

Kullanışlı Güvenlik için Temel Prensipler

Kemal Bıçakcı

Öz— Bugün artık gerçek hayattaki güvenlik problemlerinin çoğunun insan kaynaklı olduğundan eminiz. Söz konusu bu problemlerin ancak insanların rahat ve doğru kullanabilecekleri güvenlik sistemlerinin tasarlanması yolu ile ortadan kaldırılabileceği konusunda uzmanlar hemfikirlere. Bu çalışmada “kullanışlı güvenlik” hedefi yolunda oluşturduğumuz 10 altın kuralı içeren bir liste sunulacaktır. Ayrıca konu ile ilgili bir proje kapsamında tasarladığımız resim-şifre tabanlı şifre yönetim web arayıcı eklenti programı tanıtılacak, bu projeden çıkardığımız dersler ve edindiğimiz tecrübeler paylaşılacaktır.

İndeks Terimleri— Güvenlik, Kullanışlılık, İnsan-Bilgisayar Etkileşimi, Kullanıcı Çalışması, Şifre, Parola, Şifre Yönetimi

I. GİRİŞ

PGP güvenli e-posta yazılımının temel amacı e-posta mesajlarını şifreleyerek ve imzalayarak göndermektir. Whitten ve Tygar PGP 5.0’ın kullanışlılığını ölçerler ve eğitilmiş ve e-posta konusunda tecrübeli 12 kullanıcıdan sadece üçte birinin 90 dakikalık süre içerisinde PGP 5.0 kullanarak şifreli ve imzalı e-posta gönderebilmeyi başardıklarını gözlemlerler [1]. Bu çarpıcı sonucun ortaya konduğu 1999 yılından günümüze gelinceye kadar “kullanışlı güvenlik” gittikçe önem kazanan bir konu olmuştur. 2005 yılından bu yana her sene düzenlenen ve sadece kullanışlılık konusuna odaklanan SOUPS (Symposium on Usable Privacy and Security) güvenlik konferansları serisi [2] bu konuya verilen önemin göstergelerinden sadece bir tanesidir.

Bu bağlamda bilgi güvenliği konusunda insan unsurunun dikkate alınması gerektiği konusunda çarpıcı bir alıntı yapmak uygun olacaktır: “*İnsanoğlu yüksek kalitede kriptografik anahtar saklama kabiliyetinden yoksundur ve kriptolojik işlemlerini yapmada kabul edilemez ölçüde yavaştır. İnsanlar iri, bakımı zor, yönetimi pahalı varlıklardır ve ayrıca çevreyi de devamlı kirletirler. Şaşılabilecek bir durumdur ki bütün bunlara rağmen bu aygıtlar devamlı üretilirler ve kullanılırlar. O kadar her tarafa yayılmışlardır ki, protokol tasarlarken bu varlıkların sınırlı yeteneklerini dikkate almak zorunluluğu vardır [3].*” Yine güvenlik problemlerinin temelinde yatan en büyük faktörün bir diğer ifadeyle güvenlik zincirinin en zayıf halkasının insan ögesi olduğunu gösterir bazı örnekler ve rakamlar vermek gerekirse:

Bu makale 26 Mart 2010 tarihinde gönderilmiştir. Bu çalışma TÜBİTAK tarafından 107E227 no’lu proje kapsamında desteklenmektedir.

K. Bıçakcı TOBB Ekonomi ve Teknoloji Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümü öğretim üyesidir (telefon: 90-312-2924262, faks: 90-312-2924180, e-posta: bicakci@etu.edu.tr).

- Olta saldırıları (phishing attacks) olarak bilinen ve ilk başta artık herkes tarafından bilindiği ve modasının geçtiği düşünülebilen saldırı türleri 2009’un son çeyreğinde de halen yoğun bir şekilde devam ettirilmektedir [4].
- Bir zamanlar ABD’nin en çok aranan bilgisayar korsanı olan Kevin Mitnick yaptığı açıklamada “*Hiçbir zaman şifre kırmak zorunda kalmadım, şifrenin ne olduğunu sadece uygun bir dille sahibine sormak gerekti [5].*” demiştir.
- 2006 yılında yapılan bir anket güvenlik problemlerinin % 60’ının insan kaynaklı olduğunu göstermiştir. Bir önceki yıl için ise bu rakam % 47 seviyesinde [6].

