittir.

3.2.1.3 Metodoloji

Yukarıda listelenen hipotezleri test etmek ve gridWord'ü PCCP ile karşılaştırmak için toplamda 18 katılımcı ile gerçekleştirilen bir laboratuvar deneyi yapılmıştır.

Katılımcıların hepsi TOBB Ekonomi ve Teknoloji Üniversitesi öğrencileri olup, 2011 yaz döneminde BIL461 İşletim Sistemleri dersini alan öğrencilerden oluşmaktadır. Deney tasarımı olarak katılımcılar arası (between-participant) bir tasarım şekli seçildi. Bu deney tasarımının avantajları:

- Birden fazla değişken veya bir değişkenin birden fazla seviyesi aynı anda karşılaştırılmalı olarak test edilebilir.
- Zaman sorunu ortadan kaldırabilmektedir.

Dezavantajları:

- Anlamlı veriler elde edebilmek için çok fazla sayıda kullanıcıya ihtiyaç duyulmaktadır.
- Test grupları arasındaki farklılıkların, test edilen nesne/sistem üzerindeki etkisinin sonuçlara yansımasıdır.

Her iki sistemden gridWord 3 kelime ile PCCP ise 3 adet resim ile parametrelendirilmiştir, bu sayede yaklaşık bir parola uzayı her iki sistem için ortak durumu getirilmiştir. Her iki yöntemde üzerinde Windows 7 çalışan 1366x768 piksel çözünürlüğünde erkâna sahip bir dizüstü bilgisayarda gerçekleştirilmiştir. Katılımcılar her iki yönteminde kullanmak için laboratuvara davet edildikten sonra her katılımcının bir veya iki seferlik yöntemlere alışmak amaçlı denemeler yapmasına izin verilmiştir. Daha sonra kullanıcılardan 1 saat içerinde kendilerinden kullanılması istenilen yöntem ile (gridWord veya PCCP) oluştura bildikleri kadar hesap oluşturmaları istenilmiştir. Her iki yöntem için de katılımcıların izlemesi gereken 5 adım vardır. gridWord için tamamlanması gereken 5 adım:

1. Parola Oluşturma: Katılımcılar isim, soy isim ve kullanıcı adını girdikten sonra “Parola Oluştur” düğmesine basarak bir sonraki ekrana geçmektedirler. Bu ekranda sistem tarafından rastgele atanmış 3 kelime üst kısımdaki açılır kutularda belirmekte ve bu kelimelere denk gelen tuval üzerindeki hücrelerin renkleri değiştirilerek seçilmiş oldukları belirtilmektedir. Kullanıcı isterse sistem tarafından atanan bu parolayı değiştirmek için “Parola Değiştir” düğmesini kullanabilmektedir. Bu adimi bitirmek için kullanıcının “Parolamı Onayla” düğmesine tıklaması gerekmektedir.

2. Parola Onaylama: Bu adam da katılımcılardan bir önceki adımda oluşturdukları parolalarını ayni sıra ile girerek onaylamaları istenilmektedir. Kullanıcı parolasını 3 farklı şekilde gire bilmektedir (i) üst kısımda yer alan açılır kutuları kullanarak, (ii) tuval üzerindeki uygun hücreleri tıklayarak veya (iii) bu iki yöntemi melez bir şekilde kullanarak.
3. Anket: Katılımcıdan kullandığı parola yöntemi ile alakalı olarak iki tane çoktan seçmeli soruyu yanıtlaması beklenmektedir.
4. Zihinsel Test (Mental Rotation Test - MRT): Katılımcıların çalışan görsel hafızalarını sıfırlamak amaçlı MRT yapbozunu çözmeleri istenilmektedir.
5. Parola Girişi: Katılımcılardan oluşturdukları parolaları ile sisteme giriş yapmaları istenilmektedir. Parola onaylama adımının aynisidir.

PCCP için tamamlanması gereken 5 adım:

1. Parola Oluşturma: gridWord de olduğu gibi kullanıcılar kişisel bilgilerini girdikten sonra "Parola Oluştur" düğmesine basarak bir sonraki ekrana geçmektedirler. Bu ekranda (Şekil 3-3) kullanıcıdan resim üzerindeki görüntü kapısının içinde kalan bir noktaya tıklaması istenilmekte ve tıklanan noktaya bağlı olarak yeni bir resim belirmektedir. Katılımcı isterse "Değiştir" düğmesine tıklayarak görüntü kapısının yerini değiştirebilir.
2. Parola Onaylama: Bu adımda katılımcıdan bir önceki adımda oluşturduğu parolasını tekrar girerek onaylaması beklenmektedir. Fakat bu sefer resim üzerinde görüntü kapısının yer almayacaktır, katılımcı orijinal noktayı merkezine alan 19x19 piksellik yanılma payı ile tıklama yapmak zorundadır.
3. Anket: Katılımcıdan kullandığı parola yöntemi ile alakalı olarak iki tane çoktan seçmeli soruyu yanıtlaması beklenmektedir.
4. Zihinsel Test (Mental Rotation Test - MRT): Katılımcıların çalışan görsel hafızalarını sıfırlamak amaçlı MRT yapbozunu çözmeleri istenilmektedir.
5. Parola Girişi: Katılımcılardan oluşturdukları parolaları ile sisteme giriş yapmaları istenilmektedir. Parola onaylama adımının aynisidir.

3.3 Öncü Çalışmanın Sonuçları

Öncü çalışmanın birinci hipotezi olan gridWord'ün başarım oranları PCCP'nin başarım oranlarından daha yüksek olacaktır kısmen desteklenmiştir. gridWord'de parola oluşturma adımı PCCP'nin parola oluşturma adımından farklılık göstermektedir: gridWord'de kullanıcılar kendilerine önerilen parolayı sadece kabul edebilmektedirler fakat PCCP'de kullanıcılar kendilerine gösterilen görüntü kapısı yardımı ile kendileri tıklayarak seçmektedirler. Bu yüzden PCCP'de kullanıcılar parolalarını girmeden önce gridWord'e kıyasla bir kez daha fazla ara yüzü kullanmış olmalarının bu hipotez üzerinde etkisi olduğunu düşünmekteyim. İkinci hipotez olan gridWord'ün parola giriş süreleri PCCP'nin parola giriş sürelerinden daha kısa olacaktır desteklenmemiştir.

4 ÖNERİLEN YÖNTEM (gridWordX)

Bu tez kapsamında geliştirilmiş olan gridWordX yönteminden. Bu yöntem doğrultusunda ileri sürülen hipotezlerden ve bu hipotezlerin doğruluğunu kanıtlamak için yapılmış olan kullanıcı çalışmalarından bahsedilecektir. Ayrıca önerilen yöntemin geliştirilme aşamalarından ve teknik detaylarına da değinilecektir.

4.1 Yeni Sürüm: gridWordX

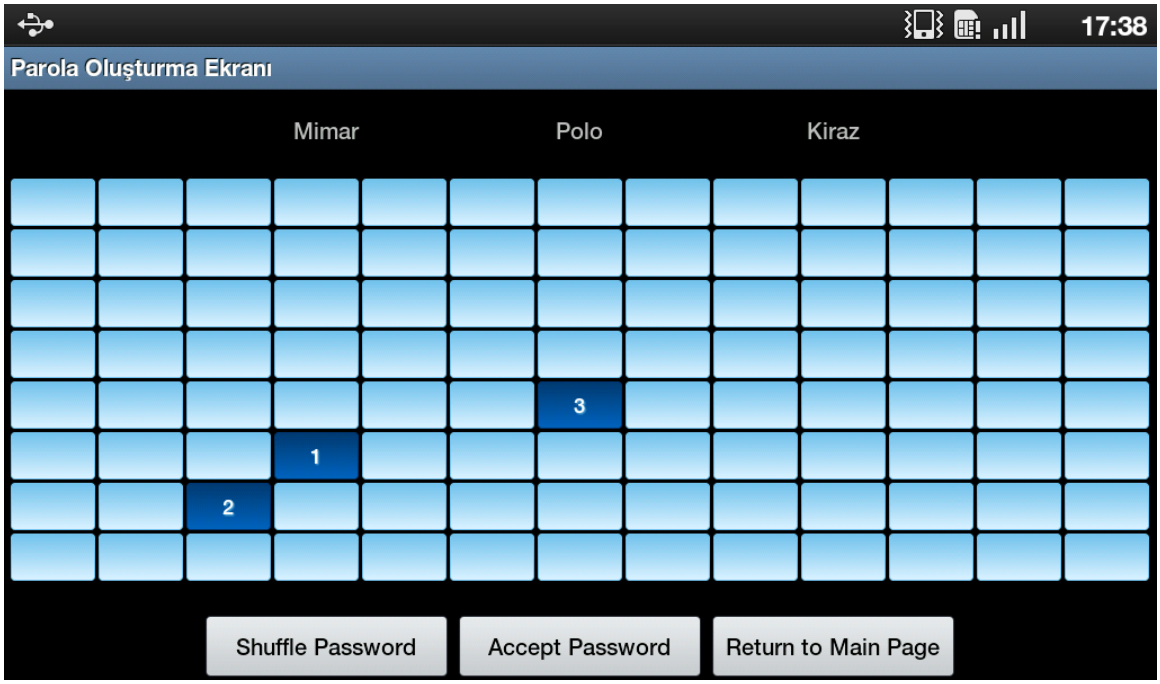
Pilot çalışmadan elde edilen verilere göre kullanışlılığını artırabilmek için tuval üzerindeki hücre sayısını düşürmeye karar verdik. Toplamda 400 (16 satır ve 25 sütun) olan hücre sayısı (kelime sayısı) 104 e düşürüldü (8 satır ve 13 sütun). Tuvalin boyutlarını sabit tutmak ve dokunmatik ekranlarda kolaylık sağlayabilmek için hücrelerin boyutu yaklaşık olarak 4 katına çıkartıldı. Hücre sayısını düşürmek şüphesiz ki güvenlik açısından zafiyete sebep olacak fakat burada alınması gereken karar güvenlikten verilecek olan taviz ile kullanışlılık açısından yapılacak olan faydanın birbirini en uygun şekilde dengelemesidir. Bir diğer değişiklikte hücreler ile eşleştirilen somut kelimelerin hücrelerin üzerinde etiketlendirme olarak yazılmasıdır ve bu kelimeler alfabetik olarak sıralanmış şekilde hücrelere atandılar. Hücreleri

