**ISSN:1306-3111**
e-Journal of New World Sciences Academy
2011, Volume: 6, Number: 1, Article Number: 1A0134

**ENGINEERING SCIENCES**
Received: October 2010
Accepted: January 2011
Series : 1A
ISSN : 1308-7231


**Çetin Elmas**
**Abdullah Orman**
**Murat Dener**
Gazi University
celmas@gazi.edu.tr
Ankara-Turkey

# İNTERNETTE BİLGİ GÜVENİLİRLİĞİNİ ARTIRACAK BİR UYGULAMA GELİŞTİRİLMESİ

**ÖZET**

Bilgisayar teknolojileri gelişip yaygınlaştıkça, günlük iş ve işlemler elektronik ortamlara taşınmakta ve kolaylaşmaktadır. Bunun sonucu olarak bilgi ve bilgisayar güvenliğinin önemi ve karşılaşılan tehditler, gerek sayı gerekse çeşitlilik açısından artmıştır. Bu bağlamda, Internet ten girilen bilgilerin (e-posta,şifre,kredi kart no) güvenilirliğini sağlamak amacıyla bir uygulama (sanal klavye) geliştirilmiştir. Mevcut sanal klavyeler sadece klavye dinleme sistemlerini (key logger) önlerken, yapılan uygulama buna ek olarak görüntü yakalama sistemlerini (screen logger) de önlemiştir. Bu çalışmanın, kötü niyetli olarak geliştirilen yazılım türlerinin daha iyi bilinmesi, tanınması ve gerekli önlemlerin alınmasına büyük katkılar sağlayacağı ve gerçekleştirilen uygulama sayesinde karşılaşılabilecek zararları azaltılabileceği değerlendirilmektedir.

**Anahtar Kelimeler:** Bilgi Güvenliği, Bilgisayar Güvenliği, Klavye Dinleme Sistemleri, Görüntü Yakalama Sistemleri, Sanal Klavye

# DEVELOPMENT OF AN APPLICATION FOR INFORMATION TRUSTWORTHINESS ON INTERNET

**ABSTRACT**

As information technologies being developed and becoming widespread, daily routines and works have switched to electronic media and made life easier. So the importance of information and computer security and threats encountered has increased in diversity as well as in quantity. So an application (virtual keyboard) is developed for the purpose of providing reliability of informations (e mail, password, credit cart no) which entered by internet. While available virtual keyboards only prevent from key loggers, this application in addition that prevents from screen loggers. This comprehensive work contributes to the computer users to know the threats of malicious software in details. The features of these wares and risks have been updated. Also, It is evaulated that the risks is reduced owing to developed application.

**Keywords:** Information Security, Computer Security, Key Loggers, Screen Loggers, Virtual Keyboard

## 1. GİRİŞ (INTRODUCTION)

Bilişim teknolojilerinin bizlere sağladığı kolaylıklar arttıkça elektronik ortamların kullanımı yaygınlaşmakta, bilginin işlendiği, taşındığı ve saklandığı ortamlara erişimler, zamandan ve mekândan bağımsız hale gelmektedir. Doğal olarak, toplumların gelişmesi hızlanmakta; iş ve işlemleri yapış şekilleri değişmekte; üretimleri ve tüketimleri artmakta; sosyal ve kültürel hayattaki değişimler ve dönüşümler hızlanmakta; bilişim teknolojilerinden beklentileri artmakta ve sanal ortamlara daha bağımlı hale gelmektedirler. Elektronik ortamlarda yapılan iş ve işlemlerin artması, bu ortamlardaki bilgi miktarını her geçen gün hızla arttırmaktadır. Elektronik ortamların hızla yaygınlaşması, büyük bir tehlikeyi de beraberinde getirmektedir. Bu tehlike, elektronik ortamı oluşturan sistemlerin ve bu ortamlardaki bilginin korunmasıdır [1].

Elektronik ortamlarda bilginin korunması için, bu ortamları kullanan kişiler, kurumlar ve devletler, büyük çaba, emek ve para harcamakta, yeni yöntemler ve teknikler geliştirmekte ve bunları kullanarak kişisel ve kurumsal bilgi güvenliklerini sağlamaya veya arttırmaya çalışmaktadırlar. Bunun doğal sonucu olarak, sistemlerde meydana gelebilecek güvenlik açıklarının azalması beklenirken; bu beklentilerin de aksine, saldırılar ve saldırganların keşfettiği korunmasızlıklar ya da açıklar da hızla artmaktadır. Bu tehditlerin başında, kötücül ve casus yazılımlar kullanılarak gerçekleştirilen saldırılar gelmektedir. 2000 yılından bu yana elektronik ortamlara yapılan saldırılar ve bu ortamlardaki korunmasızlık türlerinde, 6 kattan fazla artış olmuş ve bunların sayısı 150.000'lere ulaşmıştır [2 ve 3].