Örneklerin ve istatistiksel verilerin sayısını arttırmak mümkün fakat “Kullanışlı Güvenlik neden gereklidir?” sorusuna şu şekilde özet bir cevap vermek isteriz:

- İnsan ögesini barındıran güvenlik problemlerinin doğru ve etkin çözümü
- Yanlış/eksik kullanım veya kullanılmama kaynaklı güvenlik sorunlarının giderilmesi
- Güvenlik konusunda bilinçsiz fakat güvenlik ihtiyaçları olan kullanıcıların güvenlik kararlarını doğru ve mantıklı bir şekilde verebilmeleri

Ancak güvenliğin kullanışlı olması şartı ile sağlanabilir.

Biz bu çalışmada önce kullanışlı güvenlik kavramının bir tanımını yapmaya çalışacağız (Bölüm 2). Bu tanımın ardından kullanışlı güvenliğin sağlanabilmesi için öngördüğümüz 10 kuraldan oluşan bir liste sunulacaktır (Bölüm 3). Sonrasında, kullanışlı güvenlik konusu kapsamında bir “örnek-inceleme” olarak kabul edilebilecek olan parola tabanlı kimlik kanıtama sistemlerinin kullanışlılık ve güvenlik problemleri ve bu problemlerin çözümüne yönelik yapmış olduğumuz çalışmalar özetlenecektir (Bölüm 4). Kullanışlı güvenlik konusunda gelecekteki çalışmalar konusunda fikirler ve öneriler içeren sonuç kısmı ile bu makale sonlanacaktır (Bölüm 5).

II. KULLANIŞLI GÜVENLİK TANIMI

TANIM: Bir (güvenlik) yazılımı (donanımı, sistemi); o yazılımı kullanması beklenen kişilerce

- güvenilir ve gerekli bulunuyorsa
- yapılması gerekenler doğru bir şekilde anlaşılıyor ve güvenli bir şekilde yapılabilirse
- devamlı kullanımda yeteri kadar rahat ve sorunsuz kullanılabilirse

bu yazılım (donanım, sistem) *Kullanışlı Güvenlik (usable security)* özelliğine sahiptir.

Yukarıdaki tanımda dikkat edilmesi gereken birkaç nokta vardır. Öncelikle güvenlik kelimesi parantez içerisine

alınmıştır. Çünkü kullanılan yazılımın birincil amacı çoğu zaman güvenlik değildir. Örneğin PGP programını insanlar sayısal imza atmak/doğrulamak için değil e-posta alıp/göndermek için kullanırlar. Fakat ikincil amaç olarak bu birincil amacın güvenli bir şekilde gerçekleştirilmesi beklenir. Güvenlik ile ilgili kullanışlılık problemlerinin temelinde güvenliğin çoğu zaman birincil (ana) amaç olmaması yatar. Bu konuya bir sonraki bölümde tekrar dönülecektir.

İkinci bir not olarak belirtmeliyiz ki biz bu çalışmada ağırlıklı olarak yazılımsal güvenlikteki kullanışlılık konularına değineceğiz. Ama unutulmamalıdır ki çoğu zaman bilgi güvenliği denildiğinde donanım, süreçler, kurallar, vb. unsurların ve elbette ki insanların da içinde yer aldığı daha geniş bir sistem düşünülmelidir.

III. KULLANIŞLI GÜVENLİK PRENSİPLERİ

Aşağıda kullanışlı güvenlik hedefini gerçekleştirebilmesi için bir ilk başvuru kaynağı olarak kullanılabilir bir liste oluşturulmaya çalışılmıştır. Elbette bu liste yeni bilgi ve tecrübelerin ışığında ekleme/çıkarmalara ve düzeltmelere açık bir listedir.

A. Otomasyon

Güvenlik tasarımcıları öncelikle kullanıcıyı güvenli çemberinin dışına çıkarmanın yollarını araştırmalıdır. Eğer son kullanıcıya sormadan veya kullanıcının girdi sağlamasının gerekmediği bir yöntem ile güvenlik otomatik olarak etkin ve doğru bir şekilde devreye girebiliyorsa güvenliğin kullanışsızlık gibi bir problemi söz konusu olamaz. Örneğin belki de çoğumuzun farkında olmadığı bir uygulama olarak günümüzde iletim aşamasındaki e-posta güvenliği uygulama protokollerinin SSL üzerinde çalışması yolu ile belli oranda sağlanabilmektedir (fakat halen e-postalarımız sunucularda şifrelenmeden saklanmakta). Bir diğer örnek; Belfanz ve arkadaşları yaklaşık 140 dakika süren ve 38 manuel aşama içeren güvenli kablosuz ağ konfigürasyon problemini otomasyon yardımı ile 1 dakika 39 saniyede tamamlanabildiğini göstermişlerdir [7].