somut kelimeler ile etiketlendirmek gridWordX'i tanımaya dayalı kimlik doğrulama yöntemleri sınıfına dâhil etmektedir [3].

4.1.1 Geliştirme Süreci ve Parametrelendirme

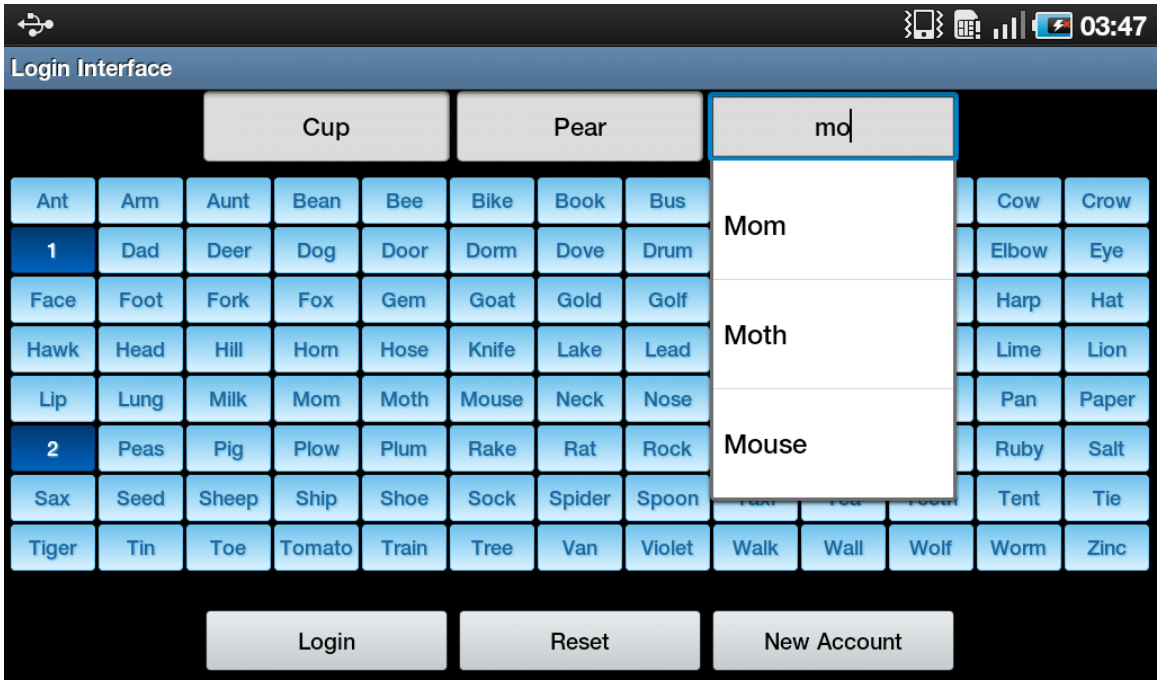
gridWordX, yapılan kullanıcı deneyleri kapsamında iki farklı platform için gerçekleştirilmiştir. İlk olarak akıllı telefonlarda kullanacak olan yöntemler için (metin tabanlı parolalar ve gridWordX) uygulamalar geliştirilmiştir. Akıllı telefon olarak Android işletim sistemi tabanlı bir telefon kullanılacağı için uygulamalar Java programla dili ve Android Development Tools kullanılmıştır. Geliştirme ortamı olarak Google tarafından resmi olarak önerilen Eclipse düzenleme programı kullanıldı. Şekil 4.1 ve Şekil 4.2 de gridWordX'in parola oluşturma ekranları görülmektedir.

Şekil 4-1 gridWordX Parola Oluşturma Ekranı 1



Şekil 4-2 gridWordX Parola Oluşturma Ekranı 2

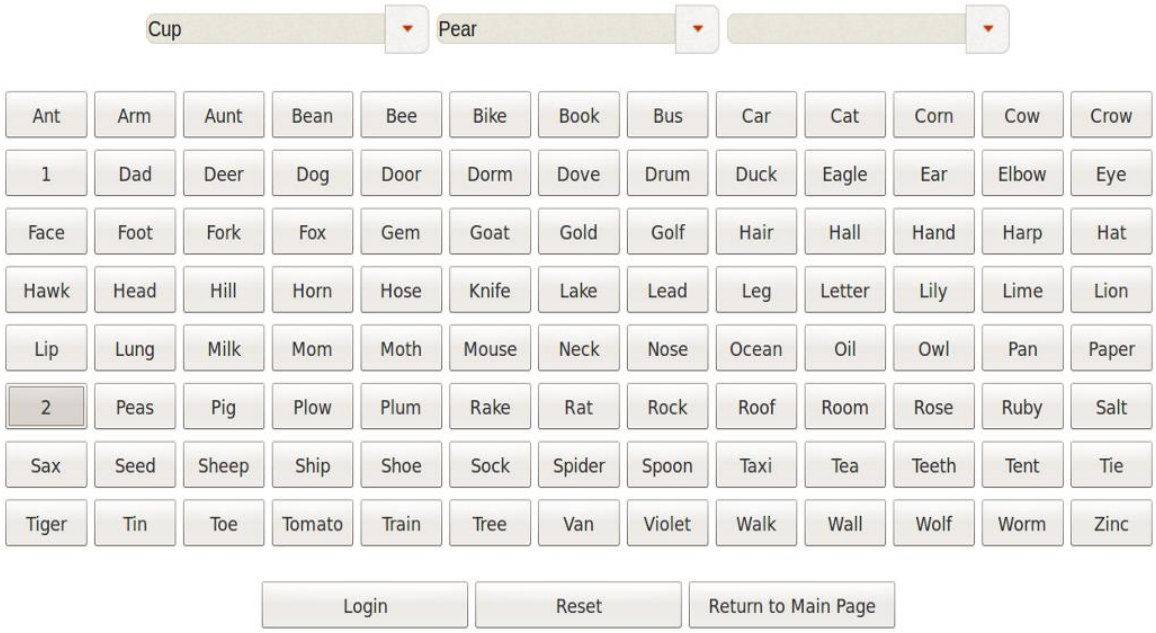
gridWordX'in parola giriş ekranı ise Şekil 4.3 de görülmektedir.



Şekil 4-3 gridWordX Parola Giriş Ekranı

Masaüstü bilgisayarlar için gridWordX ve metin tabanlı parola yöntemlerinin internet ortamında çalışan benzer versiyonları geliştirilmiştir. Bu geliştirme sürecinde kullanılan teknolojiler ise PHP, JavaScript ve HTML olmuştur. Şekil 4.4 de gridWordX'in internet üzerinde çalışan versiyonunun görüntü yer almaktadır.

gridWordX için seçilecek olan kelime uzunluğu 3 olarak atanmış bu sayede 104 adet hücre ile yöntemin entropi seviye yaklaşık olarak 20 bit civarlarında olmuştur ($104*103*102 = 1092624 \cong 2^{20}$). Metin tabanlı parolalarda da ayni seviyede entropi düzeyini yakalamak için NIST'in önerdiği formüle göre bir tanım yapıldı. Katılımcılardan en az 8 karakterli bir parola oluşturmaları istenildi (NIST'in formülüne göre 8 karakterli insanlar tarafından üretilen bir parolanın entropi değer 18 bittir). Kullanışlı güvenlik alanındaki akademik çalışmalara katkıda bulunmak için bütün uygulamaların kaynak kodları erişime açıktır [58].



Şekil 4-4 gridWordX'in Internet Ortamında Çalışan Versiyonu

4.1.2 Hipotezler

Pilot çalışma bittikten ve ara yüzlerdeki değişiklikler yapıldıktan sonra daha ayrıntılı ve düzgün bir kullanıcı deneyi gerçekleştirilmiştir. Bu tez kapsamında gridWordX'in kullanışlılığını test ettiğimizi hatırlayarak hipotezlerimize bakalım:

1. Mobil cihazlar üzerinde gridWordX'in parola giriş süreleri metin tabanlı parolaların giriş sürelerinden daha kısa sürecektir.
2. Masaüstü bilgisayarlarda gridWordX parola giriş suresi olarak metin tabanlı parolalar ile benzer/yaklaşık sonuçlar verecektir.
3. Mobile cihazlarda kullanıcıların çoğunluğu parolalarını girmek için tuval üzerine tıklamayı tercih edeceklerdir.
4. Masaüstü bilgisayarlarda kullanıcıların çoğunluğu parolalarını girmek için açılır kutuları (klavye ile girmeyi) tercih edeceklerdir.

Son iki hipotezin eklenmesindeki temel sebep, dokunmatik ekranlarda sanal klavye yerine hücrelerin kullanılmasının gridWordX'in temel farkı olacağının düşünülmesidir. Bu varsayım yapılan pilot çalışma sonucunda ortaya çıkmıştır.

Çalışma 33 gönüllünün katilimi ile gerçekleştirilmiştir. Bütün katılımcılar pilot çalışmada olduğu gibi TOBB Ekonomi ve Teknoloji Üniversitesi öğrencileridir ve herkes en az temel seviyede bilgisayar ve mobil cihaz kullanıcısıdır. Katılımcıların yaşları 18 ile 29 arasında değişmektedir. Gerçekleştirilen deneylerde konu içinde (within-subject) metodu kullanıldı bu metodun seçilmesinde ki temel sebep iki ayrı yöntem karşılaştırırken gruplar arasındaki farklılıkların deney sonuçları üzerinde etkiye sahip olamamasını sağlamaktı.

Deneyler, laboratuvar tabanlı ve web tabanlı çalışmalar olarak iki farklı şekilde gerçekleştirilmiştir.

4.1.3 Laboratuvar Çalışması

Laboratuvar çalışmasında her katılımcı iki tane kişisel oturumu tamamlamıştır. Bu iki oturum arasında üç haftalık bir ara verildi ve bu arada web tabanlı deneyler

gerçekleştirildi. Katılımcılar ilk oturumu gerçekleştirmeden önce kendilerine sözel olarak bazı bilgilendirmeler yapılmıştır:

- Deneyi gerçek hayattaki gibi ciddi bir şekilde yapmalısınız. Parolalarınız önemli bir hesabi koruyormuş gibi davranmalısın.
- Metin tabanlı parolalarınız en az 8 karakterden oluşmalıdır.
- Daha önceden kullandığınız metin tabanlı parolaları kullanmamalısınız.
- Parolalarınızı herhangi bir yere not etmemelisiniz.

Ayrıca kullanıcıları mümkün olduğu kadar rahat etmeleri ve deneyde ortamını normal koşullar gibi yapmak için deneyin amaçlarında katılımcıları test etmek gibi bir olgu olmadığını bu konuda rahat hissetmeli gerektiğini vurguladık ve tek amacın yöntemleri test etmek olduğunu söyledik.

Bu laboratuvar çalışmasının temel amacı gridWordX'in değerlendirilmesini yapmaktı özellikle cihaza giriş olanakları kısıtlı olduğu zamanlar için (fiziksel klavye yerine dokunmatik ekranlardaki gibi sanal klavyelerin kullanıldığı zamanlar gibi). Mobil cihazlar için geliştirilen uygulamalar Samsung Galaxy TAB üzerinde çalıştırılarak katılımcılardan kullanmaları istenildi. Her katılımcının kendi (eğer uygun ise) mobil cihazını kullanılmamasının sebebi ise farklılık gösteren erkân boyutlarının elde edilecek olan sonuçlar üzerinde istenilmeyen farklılıklara sebep olmasıydı. Samsung Galaxy TAB'in teknik özellikleri şunlardır; 600x1024 piksellik çözünürlük, 7 inç ekran boyutu ve 170 dpi. Her iki uygulamada tam ekran olarak çalıştırılmıştır.

Laboratuvar çalışması üç adımdan oluşmaktadır. Bu üç adim her iki yöntem (gridWordX ve metin tabanlı parolalar) içinde ayni olduğundan burada sadece gridWordX için anlatılmıştır.

1. Parola Oluşturma ve Onaylama: Katılımcılar ad, soyadı ve kullanıcı adlarını girdikten sonra "Parola Oluştur" düğmesine basarak bir sonraki ekrana

geçeklerdir. Bu ekranda katılımcılara sistem tarafından atanmış olan üç kelime uygulamanın üst kısmındaki açılır kutularda yer almaktadır ve kelimeler ile eşleştirilmiş olan hücrelere tuval üzerinde renklendirilmiş ve sadece bu hücrelerin üzerine kelimeler etiketlenmiştir (Şekil 4-2 gridWordX Parola Oluşturma Ekranı 2). Eğer kullanıcı kendisine atanan paroladan memnun değil ise "Değiştir" düğmesine basarak farklı bir parola isteyebilmektedir fakat yeni parolada sistem tarafından rastgele olarak atanmaktadır. "Parolayı Onayla" düğmesine basıldıktan sonra katılımcılardan bir önceki adımda kendilerine atanan parolalarını onaylamalarını isteyen bir ekran gelmektedir. Bu ekranda kullanıcılar parolalarını girmeleri gerekmektedir, parolalarını isterlerse açılır kutular yardımı ile isterler ise tuval üzerindeki hücreleri tıklayarak veya iki giriş şeklini melez olarak kullanmak şekli ile parolalarını onaylayabilirler. Parolaların katılımcıya atandığı sıra ile girilmesi önelidir aksi takdirde yanlış olarak değerlendirilir.

2. Zihinsel Test (Mental Rotation Test - MRT): Katılımcıların çalışan görsel hafızalarını sıfırlamak amaçlı MRT yapbozunu çözmeleri istenilmektedir.
3. Parola Girişi: Katılımcıların parolalarını girmeleri gereken kişimdir ve parola onaylama adimi ile ayni şekilde çalışmaktadır.

4.1.4 Web Çalışması

Web çalışmasının temelinde gridWordX'in performans ve kullanışlılığını klasik masaüstü cihazlarda test etmek ve sonuçları metin tabanlı parolaların sonuçları ile karşılaştırmaktır. Ayrıca gridWordX'in katılımcıların kendi ev ortamlarında kullanırken oluşacak olan performanslarını izlemek de diğer sebeptir. Bu web çalışması da laboratuvar çalışması gibi iki oturumdan oluşmaktadır. Oturumlar arası bir haftalık bir süreç ile ayrılmıştır ve iki oturumda araya başka bir çalışma girmeden art arda yapılmıştır. Web çalışmasının ilk ayağı laboratuvar çalışmasından bir hafta sonra gerçekleşmiş ve kullanıcılar elektronik posta yolu ile yaklaşan çalışma tarihi hakkında bilgilendirilmişlerdir.

Katılımcılar kendilerinden ziyaret etmeleri istenilen internet sitesine gittikleri zaman mobil cihazlarda gördükleri ara yüze benzer bir ara yüz ile karşılaşmışlardır (Şekil 4-4 gridWordX'in Internet Ortamında Çalışan Versiyonu). Eğer kullanıcılar parolalarını 3 seferden fazla olarak yanlış girerler ise sistem kendilerine elektronik posta yolu isle şifrelerini hatırlamak isteyip istemediklerini sormaktadır.

Bu adımdan bir hafta sonra katılımcılardan ayni internet sayfasını ziyaret ederek bir hafta önceki işlemleri tekrarlamaları istenilmiştir. Katılımcılar yine elektronik posta yolu ile bu süreç hakkında bilgilendirilmeye devam edilmiştir.

5 KULLANILABİLİRLİK ÇALIŞMASI

Bu kısım da önerilen yöntem ve karşılaştırılmada kuşanılacak olan yöntemleri bilimsel olarak karşılaştırabilmek için yapılan kullanıcı çalışmalarından bahsedilecektir. Aşağıda bahsedilen alt başlıklar şöyle sıralanmaktadır: (i) çalışma sırasında katılımcılardan toplanan veriler, (ii) toplanan verilerin sonuçları, (iii) sonuçlar üzerinde tartışma ve (iv) güvenlik analizi.

5.1 Toplanan Veriler

Toplanan veriler zaman ve başarım oranları, parola değiştirme sayıları, parola giriş yöntemi ve anketten oluşmaktadır.

5.1.1 Zaman ve Başarım Oranları

Metin tabanlı parolalar ve gridWordX için parola oluşturma ve onaylama süreçleri için zaman değerleri toplanmıştır. Pilot çalışmada toplam zamanın yani sıra tıklama zamanı olarak belirtilen kullanıcının tuval üzerinde ki ilk tıklamasıyla son tıklaması arasındaki gecen sureyi gösteren zaman bu çalışmada toplanamamıştır. Çünkü pilot çalışmada gridWord, PCCP ile karşılaştırılmışken (her iki yöntem içinde tıklama söz konusudur) bu çalışmada metin tabanlı parolalar için böyle bir parametre kullanılamamaktadır.