Fakat günümüz teknolojisi ile bazı kritik güvenlik işlemlerinin tamamen otomatik hale getirilmesi mümkün değildir (veya söz konusu otomasyon kullanışlılığı azaltmaktadır). Bu sebeple diğer 9 prensibe gereksinim kaçınılmazdır.

B. Yenilikçi Çözümler

İnsan-Bilgisayar Etkileşimi ve Kullanışlı Arayüz Tasarımı sadece güvenlik konusunda değil daha genel anlamda oldukça etkin çözümler sunan ve belli olgunluğa ulaşmış bilim dallarıdır. Kullanışlı güvenlik konusunda çalışacak olan uzmanların elbette bu ve diğer (bilişsel psikoloji, sosyoloji, ekonomi, yapay zeka, vb.) bilim dallarından yararlanmaları gereklidir. Fakat şöyle bir yanılgıdan ise kaçınılmalıdır. Güvenliğin kullanışlı hale getirilebilmesi için güvenlik konusunda da uzmanlık gerekirken ve ancak güvenlik uzmanı gözlüğü ile farklı bir bakış açısı ile yenilikçi çözümler mümkün olabilmektedir. Dolayısıyla güvenliğin kullanışlı hale

getirilmesi sadece standart ve genelleştirilmiş pratikler yardımı ile mümkün olamayacaktır. Örneğin; Açık Anahtar Kriptografisinin güvenli çalışabilmesi için açık anahtarların güvenli bir şekilde paylaşılması gerektiği bilinmektedir. Güvenilir Sertifika otoritelerince imzalanmış sertifikalar bu problemin geleneksel çözümüdür. Lakin bu geleneksel çözüm kullanışlılık konusunda problemler barındırmaktadır. Bu konuda kablosuz ağ konfigürasyonu için uygulanan yenilikçi ve çok daha kullanışlı bir çözüm; açık anahtarların yer sınırlı kanallar üzerinden (kızıl ötesi iletim gibi) taşınması ve bu işlemin fiziksel olarak girişi kontrol altında tutulan kayıt odasında yapılmasıdır [7]. Takdir edilmelidir ki, bu şekilde bir yenilikçi çözüm önerebilmek hem problemin doğasını hem de uygulama gereksinimlerini dikkate almak kaydıyla oluşturulabilir.

C. “Herkes Benim Gibidir” Yanılgısı

Güvenlik konusunda sistem geliştirenleri veya daha genel anlamda herhangi bir konuya yoğunlaşmış uzmanlaşanları bekleyen büyük bir tehlike vardır. Geliştirilen sistemi kullanacak olanların (veya ilgili diğer kişilerin) kendisi gibi olduklarını zannetmek ve dolayısıyla kullanım ile ilgili karşılaşılabilecek problemleri öngörememek tehlikesi. Hatta bu yanılgı öyle bir boyuta çıkabilir ki kullanışsızlığı kabul etmek yerine suçu kullanıcıya atmak, kullanıcının beceriksiz, vb. olduğunu iddia etmek sıklıkla görülebilmektedir.

Yine bir örnek vermek gerekirse; Norveç’te bir e-banka sitesi 11 haneli hesap numarası yerine girilen hatalı 12 haneli hesap numarasını 11 haneye otomatik olarak çevirip, kullanıcı onayından sonra istenmeyen bir hesaba para transferinde bulunuyor. Banka işlemin kullanıcı tarafından doğrulandığından hareketle kusuru üzerine almıyor. Kullanıcı yanlış girildiği belli olan 12 hanelik numarayı bankanın kabul etmemesi gerektiğini söyleyerek itiraz ediyor. Mahkeme karar vermeden önce “kullanışlılık” deneyi yapılmasına karar veriyor. Deneyde kullanıcıların % 97,3’ü aynı hatayı yapınca mahkeme kararı banka aleyhine oluyor [8]. Bu konuda ilginç bir diğer not FBI ajanlarının diğer kişilerin kendileri gibi düşünmediklerini hatırlamaları için devamlı eğitim gördükleri bilgisidir [8].