Toplam zaman olarak nitelendirilen süreç katılımcının parola ekranını ilk gördüğü andan parola girişine son verdiği eyleme (düğmeye tıklama veya son hücreyi seçme) kadar gecen suredir. Metin tabanlı parolalar için parola oluşturma ve onaylama adımları ayni ekran üzerinde yapılırken, gridWordX için bu iki adim ayrı fakat ardışık ekranlarda yapılmaktadır. Bu yüzden gridWordX'in toplam zamanı bu iki ekranda gecen surelerin toplamı olarak hesaplanmıştır.

Toplam zaman sadece parolalarını başarılı bir şekilde girebilen katılımcılar için değerlendirilmeye alınmıştır. Eğer bir parola girme girişimi 3 den daha az girişimde tamamlanmış ve bastan başlatılmamış ise başarılı olarak adlandırılmakta ve

değerlendirilmeye katılmaktadır. Her toplam zaman o ana kadar yapılan başarısız girişimlerde gecen süreleri de içermektedir.

Başarılı bir şekilde yapılan girişimlerin toplam girişimlere oranı başarım oranı olarak ölçülendirilmiştir. Başarım oranları parola oluşturma, onaylama ve girişi adımları için ayrı toplanmıştır.

5.1.2 Parola Değiştirme Sayısı

Parola oluşturma sırasında katılımcıların "Değiştir" düğmesini kullanma sayıları, gridWordX'in başarım oranları üzerindeki etkisini ölçmek için toplanmıştır.

5.1.3 Parola Giriş Yöntemi

Daha önce bahsedildiği gibi gridWordX de 3 farklı parola giriş yöntemi mevcuttur. Bunlar, üst kısımda yer alan açılır kutular ile parolanızı sanal klavye veya tam boyutlu fiziksel klavye ile yazmak, tuval üzerindeki hücreleri seçerek girmek veya bu iki yöntemi ortak kullanmak. Yapılan laboratuvar ve web çalışmaların bu 3 yöntemin kullanılma sayılarının başarım oranları ve zamanlar üzerindeki etkisi ölçülmek için kayıt edilmiştir.

5.1.4 Anket

Katılımcılar hakkında bilgi toplamak için demografik bir anket uygulanmıştır ayrıca ankette katılımcıların gridWordX hakkındaki izlenimlerini değerlendirmek için yöntemle alakalı bazı sorularda yer almaktadır.

5.2 Verilerin Sonuçları

Önceki başlık altında çalışma sırasında toplanan verilerden bahsedilmişti bu başlık altında ise elde edilen bu verilerin ne anlama geldiklerinden bahsedilecektir.

5.2.1 Zaman ve Başarım Oranları

Şekil 5-1 Parola Oluşturma ve Onaylama Zamanları gridWordX ve metin tabanlı parolaların laboratuvar ve web ortamındaki surelerini göstermektedir. Laboratuvar ve web çalışmaları için zamanlar toplanmış ve bir şekil olarak gösterilmiştir. Şekil 5-2

Parola Girişi – Laboratuvar Çalışması ve Şekil 5-3 Parola Girişi – Web Çalışması gridWordX ve metin tabanlı parolalar için laboratuvar ve web çalışmalarında parola girişi adımdaki sureleri göstermektedirler. Laboratuvar ve web çalışmalarının her ikisinin de ikişer adımdan oluştuğunu hatırlatarak şekillerdeki sunum yönteminin bu iki adimi birleştirerek yapıldığına dikkat edilmelidir.

Mobil cihazlarda (laboratuvar çalışmasında) metin tabanlı parolalar ile gridWordX'in parola giriş sureleri arasında istatistiksel olarak anlamlı bir fark bulunmuştur. Bu iki yöntemi istatistiksel olarak karşılaştırmak için paired-sample Wilcoxon testi kullanılmıştır. Eğer sonuçlarımız normal bir dağılım göstermiş olsaydılar paired-sample T-test kullanılabilecekti. Paired-sample Wilcoxon, T-test gibi verilerin normal olarak dağılım var sayarak bir değerlendirme yapmadığı için T-test'e tercih edilmiştir. (ilk parola girişi: V=56, p=0,000014 son parola girişi: V=429, p=0,001437). Bu istatistiksel sonuçları göz önüne alarak birinci hipotezimizin tam olarak desteklendiğini söyleyebiliriz.

Çizelge 5.1 gridWordX ve Metin Tabanlı Parola Başarım Oranları

	Oluşturma ve Onaylama	Parola Girişi 1	Parola Girişi 2	Parola Girişi 3	Parola Girişi 4
gridWordX Başarım Oranı	33/33 %100	33/33 %100	22/33 %66.67	33/33 %100	32/33 %96.97
Metin Parolalar Başarım Oranı	33/33 %100	33/33 %100	26/33 %78.79	33/33 %100	33/33 %100

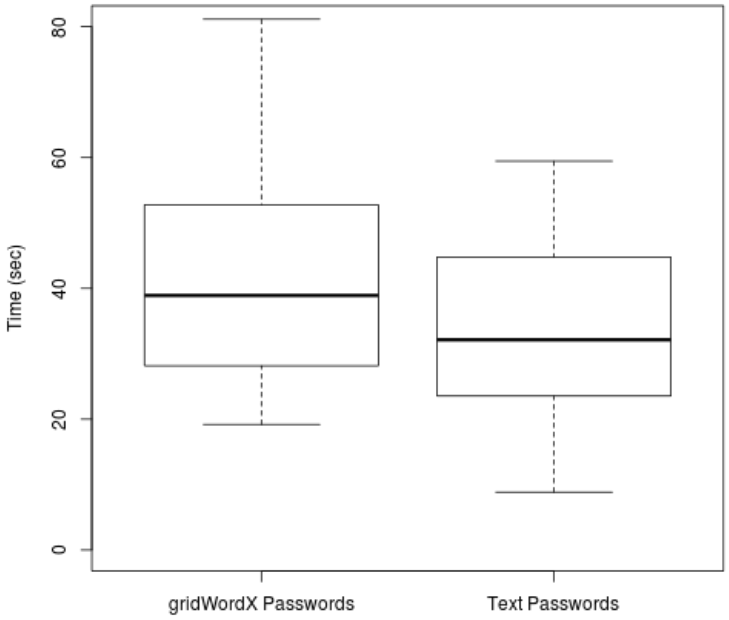
Çizelge 5.1 de gridWordX ve metin tabanlı parolaların bütün laboratuvar ve web çalışmalarındaki başarım oranları verilmiştir. Görüldüğü gibi gridWordX'in başarım oranları sadece web çalışmasının ilk adımında ve laboratuvar çalışmasının son adımında metin tabanlı parolalardan düşük çıkmıştır. Fakat bu farklılık istatistiksel olarak Chi-square testi ile karşılaştırıldığı zaman herhangi bir anlamlı farklılığa rastlanmamaktadır (ikinci parola girişi: χ^2 = 1,2222, df = 1, p = 0,2689 son parola girişi: χ^2 = 1.015, df = 1, p = 0,3136).

Çizelge 5.2 Değiştirme Sayısının Başarım Üzerindeki Etkisi

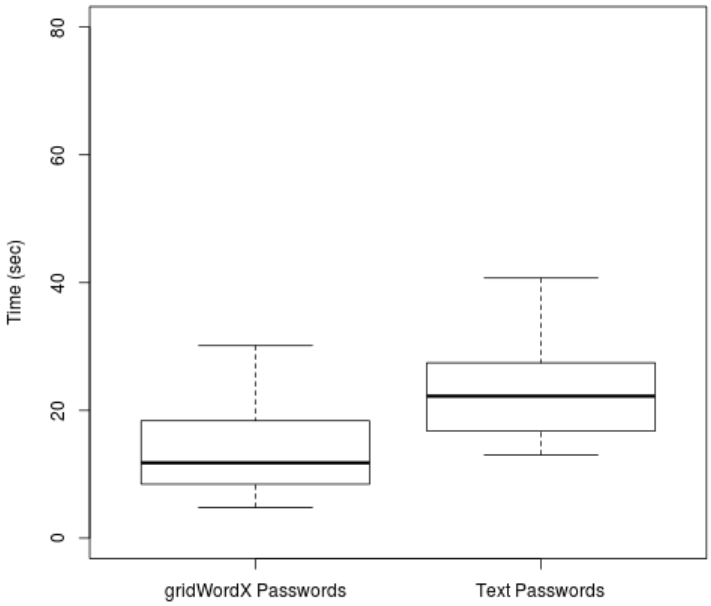
Değiştirme Sayısı	Deneme Sayısı	Onaylama Başarım O.	Parola Girişi 1	Parola Girişi 2	Parola Girişi 3	Parola Girişi 4
Düşük (0-5)	23(%69.70)	%100	%100	%65.22	%100	%95.65
Yüksek (>5)	10(%30.30)	%100	%100	%70	%100	%100

5.2.2 Parola Değiştirme Sayısı

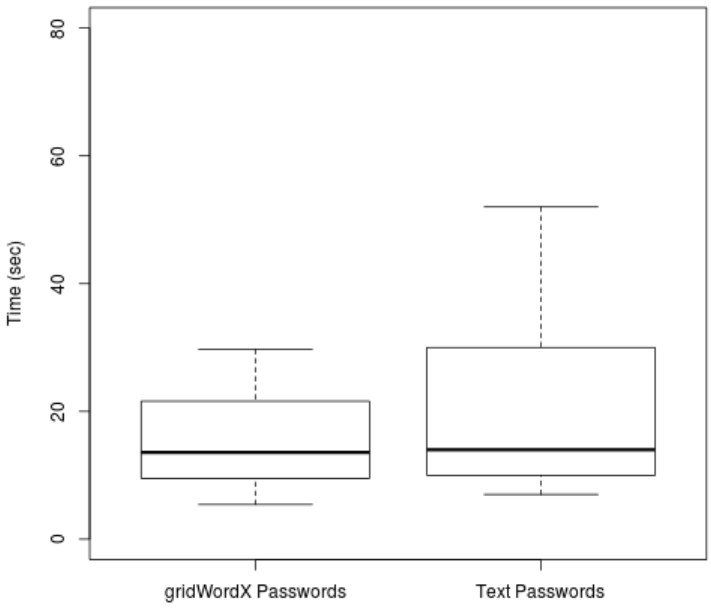
gridWordX'in ortalama parola değiştirme sayısı 5.15 ve ortanca parola değiştirme sayısı 5 dir. Çizelge 5.2 bu konuda detaylı bilgiyi içermektedir.