Söz konusu yanılgı ile ilintili üzerinde durulması gereken diğer bir konu *güvenlik eğitimi* konusudur. Güvenlik eğitimi önemlidir ama kullanışlı güvenliğin alternatifi değildir. Bir şirket çalışanlarını eğitmek belki mümkündür ama genel İnternet kullanıcı kitlesinin eğitiminden söz etmek ne ölçüde gerçekçidir? Ayrıca, söz konusu eğitimin hangi şartlarda verileceği, ne zaman ve nasıl verildiği özenle sorgulanmalıdır.

D. Teori-Pratik Çelişkisi

Güvenlik konusunda çalışanları tehdit eden bir diğer yanılgı psikolojideki ismiyle *sıfır risk yanılgısı*dır. Bilinmelidir ki teorideki en iyi güvenlik yöntemi daha az güvenli görülen yöntemlere göre pratikte çok daha az etkin olabilmektedir. Bir diğer ifadeyle teori ile pratik arasında teoride fark yoktur ama pratikte vardır. Ne demek istediğimizi yine bir örnekle açıklamak yerinde olacaktır:

olduğunun farkına varmak kullanışlı güvenliği sağlamanın olmazsa olmazlarındandır.

Bugün güvenliği ölçmek için anahtar uzunluğu, paket işleme performansı, algoritma hızı, vb. ölçümü kolay ve güvenlikle de çok ilgili olmayabilen metrikler tercih edilmektedir. Bir güvenlik sisteminin kullanışlılığını ölçmek ise çok daha zor bir işlemdir. Kullanışlılığın bir metrik olarak kullanılmamasının altında bu durumun yattığını söylemek yanlış olmayacaktır.

Kullanışlılık (usability) kelimesinin ISO/IEC 27001:2006 standardında ve NIST tarafından yayınlanan 800-30 no'lu risk yönetim dökümanında bahsi bile geçmemektedir [9]. Bir problemi çözmek için elbetteki önce o problemin varlığını bilincinde olmamız gerekmektedir.

I. Doğru Metaforlar

Kullanıcıların zihinlerindeki güvenlik modeline uygun davranmak ve doğru oluşturulmuş metaforlar kullanarak kullanıcının daha önceden bildikleri ile yeni güvenlik kavramları arasında bir bağ oluşturmak çok etkin bir kullanışlılık artırıcı yöntemdir.

İşletim sistemlerinde dosya silme işlemi yaptığımızda esasında sadece o dosyanın diskte nerde saklandığı bilgisi silinmekte ve fiziksel olarak o dosya erişilebilir halde kalmaktadır. Bu durumun oluşturduğu güvenlik risklerine karşın Macintosh işletim sistemi yeni bir komut yardımı ile “*güvenli silme*” özelliğini ve bu dosyanın fiziksel olarak silinmesini de sağlamaktadır. Fakat kullanıcının bu işlemi doğru anlaması ve yanlış kullanımdan kaynaklı problemlerin giderilmesi için bu işlem ile birlikte kâğıt kırma makinesi metaforunun kullanılması ve kullanıcıya gösterilmesi önerilmiştir [10]. Yani çoğumuzun bildiği gibi nasıl ki kırma makinesine gönderdiğimiz bir kâğıdı tekrar birleştirmek mümkün değil ise öyle de benzer bir işlemi bilgisayar ortamında yapar isek kâğıt kırma makinesini görmüş olmak geriye dönüşün mümkün olmayacağını anlamamıza ve daha dikkatli olmamıza yardımcı olacaktır. Aksi halde “*güvenli silme*” tabirini çoğu kullanıcının “*istenildiğinde geri dönüş yapılabilir silme*” olarak algılaması hiç de sürpriz değildir.

J. Deney, Deney, Deney

Hızlı prototip ve küçük kullanıcı çalışmaları ile pek çok kullanışlılık problemini zamanında tespit etmek ve gerekli düzeltmeleri yapmak mümkündür. Zannedilenin aksine bu çalışmaların geniş kapsamlı ve maliyeti yüksek olması gerekmemekte, sıkça tekrar edilen ve yazılım geliştirme sürecine tümleştirilmiş küçük kapsamlı deneyler çoğu zaman yeterli olmaktadır. O yüzden bu prensibi “Deney, Deney, Deney” olarak isimlendirdik. Konumuzla ilgili bazı çarpıcı deney sonuçlarını aktarmak istiyoruz:

1. Nobel ödüllü Kahneman ve Tversky'nin yapmış oldukları deneyde [8] deney katılımcılarının %84'ü kendilerine önerilen garanti 500 \$ miktarındaki parayı %50 kazanma şanslarının olduğu 1000 \$'a tercih etmiştir. Aynı soru 1000 \$'ın 500 \$'ını kesin kaybetmek mi istersiniz yoksa 1000 \$'ın hepsini %50 ihtimal ile

kaybetmek mi diye sunulunca aynı oran %31'e iniyor. Bir diğer ifadeyle garanti 500\$'ı tercih edenlerin oranı %53 oranında azalıyor. Aynı soruyu farklı bir şekilde sununca kullanıcıların fikirlerinin bu ölçüde değişmesi sonucu daha sonra yapılan pek çok farklı deney ile doğrulanmıştır.

2. *Site-tanuma resimlerinin* başarı oranı %8 olarak ölçülmüştür [8]. 25 kullanıcıdan 23'ü kendilerine ait gerçek bir e-bankacılık işleminde seçtikleri resim yerine “xxx bankası ödüllü STR teknolojisini şu anda iyileştiriyor. Eğer seçtiğiniz resim 24 saat içerisinde gözükmezse müşteri servisi ile bağlantıya geçiniz.” şeklinde bir uyarı mesajı çıkmasına rağmen bankacılık işlemlerine devam etmişlerdir.

3. İnternet'te Kimlik Doğrulama İşlemi için Almanya'da bir üniversitede bedava dağıtılan Akıllı Kartları kullanmak isteyenlerin oranının %0 olduğu görülmüştür [8].

Evet, kullanışlı güvenlik konusunda daha pek çok doğru bilineni sorgulamak ve sürpriz sonuçlar yakalamak mümkün gözükmektedir. Bu bağlamda hatırlatmak isteriz ki; kullanıcı çalışmalarının etik sorunlarının olabileceği öngörülerek bazı üniversitelerin bünyesinde oluşturulmuş etik kurullarından çalışma öncesinde izin alınması gerekli görülmektedir.

IV. RESİM-ŞİFRELER VE ŞİFRE-YÖNETİM PROGRAMLARI

Bu bölümde Bölüm 3'de aktardığımız prensiplerin büyük bir kısmını uygulama ve kullanma şansı bulduğumuz bir örnek çalışma sunulmaktadır.

Hepimizin kullana geldiği ve problemlerinin artık hemen herkes tarafından bilindiği metin tabanlı şifrelere alternatif olabilecek kullanışlı ve güvenli çözümler önermek amacıyla yürüttüğümüz proje ile bilişsel psikolojinin insanların resim hafızasının metin hafızasından üstün olduğunu ortaya koyan sonuçlarından yararlanılması hedeflenmiştir. Araştırma sorularımız iki tane:

1. Bir fotoğraf bin sözcüğe bedeldir prensibini problemimizin çözümü için nasıl ve ne şekilde kullanmalıyız?
2. Bu prensip doğruysa hala niye resim-şifreler günlük hayatta yaygınlaşmıyor? Sebepler ne olabilir?

Bu sorulara yanıt olarak önerdiğimiz çözüm resim-şifreleri şifre-yönetim programları ile birleştirmemiz sonucunda geliştirdiğimiz ve GPEX (Graphical Passwords as Browser EXtension) adını verdiğimiz Firefox web tarayıcı eklenti programıdır. GPEX eklentisini geliştirirken hipotezimiz parolaların kullanışlılık ve güvenlik problemlerinin temelinde yatan sebebin bugün bir değil pek çok farklı parola hatırlama gereksiniminin ortaya çıkmış olmasıdır diye özetleyebiliriz. Bir diğer ifadeyle insan beyninin kapasitesi onlarca farklı ve güvenli (yeterli uzunlukta ve tahmin edilmesi zor) parola ile baş edememektedir. Dolayısıyla ya tahmin edilmesi kolay parolalar seçmesi ya da aynı parolayı farklı sitelerde kullanarak daha farklı türden bir güvenlik açığına sebebiyet verilmektedir. Bu açmazın çözümü parola yönetim programlarıdır. Bu programları kullanarak tek bir temel (ana) (master) parola ile güvenli bir şekilde farklı siteler için farklı parolalar üretebilmek mümkün hale gelmektedir. Bizim GPEX

programı ile desteklediğimiz ekstra bir özellik ise seçilen temel parolanın resim-şifre tabanlı olabilmesini sağlamaktır. Bu şekilde temel parolanın güvensiz kişilerce veya olta saldırısı sitelerince ele geçirilme riskini ortadan kaldırmak mümkün hale gelmiştir [11]. Ayrıca yaptığımız kullanıcı çalışmaları ile GPEX'in hızlı, doğru ve kolay kullanılabilir bir uygulama olduğu ve resim-şifrelerin sistemin uzun süreler kullanılmaması durumunda dahi unutulmadığı ortaya konulmuştur [12].