Şekil 5-1 Parola Oluşturma ve Onaylama Zamanları



Şekil 5-2 Parola Girişi – Laboratuvar Çalışması



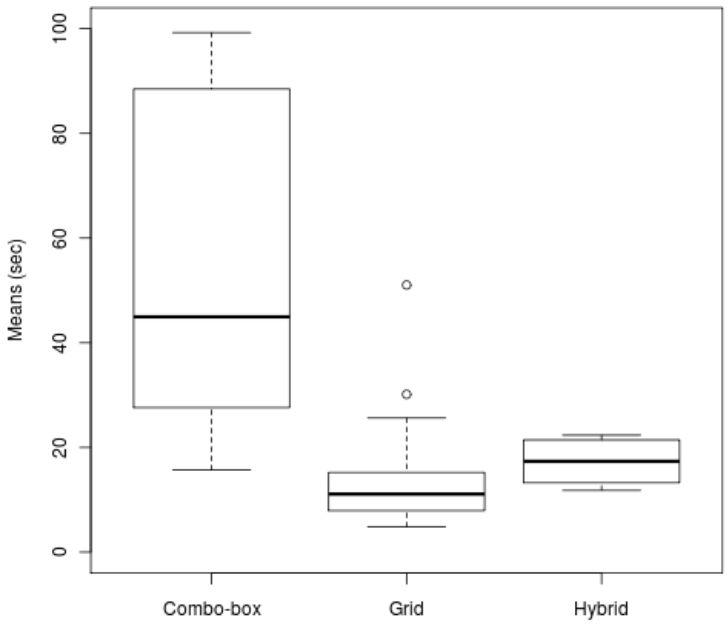
Şekil 5-3 Parola Girişi – Web Çalışması

5.2.3 Parola Giriş Yöntemi

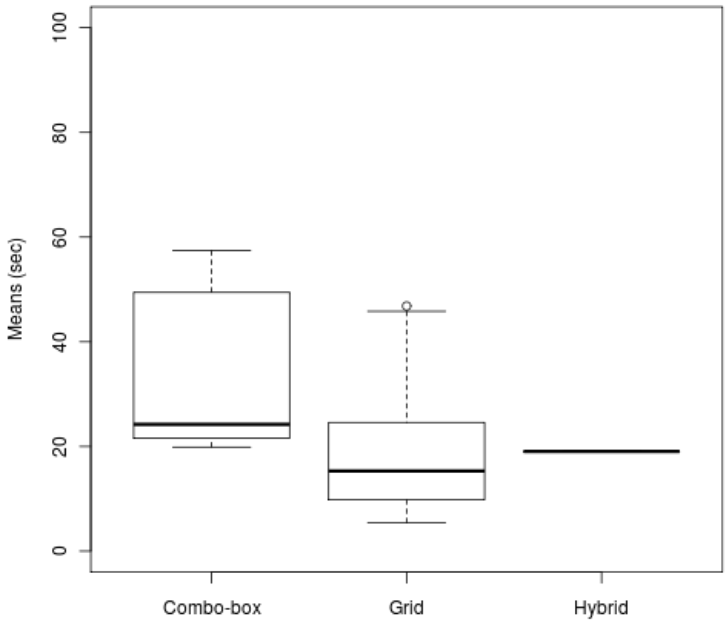
Çizelge 5.3 Parola Giriş Yöntemi Frekansları

	Oluşturma ve Onaylama	Parola Girişi 1	Parola Girişi 2	Parola Girişi 3	Parola Girişi 4
Grid	27	28	28	30	28
Açılır Kutu	4	2	1	1	3
Grid + A.K.	2	3	4	2	2

Çizelge 5.3 de görüldüğü gibi katılımcılar büyük çoğunlukla parolalarını girmek için tuval üzerindeki hücreleri kullanmayı tercih etmektedirler. Bu sonuçlar ışığında üçüncü hipotezimizin tam olarak desteklendiğini söyleyebiliriz. Ayrıca Şekil 5-4 ve Şekil 5-5 den anlaşıldığı gibi gridWordX de hücrelerin (dokunmatik ekranın) kullanımı parola girişinde büyük ölçüde zaman açısından performans artışına yol açmaktadır.



Şekil 5-4 Parola Giriş Yöntemine Göre Zaman Performansı (Laboratuvar Çalışması)



Şekil 5-5 Parola Giriş Yöntemine Göre Zaman Performansı (Web Çalışması)

5.2.4 Kullanıcı Algıları ve Görüşleri

Her katılımcıdan çalışma kapsamında gridWordX ile alakalı olarak bir anket doldurmaları istedik. Bu anket 10 sorudan oluşmakta ve her soru 10'luk bir puanlandırma sistemi ile cevaplandırıldı. Bu puanlama sisteminde 1 kesinlikle katılmıyorum anlamına gelirken, 10 kesinlikle katılıyorum anlamına gelmektedir.

Genel olarak anket sonuçlarına göre katılımcıların gridWordX'e karşı olan tutumları oldukça olumluydu. Katılımcılar, gridWordX'i parola oluşturması kolay, kullanımı hem mobil cihazlar hem de masaüstü bilgisayarlar için kolay ve en az metin tabanlı parolalar kadar güvenli bulmuşlardır. Çalışmaya başlamadan önce katılımcılara yapılan bilgilendirme aşamasında deneyin sağlığı için katılımcılardan metin tabanlı parolalarını oluştururken daha önce kullandıkları parolalarını kullanmamaları istenmişti. Fakat anket sonuçlarından anlaşıldığı üzere 33 katılımcıdan 16'si daha

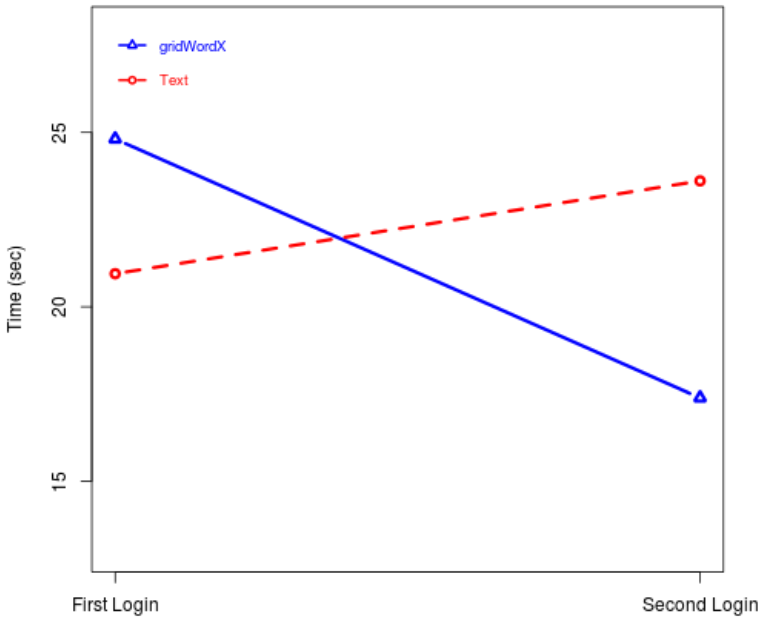
önce kullandıkları parolalarının aynisini veya benzer bir şeklini kullandıklarını belirtmişlerdir.

5.3 Tartışma

Birinci hipotezimiz olan "Mobil cihazlar üzerinde gridWordX'in parola giriş süreleri metin tabanlı parolaların giriş sürelerinden daha kısa sürecektir" yapılan kullanıcı çalışmalarına göre tam olarak desteklenmiştir. Çalışmalar sunu göstermiştir ki kullanıcılar mobile cihazlarda gridWordX'i kullanırken metin tabanlı parolalara oranla istatistiksel olarak anlam taşıyacak derecede hızlılar.

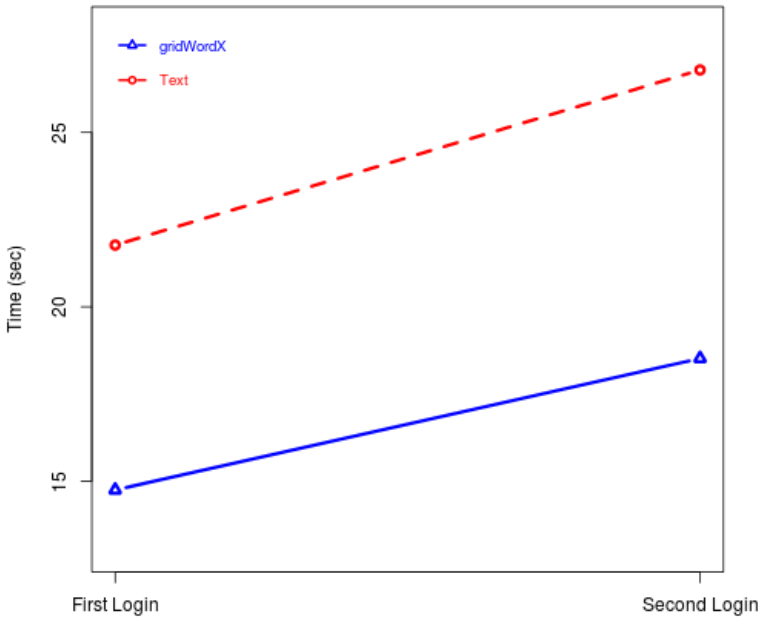
İkinci hipotezimiz olan "Masaüstü bilgisayarlarda gridWordX parola giriş suresi olarak metin tabanlı parolalar ile benzer/yaklaşık sonuçlar verecektir" da birinci hipotezimiz gibi tam olarak desteklenmiştir. Burada ki sonuçları açmak gerekirse masaüstü bilgisayarlarda gridWordX metin tabanlı parolalardan çok küçük bir seviyede yavaştır fakat bu fark istatistiksel olarak bir anlam ifade etmediği için ikinci hipotezimiz de desteklenmiştir.

Parola giriş surelerini biraz daha dikkatli incelersek görünüyor ki, gridWordX'in masaüstü cihazlardaki parola giriş suresi ikinci kullanımda birincisine oranla daha azdır. Bu farkın gerçekliliği konusunda her ne kadar emin olamasak da, eğer doğru ise, katılımcıların gridWordX'i ilk kullanımlarında ara yüz ve kullanım şekli ile kazandıkları aşinalık ikinci kullanımda daha hızlı olmalarını sağlamıştır (Şekil 5-6).



Şekil 5-6 Masaüstü Parola Giriş Süreleri

Şekil 5-7 de mobil cihazları kullanırken elde edilen parola giriş sureleri verilmiştir. Bu şekilden de görüldüğü gibi her iki yönteminde parola giriş süreleri artmaktadır. Bu artısın sebebi katılımcıların ilk hafta parolalarını girmeden önce parolalarını oluşturmak onaylamak için her iki yöntemi de mobil cihazlar üzerinde kullanarak parola giriş için kazandıkları aşinalığın, mobil cihazlarda ikinci parola girişi için olmamasından kaynaklandığını tahmin etmekteyiz (Şekil 5-7).



Şekil 5-7 Mobil Cihaz Parola Giriş Süreleri

Üçüncü hipotezimiz olan "Mobile cihazlarda kullanıcıların çoğunluğu parolalarını girmek için tuval üzerine tıklamayı tercih edeceklerdir" tam olarak desteklendiğini Çizelge 5.3 deki veriler açık bir şekilde göstermektedir.

Dördüncü ve son hipotezimiz olan "Masaüstü bilgisayarlarda kullanıcıların çoğunluğu parolalarını girmek için açılır kutuları (klavye ile girmeyi) tercih edeceklerdir" tahminlerimizin tersine olarak elde ettiğimiz veriler tarafından desteklenmemiştir. Katılımcılar gridWordX'i hangi platformda (mobil cihazlar veya masaüstü bilgisayarlar) kullanıldıklarına bakılmaksızın, gridWordX'in grafiksel parola özelliği olan hücrelerini kullanmayı tercih etmişlerdir. Katılımcıların bu davranışı pilot çalışmamızda gözlemlediğimiz sonuçlara uyum göstermemektedir. Çünkü daha öncede bahsedildiği gibi pilot çalışmada katılımcıların büyük çoğunluğu parolalarını klavye kullanarak açılır kutulardan girmişlerdi. Bu davranış değişiminin başlıca iki sebepten kaynaklanabileceğinin kanısındayım. Öncelikle, gridWordX'in ara yüzünde yapılan iyileştirmeler uygulamanın kullanımını daha kolay hale getirmiş

olması ve pilot çalışmanın aksine bu çalışmada katılımcılara ilk olarak mobil cihazlarda denemeler yapılmasının istenilmesi bir sebep olabilir. Diğer sebep ise, katılımcıların tercihleri olabilir. Çalışmanın kapsamının küçüklüğü sebebiyle bu konuda net bir kanıya varabilmek şimdilik mümkün görünmemektedir.

Hipotezlerle alakalı olan sonuçların yani sıra gözlemlenen diğer sonuçlarda su şekildedir.

Çizelge 5.1 den de anlaşıldığı gibi her ne kadar istatistiksel olarak anlamlı olmasa da gridWordX'in başarım oranları metin tabanlı parolalardan çok küçük bir fark ile daha düşüktür. Bu sonucun gözlenmesinde ki sebeplerden birisi katılımcıların gridWordX için sistem tarafından atanan ve kendilerine tamamen yeni olan bir parola kullanıyor olmalarına karşın metin tabanlı parola olarak daha önceki parolalarını veya benzer sürümlerini kullanmaları olabilir. Buna ek olarak katılımcıların metin tabanlı parolaları incelendiği zaman, bazı katılımcıların "qwertyui" gibi çok kolay parolalar kullandıklarının farkına varılmıştır. Bu tip bir parola kullanıcısının hatırlamasını oldukça kolaylaştıracağı için başarım oranlarında pozitif yönde bir etkiye sahip olacaktır (ayni durum parola giriş süreleri içinde geçerlidir). Bu duruma çözüm olarak ileride yapılacak olan muhtemel çalışmalarda gridWordX de yapıldığı gibi metin tabanlı parolalar için de sistem tarafından önerilen parolalar kullanılabilir veya katılımcıları daha güvenli parolalar seçmeleri konusunda cesaretlendiren farklı sistemler uygulanabilir.

Çizelge 5.2 den anlaşılacağı üzere katılımcıları kendilerine sistem tarafından verilen parolalarını değiştirme sayılarına göre ikiye ayırdık; 5 den fazla sayıda değiştirme yapanlar ve 5 den az sayıda değiştirme yapanlar. Daha önce grafik parolalar ile ilgi yapılan çalışmalar [57] da olduğu gibi bu çalışmada da değiştirme sayısının başarım oranı ile doğru orantılı olduğu ortaya çıkmıştır.

5.4 Güvenlik Analizi

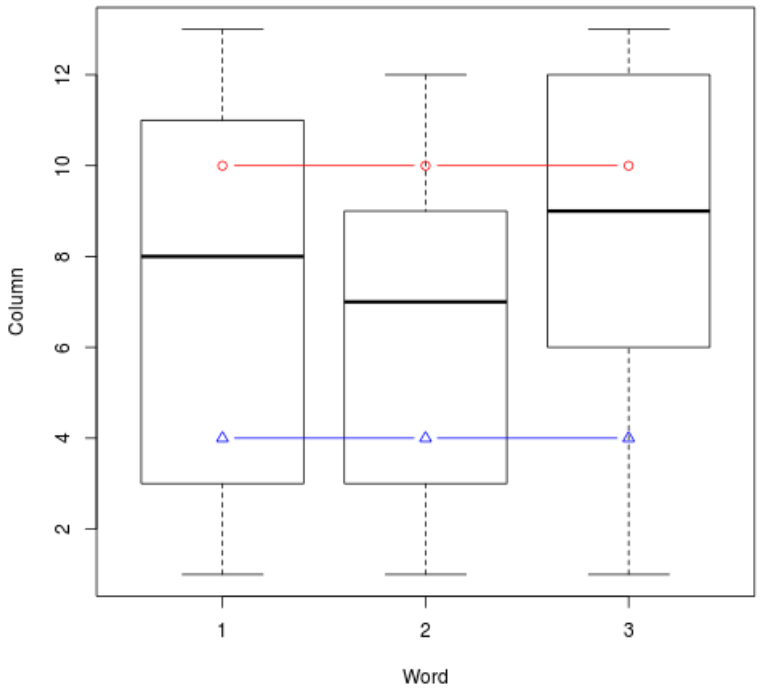
Bu başlık altında gridWordX'in güvenlik analizi yapılacaktır. gridWordX'in teorik parola uzayı daha önce de bahsedildiği gibi yaklaşık olarak 20 bittir. Fakat bu teorik parola uzayının değerini gerçek hayatta düşüren iki önemli faktör vardır; sıcak nokta (hotspots) problemi ve kullanıcıların grid üzerinde izledikleri modeller/yolar (pattern) [59]. Daha önceki çalışmalarda [57-59] kullanılmış olan teknikleri kullanarak gridWordX parolalarının güvenlik analizi gelecek olan paragrafta yapılacaktır.