<http://myuceel.etu.edu.tr/gpexV2.1.xpi> adresinden son sürümü elde edilebilen GPEX açık kaynak kodlu Firefox şifre yönetimi eklenti programının nasıl kullanılacağı aşağıda anlatılmaktadır:

1. Kullanıcı öncelikle ziyaret ettiği web sitesinin *Password* alanına çift tıklar.
2. Açılan penceredeki görsel alanda sunulan toplam 150 ikondan belli sayıda seçerek (bu ikonların üzerine tıklayarak) GPEX şifresini oluşturur. Kullanıcı oluşturulacak olan site parolasını görmek isterse açılan pencerede "Show Password Before Enter" kutusunu işaretler (Bakınız Şekil 6).
3. Enter Password düğmesine basılması ile birlikte *Password* alanı üretilen şifre ile otomatik olarak doldurulur.

GPEX'in kullanımı yukarıda anlatıldığı üzere oldukça kolaydır. Daha önce kullanılan metin tabanlı şifrelerin GPEX programınca üretilen şifrelerle değiştirmek için yukarıdaki adımları yeni şifrenin sorulduğu ve doğrulandığı parola yenileme ekranında iki kere gerçekleştirmek gerekmektedir.

GPEX'in avantajlarının en önemlileri kısaca aşağıda özetlenmektedir:

1. Tek sabit bir temel şifre: GPEX'de temel şifreyi (master password) değiştirmeden her web sayfasına (örneğin: gmail) farklı şifre üretebilme özelliği bulunmaktadır. Farklı site şifreleri aşağıdaki formül yardımı ile üretilmektedir:

Web sayfası şifresi = H^n (Web sayfası URL || Master Password) (1)

H : güvenli bir özet işlevi (hash function)

n : Şifre güçlendirme sabiti (ileride açıklanacak)

|| : birbirine bağlama (yan-yana girdi)

URL: örneğin gmail.com

2. Olta Saldırı Koruması: Şifre tekrar kullanım problemlerini ve olta saldırılarını engelleme özelliği kullanıcılara kullanışlı bir çözüm sunmaktadır.

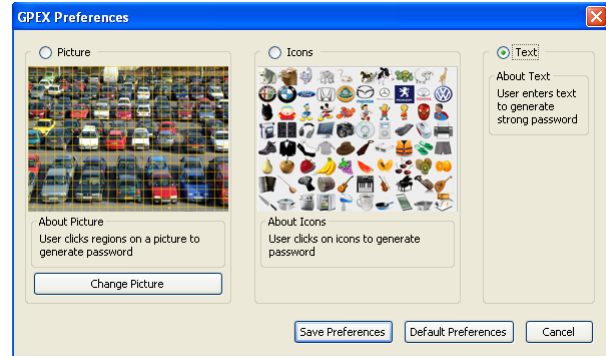
Yukarıdaki formül 1 ile ürettiğimiz web sayfası şifresi URL'i bir girdi olarak aldığı için ziyaret edilen bir olta saldırı sitesince elde edilecek şifre gerçek şifre ile aynı olmayacaktır.

3. Farklı Yöntem Desteği: GPEX sisteminde farklı parola yöntemleri desteklenmektedir. Şekil 7'de gösterilen GPEX tercih menüsünden kullanıcılar resim, ikon veya metin tabanlı tercihlerini yaparak temel şifrelerini istedikleri türden atayabilmektedir.

Bu şekilde bir tercih sistemi yardımı ile farklı şifre yöntemlerini çok daha gerçekçi bir alan çalışması yaparak karşılaştırabilme imkânı sağlanmaktadır.



Şekil 6. GPEX Kullanıcı Arayüzü



Şekil 7. GPEX Tercih Ekranı

4. Çevrim-Dışı Atak Direnci: Formül 1'de $H()$ fonksiyonu bir kez yerine n kez uygulanarak çevrim-dışı ataklara karşı direnç n kez arttırılmaktadır.

Ele geçtikleri web sitesi şifresini kullanarak temel şifrenin ne olduğuna yönelik bir saldırı gerçekleştirenler $H()$ fonksiyonunu n kat daha fazla çalıştırma zorunda kalmış olacaklardır. Dolayısıyla çevrim-dışı atağın sonlandırılması için n kat daha fazla süreye ihtiyaç duyulacaktır.

GPEX v2.1'de n değerini sabit olarak değil de temel şifrenin güvenliğine bağlı olarak seçerek kendinden-uyarlamalı bir sistem önerilmektedir. Ayrıca bu yeni sürümde kullanıcılara şifrelerinin güvenlik seviyeleri konusunda bir geri bildirimde bulunmaktadır.

5. Şifre kuralları: Ziyaret edilen web sitesinin kurallarına

uygun şifre üretimi yine GPEX'in getirdiği yeniliklerdendir.

Merkezi sunucuda sakladığımız ve her GPEX istemcide en son güncel kopyasının tutulduğu bir XML şifre politikası dosyası yardımı ile formül 1'in çıktı değerinin işlenmesi ve ziyaret edilen siteye ait kurallara uygun hale getirilmesi mümkün olmaktadır.

Yer darlığı sebebiyle resim-şifreler konusunda yürüttüğümüz çalışmaların tamamı burada aktarılamayacaktır. Sadece GPEX'in gerçek hayatta nasıl kullanıldığını tespit amacıyla tamamladığımız alan çalışmasından kısaca bahsetmek isteriz. Söz konusu bu çalışmada 20 üniversite öğrencisi GPEX'i ortalama 1.5 aylık süre boyunca ziyaret ettikleri toplamda 7 farklı site için 1197 kez kullanmışlardır. Bu çalışmanın sonunda elde ettiğimiz bulgular şu şekildedir:

- Hatasız giriş oranı: % 98.5 (toplam 19 hatalı giriş).
- Şifresini unutanların oranı: % 0
- Ortalama giriş süresi: 6.24 saniye.
- GPEX'in kullanışlılığına verilen puan: 4,525 / 5.
- GPEX'in güvenliğine verilen puan: 4,75 / 5.

Resim-şifre ve şifre yönetim programları konularında daha fazla bilgi almak isteyenlere GPEX'in farklı bir üslupla tanıtıldığı blog yazımızı [15] ve diğer akademik yayınlarımızı okumalarını öneririz [11] [12].

V. SONUÇ

Kullanışlılık konusu bilgi güvenliğinin oldukça yeni ve önemli bir alt-konusudur ve pek çok farklı ve yeni çalışma alanlarını içerisinde barındırmaktadır. Biz bu çalışmada genel amaçlı bir kullanışlı güvenlik prensipleri listesi oluşturduk ve resim-şifreler ve şifre yönetimi konularında yaptığımız çalışmaları bir örnek çalışma olarak özetle aktarmaya çalıştık. Makalemizin sonunda yürüttüğümüz proje sonundaki edinimlerimizi ve bu konuda çalışmak isteyenlere önerilerimizi yine kısaca aktarmak istiyoruz:

1. Belki de önemi gereği kullanışlı güvenlik konusunda en çok çalışılan konunun parolalar olduğu görülmektedir. Fakat nerdeyse her güvenlik konusunun bir de kullanışlılık yönü bulunmaktadır. Bu sebeple yeni konu bulmak yönünden herhangi bir sıkıntı söz konusu değildir.
2. Örneğin veri yedeklemesi, sabit disk şifreleme, mobil uygulamalar, vb. konular nerdeyse hiç çalışılmamış kullanışlı güvenlik konularıdır. Veri mahremiyeti kontrolü gibi üzerinde fazlaca çalışılmış konularda bile problemin zorluğu sebebiyle yeni yaklaşımlara şiddetle ihtiyaç duyulmaktadır.
3. Seçilen konuda yeni bir kullanışlı güvenlik yöntemi önerilmeden önce mevcut sistemlerin kullanışlılığının ölçülmesi ve kullanıcı çalışmaları yürütülmesi önerilmektedir. Araştırmacıların kendi önerdikleri sistemlerin kullanışlılığı konusunda çok fazla iyimser oldukları gözlemlenmiştir. Bağımsız kullanıcı çalışmaları ile önceki hipotezlerin çoğunun geçersiz olduğu gösterilebilmektedir [13].
4. Kullanıcı deneyleri tasarlamak ve başarıyla uygulamak kesinlikle ilk görüldüğü kadar kolay bir

iş değildir. Bu konudaki uzmanlar bile “yapılan deneyin sonunda keşke bu deneyi daha farklı bir şekilde yürütmüş olsaydım demediğim hiçbir çalışma olmadı [14]” diyebilmektedirler.