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

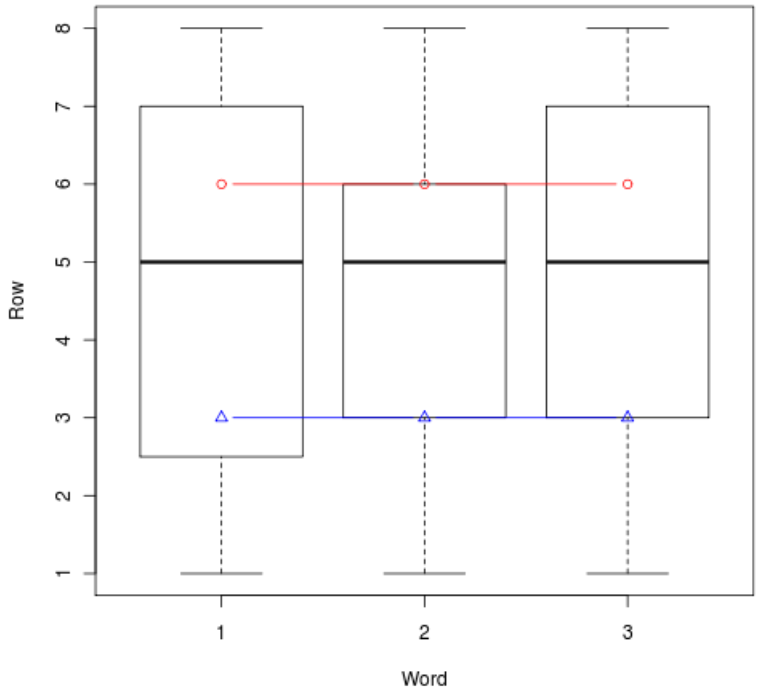
Şekil 5-8 Grid Üzerindeki Hücrelerin Seçilme Sıklıkları

gridWordX için sıcak nokta problemi kullanıcılar tarafından çoklukla seçilen hücreler (kelimeler) olarak tanımlanabilir. gridWordX de parolalar sistem tarafından rastgele atanıyor olsa da kullanıcıların parolalarını değiştirebilme seçenekleri yüzünden sıcak nokta problemi gridWordX için hala üzerinde düşünülmesi gereken bir noktadır. Şekil 5-8 de kullanıcı çalışması sonucunda her hücrenin seçilme sıklıkları gösterilmektedir. Yalnız 1 hücre 4 kere seçilmiştir ve 8 tane hücre de 3 defa seçilmiştir. Hücrelerin %36,46'sı hiç seçilmemiştir. gridWordX deki parolaların rastgele üretilmiş bir veri setinden ne derece farklılık gösterdiğini araştırmak için her biri 33 adet gridWordX parolası içeren 100 adet veri seti üretildi. Her bir parola 3 adet (x, y) çiftinden oluşmaktadır ve grid üzerindeki bir hücreye (kelimeye) denk

gelmektedir. Önceki çalışmalarda [59] yapıldığı gibi yaklaşık entropi değeri 16.88 bit olarak hesaplandı. Bu değer sahte veri kümesinin maksimum ve minimum entropi değerleri olan 17.34 ile 16.01 bitin arasında kaldığı için %1 oranıyla katılımcılardan toplanan veri kümesi şans eseri olarak oluşmuştur. Şekil 5-9 ve Şekil 5-10 da kelimelerin (hücrelerin) grid üzerindeki dağılımları gösterilmektedir. Kırmızı çizgiler sahte veri kümesinin maksimum ortanca değerini gösterirken mavi çizgiler de minimum ortanca değerini göstermektedir. Şekillerden de görüldüğü gibi gözlemlenen veri kümesinin ortanca değerleri tam olarak üretilen sahte veri kümesinin maksimum ve minimum rotanca değerlerinin içine düşmektedir. Bu sonuca dayanarak sıcak nokta probleminin gridWordX için geçerli olmadığını söylenebilir.



Şekil 5-9 Kelimelerin Satır Bazlı Dağılımı



Şekil 5-10 Kelimelerin Sütun Bazlı Dağılımı

6 SONUÇ

Parolaları sanal klavyeler aracılığı ile yazmak özellikle küçük boyutlu mobil cihazlarda zor bir durum oluşturmaktadır. Bu tez çerçevesinde önerilmiş olan gridWordX yöntemi internete erişim için kullanılan cihazların tam boyutlu fiziksel bir klavyesi olan cihazlarla olmayan cihazlar arasında sıklıkla değiştirildi durumlarda kullanıcılara parolalarını rahatlıkla girmelerini sağlayan grafiksel parolalar ile metin tabanlı parolaları melez bir şekilde kullanan yeni bir kimlik doğrulama yöntemidir. Bu yöntem çok kelimeli kimlik doğrulama yöntemlerinin üzerine inşa edilmiş olan yöntem olarak da algılanabilir.

Yapılmış olan kullanıcı çalışmaları sonucunda (laboratuvar ve web tabanlı kullanıcı çalışmaları) gridWordX'in mobil cihazlarda istatistiksel olarak anlamlı bir şekilde klasik metin tabanlı parola sistemlerinden daha kısa sürelerde kullanıcılarına sisteme giriş yapabilmelerini sağladıkları gözlenmiştir. Buna ek olarak, klasik masaüstü bilgisayarlarda gridWordX'in parola giriş süreleri metin tabanlı parolaların giriş süreleri ile oldukça yakın değerler göstermektedir. Sonuç olarak gridWordX, internete erişimin için kullanılan cihazların sıklıkla değişim gösterdiği durumlarda klasik metin tabanlı parolalara önemli bir alternatif oluşturmaktadır.

İlerde yapılacak olan çalışmalarda gridWordX'in uzun vade parola hatırlanabilirliğinin metin tabanlı parolaların hatırlanabilirlilikleri ile karşılaştırmak planlanmaktadır.

7 KAYNAKLAR

[1] C. Herley and P. Van Oorschot, "A research agenda acknowledging the persistence of passwords," Security Privacy, IEEE, vol. 10, no. 1, pp. 28 –36, jan.-feb. 2012.

[2] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: persuasive cued click-points," in Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1, ser. BCS-HCI'08. Swinton, UK, UK: British Computer Society, 2008, pp. 121–130. [Online]. Available: http: //dl.acm.org/citation.cfm?id=1531514.1531531

[3] N. Wright, A. S. Patrick, and R. Biddle, "Do you see your password?: applying recognition to textual passwords," in Proceedings of the Eighth Symposium on Usable Privacy and Security, ser. SOUPS'12. New York, NY, USA: ACM, 2012, pp. 8:1–8:14. [Online]. Available: http://doi.acm.org/10.1145/2335356.2335367

[4] S. Mackenzie, S. X. Zhang, and R. W. Soukoreff, "Text entry using soft keyboards," Behaviour and Information Technology, vol. 18, no. 4, pp. 235–244, 1999. [Online]. Available: http: //www.tandfonline.com/doi/abs/10.1080/014492999118995

[5] K. Bicakci and P. C. van Oorschot, "A multi-word password proposal (gridword) and exploring questions about science in security research and usable security evaluation," in Proceedings of the 2011 workshop on New security paradigms workshop, ser. NSPW'11. New York, NY, USA: ACM, 2011, pp. 25–36. [Online]. Available: http://doi.acm.org/10.1145/2073276.2073280

[6] R. Biddle, S. Chiasson, and van Oorschot P. C., "Graphical passwords: Learning from the first twelve years," ACM Computing Surveys 44(4), 2011.

[7] E. A. Kirkpatrick, "An experimental study of memory." Psychological Review, vol. 1, no. 6, p. 602, 1894.

[8] J. C. Yuille, Imagery, memory, and cognition: Essays in honor of Allan Paivio. Lawrence Erlbaum Assoc Incorporated, 1983.

[9] A. Paivio, T. Rogers, and P. C. Smythe, "Why are pictures easier to recall than words?" Psychonomic Science, 1968.

[10] R. N. Shepard, "Recognition memory for words, sentences, and pic-tures," Journal of verbal Learning and verbal Behavior, vol. 6, no. 1,

pp. 156–163, 1967.

[11] F. I. Craik and J. M. McDowd, “Age differences in recall and recognition.” Journal of Experimental Psychology: Learning, Memory, and Cognition, vol. 13, no. 3, p. 474, 1987.

[12] K.-P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B.-L. B. Tai, J. Cook, and E. Eugene Schultz, “Improving password security and memora- bility to protect personal and organizational information,” International Journal of Human-Computer Studies, vol. 65, no. 8, pp. 744–757, 2007.

[13] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, “Multiple password interference in text passwords and click-based graphical passwords,” in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 500–511.

[14] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, A. D. Rubin et al., “The design and analysis of graphical passwords,” in Proceedings of the 8th USENIX Security Symposium. Washington DC, 1999, pp. 1–14.

[15] P. Dunphy and J. Yan, “Do background images improve draw a secret graphical passwords?” in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 36–47.

[16] J. Goldberg, J. Hagman, and V. Sazawal, “Doodling our way to better authentication,” in CHI’02 extended abstracts on Human factors in computing systems. ACM, 2002, pp. 868–869.