5. Yapılan deneyin tüm yönleri ve aşamalarıyla ayrıntılı bir şekilde anlatılması ve bu sayede sonuçların başka araştırmacılarca da tekrar edilebilmesinin doğrulanabilmesinin önünün açılması son derece gereklidir.
6. Yapılan deneyin kısıtlarını ortaya koymak ve sonuçları objektif bir şekilde sunmak çalışmanın inandırıcılığını arttırmaktadır.
7. Son olarak; yeni önerilen yöntemlerin kısa sürede bir prototipini oluşturmak, kullanıcı çalışmalarını hızlı ve zamanında yapmak ve bu çalışmaların sonuçlarını kullanarak iyileştirmelerde ve değişikliklerde bulunabilmek kullanışlı güvenlik adına oldukça gerekli adımlardır. Yazılım mühendisliğindeki kesin çizgilerle ayrılmış aşamalar içeren şelale modelinin eksiklikleri konu kullanışlı güvenlik olunca daha da bariz hissedilmektedir.

REFERANSLAR

- [1] Alma Whitten and J. D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In 8th USENIX Security Symposium, pp. 169 – 184. Usenix, 1999.
- [2] Symposium on Usable Privacy and Security, ACM International Conference Proceeding Series, 2005-2010, <http://cups.cs.cmu.edu/soups>
- [3] C. Kaufman, R. Perlman, and M. Speciner. Network Security: Private Communication in a Public World. Prentice Hall, second edition, 2002.
- [4] Anti-phishing group web page, <http://www.antiphishing.org/>
- [5] K. Mitnick, W. Simon, and S. Wozniak. The art of deception: controlling the human element of security. John Wiley & Sons, 2002.
- [6] M. Crawford. Whoops, human error does it again. CSO Online. April 21, 2006. <http://www.csoonline.com.au/index.php/id;255830211;fp;32768;fpid;20026681>
- [7] Balfanz, D. ; Durfee, G. E. ; Grinter, R. E. ; Smetters, D. K. ; Stewart, P., “Network-in-a-Box: How to Set up a Secure Wireless Network in under a Minute,” *Proc. 13th Usenix Security Symp.*, Usenix Assoc., 2004, pp. 207–221.
- [8] Peter Gutmann: Security usability, February 2008, Draft. <http://www.cs.auckland.ac.nz/~pgut001/pubs/usability.pdf>
- [9] Jösang, A., Alfayyadh, B., Grandison, T., Alzomai, M. & McNamara, J. (2007b), Security Usability Principles for Vulnerability Analysis and Risk Assessment, in 'The Proceedings of the Annual Computer Security Applications Conference (ACSAC '07)'.
- [10] S.L. Garfinkel and A. Shelat, “Remembrance of Data Passed: A Study of Disk Sanitization Practices,” *IEEE Security & Privacy*, vol. 1, no. 1, 2003, pp. 17–27.
- [11] Bicakci K., Atalay N.B., Yuceel M., Gurbaslar H., Erdeniz B. 2009. Towards Usable Solutions to Graphical Password Hotspot Problem. In Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference, Seattle, Washington, USA, pp. 318-323, 20-24 July 2009.
- [12] Bicakci K., Atalay N.B., Yuceel M., Gurbaslar H., 2010. Usability of Password Managers: A Long Term Field Study on Graphical Password as Browser Extension (GPEX), Submitted to SOUPS 2010.
- [13] Chiasson, S., van Oorschot, P.C., Biddle, R. 2006. A Usability Study and Critique of Two Password Managers. In Proceedings of 15th USENIX Security Symposium, August 2006.
- [14] Schechter S., Common Pitfalls in Writing about Security and Privacy Human Subjects Experiments, and How to Avoid Them, <http://cups.cs.cmu.edu/soups/2010/howtosoups.pdf>

- [15] Bıçakcı K., Parola problemlerine Son.
<http://akademikguvenlik.wordpress.com/2010/03/26/parola-problemlerine-son/>