[17] C. Varenhorst et al., “Passdoodles: A lightweight authentication method,” Research Science Institute, 2004.

[18] H. Tao and C. Adams, “Pass-go: A proposal to improve the usability of graphical passwords.” IJ Network Security, vol. 7, no. 2, pp. 273–292, 2008.

[19] GrIDsure, “Gridsure corporate website,” http://www.gridsure.com, 2009, [Online; last accessed on 17-Jul-2013].

[20] L. Standing, J. Conezio, and R. N. Haber, “Perception and memory for pictures: Single-trial learning of 2500 visual stimuli.” Psychonomic Science, 1970.

[21] D. L. Nelson, V. S. Reed, and J. R. Walling, “Pictorial superiority effect.” Journal of Experimental Psychology: Human Learning and Memory, vol. 2, no. 5, p. 523, 1976.

[22] P. Corporation, “The science behind passfaces. white paper,” http:// www.passfaces.com/enterprise/resources/white papers.htm, 2009, [On- line; last accessed on 19-Jul-2013].

[23] T. Valentine, “An evaluation of the passface personal authentication system,” Technical Report, Goldsmiths College, University of London, Tech. Rep., 1998.

[24] S. Brostoff and M. A. Sasse, “Are passfaces more usable than passwords? a field trial investigation,” in People and Computers XIVUsabil- ity or Else! Springer, 2000, pp. 405–424.

[25] D. Davis, F. Monrose, and M. K. Reiter, “On user choice in graphical password schemes.” in USENIX Security Symposium, vol. 13, 2004, pp. 11–11.

[26] R. Dhamija and A. Perrig, “De´ja` vu: A user study using images for authentication,” in Proceedings of the 9th conference on USENIX Security Symposium - Volume 9, ser. SSYM’00. Berkeley, CA, USA: USENIX Association, 2000, pp. 4–4. [Online]. Available: http://dl.acm.org/citation.cfm?id=1251306.1251310

[27] K. Bicakci, N. B. Atalay, M. Yuceel, H. Gurbaslar, and B. Erdeniz, “Towards usable solutions to graphical password hotspot problem,” in Computer Software and Applications Conference, 2009. COMPSAC’09. 33rd Annual IEEE International, vol. 2. IEEE, 2009, pp. 318–323.

[28] A. Hollingworth and J. M. Henderson, “Accurate visual memory for previously attended objects in natural scenes.” Journal of Experimental Psychology: Human Perception and Performance, vol. 28, no. 1, p. 113, 2002.

[29] S. Weidenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, “Authentication using graphical passwords: Basic results,” Proc. Human-Computer Interaction International (HCII), 2005.

[30] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, “Authentication using graphical passwords: effects of tolerance and image choice,” in Proceedings of the 2005 symposium on Usable privacy and security, ser. SOUPS’05. New York, NY, USA: ACM, 2005, pp. 1–12. [Online]. Available: http: //doi.acm.org/10.1145/1073001.1073002

[31] 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, vol. 63, no. 1, pp. 102–127, 2005.

[32] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "User interface design affects security: Patterns in click-based graphical pass- words," International Journal of Information Security, vol. 8, no. 6, pp. 387–398, 2009.

[33] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in Proceedings of the 3rd symposium on Usable privacy and security. ACM, 2007, pp. 20–28.

[34] K. Gołofit, "Click passwords under investigation," in Computer Security–ESORICS 2007. Springer, 2007, pp. 343–358.

[35] A. Salehi-Abari, J. Thorpe, and P. C. van Oorschot, "On purely automated attacks and click-based graphical passwords," in Computer Security Applications Conference, 2008. ACSAC 2008. Annual. IEEE, 2008, pp. 111–120.

[36] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Computer Security ESORICS 2007. Springer Berlin / Heidelberg, 2007.

[37] S. Chiasson, R. Biddle, and P. C. van Oorschot, "A second look at the usability of click-based graphical passwords," in Proceedings of the 3rd symposium on Usable privacy and security. ACM, 2007, pp. 1–12.

[38] N. L. Clarke and S. M. Furnell, "Authentication of users on mobile telephones–a survey of attitudes and practices," Computers & Security, vol. 24, no. 7, pp. 519–527, 2005.

[39] H. Kim and J. H. Huh, "Pin selection policies: Are they really effective?" computers & security, vol. 31, no. 4, pp. 484–496, 2012.

[40] N. L. Clarke, S. M. Furnell, P. M. Rodwell, and P. L. Reynolds, "Acceptance of subscriber authentication methods for mobile telephony devices," Computers & Security, vol. 21, no. 3, pp. 220–228, 2002.

[41] D. Amitay, "Most common iphone passcodes," Retrieved June, vol. 15, p. 2011,2011.

[42] A. K. Jain, R. M. Bolle, and S. Pankanti, Biometrics: personal identification in networked society. Springer, 1999.

[43] J.-P. Linnartz and P. Tuyls, “New shielding functions to enhance privacy and prevent misuse of biometric templates,” in Audio-and Video-Based Biometric Person Authentication. Springer, 2003, pp. 393–402.

[44] E. Verbitskiy, P. Tuyls, D. Denteneer, and J. Linnartz, “Reliable biometric authentication with privacy protection,” in Proc. 24th Benelux Symposium on Information theory, 2003, p. 19.

[45] N. K. Ratha, J. H. Connell, and R. M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” IBM systems journal, vol. 40, no. 3, pp. 614–634, 2001.

[46] A. Kale, “Algorithms for gait-based human identification from a monocular video sequence,” 2003.

[47] J. Ketcham and G. E. Stelmach, “Age-related declines in motor control,” Handbook of the psychology of aging, vol. 5, pp. 313–348, 2001.

[48] D. Gafurov, “Performance and security analysis of gait-based user authentication,” Ph.D. dissertation, University of Oslo, 2008.

[49] J. Mantyjarvi, M. Lindholm, E. Vildjiounaite, S.-M. Makela, and H. Ailisto, “Identifying users of portable devices from gait pattern with accelerometers,” in Acoustics, Speech, and Signal Processing, 2005. Proceedings.(ICASSP’05). IEEE International Conference on, vol. 2. IEEE, 2005, pp. ii–973.

[50] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, “Unobtrusive user-authentication on mobile phones using biometric gait recognition,” in Intelligent Information Hiding and Multimedia Signal Processing (IIH- MSP), 2010 Sixth International Conference on. IEEE, 2010, pp. 306– 311.

[51] N. L. Clarke and S. Furnell, “Authenticating mobile phone users using keystroke analysis,” International Journal of Information Security, vol. 6, no. 1, pp. 1–14, 2007.

[52] R. Napier, W. Laverty, D. Mahar, R. Henderson, M. Hiron, and M. Wagner, “Keyboard user verification: toward an accurate, efficient, and ecologically valid algorithm,” International Journal of Human-Computer Studies, vol. 43, no. 2, pp. 213–222, 1995.

[53] M. S. Obaidat and B. Sadoun, “Verification of computer users using keystroke dynamics,” Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on, vol. 27, no. 2, pp. 261–269, 1997.

[54] M. Obaidat and D. Macchairolo, “A multilayer neural network system for computer access security,” Systems, Man and Cybernetics, IEEE Transactions on, vol. 24, no. 5, pp. 806–813, 1994.

[55] S. Hwang, S. Cho, and S. Park, “Keystroke dynamics-based authentication for mobile devices,” Computers & Security, vol. 28, no. 1, pp. 85–93, 2009.

[56] M. Jakobsson and R. Akavipat, “Rethinking passwords to adapt to constrained keyboards,” in Mobile Security Technologies, 2012.

[57] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. C. van Oorschot, “Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism,” IEEE Trans. Depend- able Sec. Comput., vol. 9, no. 2, pp. 222–235, 2012.

[58] U. Cil, “Source code of gridwordx for android-based mobile devices,” http://bicakci.etu.edu.tr/gridwordx/readme.html, Feb. 2013.

[59] K. Bicakci, N. B. Atalay, M. Yuceel, and P. C. van Oorschot, “Exploration and field study of a password manager using icon-based passwords,” in Financial Cryptography Workshops, 2011, pp. 104–118.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : ÇİL, Uğur

Uyruğu : T.C.

Doğum tarihi ve yeri : 10.01.1985 İstanbul

Medeni hali : Bekar

Telefon : 0 (505) 788 22 33

e-mail : ugur.chil@gmail.com

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet tarihi**
Lisans	Orta Doğu Teknik Üniversitesi	2010

İş Deneyimi

Yıl	**Yer**	**Görev**
2011-	TOBB ETÜ	Eğitim Asistanı

Yabancı Dil

İngilizce

Yayınlar

- M. Akpulat, K. Bicakci, and **U. Cil** "Metin ve Grafiksel Öğeleri Birleştiren Yeni bir Parola Tabanlı Kimlik Doğrulama Yöntemi", *5th International Conference on Information Security and Cryptology*, 17-18 May 2012, Ankara, Turkey.

- **U. Cil,** K. Bicakci "gridWordX: Design, Implementation, and Usability Evaluation of an Authentication Scheme Supporting Both Desktops and Mobile Devices", *IEEE Symposium on Security and Privacy, Mobile Security Technologies*, 23 May 2013, San Francisco, CA, USA.