Casus yazılımların, çok önemli kullanıcı bilgilerini fark ettirmeden karşı tarafa kolaylıkla, sinsice ve sessizce iletmesi, bilgi ve bilgisayar güvenliğinde büyük zafiyetlere sebep olabilmektedir. Ayrıca gerek kişisel, gerekse kurumsal güvenliğin sağlanmasında büyük zafiyetler oluşabilmektedir. Dolayısıyla, her düzeyde bütün bilgisayar kullanıcıları ve kurumların kendileri, çok ciddi risk ve tehditler ile karşı karşıyadır. Yine bu kullanıcılar, gerekli önlemler alınmazsa oldukça büyük zararlara uğrayabilirler. Bu riskleri en aza indirgemek ve oluşabilecek tehditlerden korunmak için; güvenlik bilincinin oluşturulması, güvenlik yazılım ve donanımlarının tanınması ve anlaşılması, belirli politikalar çerçevesinde bilgisayarların kullanımı ve denetimi gereklidir[4].

Özellikle son zamanlarda artış gösteren Internet üzerinden banka hesaplarına girilmesi ve bu hesapların içinin boşaltılması buna örnek olarak verilebilir. Bir çoğu uluslararası çalışan saldırgan grupları Internet üzerinden bilgisayarlara sızmak ve bu yolla gizli bilgilere ulaşıp bu bilgileri kullanmak yada bilgisayarı ve Internet bağlantısını başka sistemlere karşı tehdit olarak kullanmak için sürekli yeni yöntemler geliştirmektedirler.

Bu makalede, internette bilgi güvenliği için geliştirilmiş bir uygulama sunulmaktadır. İkinci bölümde çalışmanın önemine değinilmiştir. Üçüncü bölümde internette bilgi güvenliğini etkileyen kötücül yazılımlardan bahsedilmekte ve kötücül yazılım türleri açıklanmaktadır. Dördüncü bölümde, sanal klavye, uygulamanın geliştirilmesi ve gerçekleştirilen uygulamanın mevcutlardan farkı anlatılmaktadır.

## 2. ÇALIŞMANIN ÖNEMİ (RESEARCH SIGNIFICANCE)

İnternet Bankacılığı, bankacılık hizmetlerinin internet üzerinden sunulduğu bir alternatif dağıtım kanalıdır. Türkiye'de bugün internet bankacılığı, herhangi bir banka şubesinin sağlayacağı hizmetlerin hemen hepsinden, zaman ve mekandan bağımsız olarak çabuk ve kolayca yararlanılmasını sağlamaktadır. İnternet bankacılığının sağladığı faydalar şöyle özetlenebilir [5]:

- Hızlı ve kesintisiz bankacılık işlemleri,
- Şubeye gitmeden, sıra beklemeden kolay bankacılık işlemleri,

- Görerek ve seçerek bankacılık işlemi yapabilmek,
- Detaylı rapor ve bilgi alabilmek,
- Çok çeşitli bankacılık ürünlerini görerek bu ürünlerden faydalanabilmek,
- Bankacılık işlemlerini çok daha ucuza yapabilmek,
- İşlemlerin banka personeli tarafından dahi görülememesi nedeniyle, gizli ve güvenli bankacılık.

İnternet Bankacılığı, bu kadar yararlı olmasına rağmen güvenlik açıklarını da beraberinde getirmektedir.

Son günlerde çeşitli banka ve finans kurumları tarafından gönderilmiş gibi görünen, acil ve çok önemli konular içeriyormuş gibi duran sahte e-postalar (phishing-olta saldırıları) internette yayılmaktadır. Bu e-postalarda verilen linkler aracılığı ile banka müşterilerinden, kart bilgileri, kart şifreleri, internet şubesi şifreleri ve kişisel bilgileri istenmektedir. Bu eylem açık bir dolandırıcılık girişimidir.

Dolandırıcılar phishing yöntemiyle kullanıcının gizli bilgilerini elde etmenin yanı sıra bu bilgilere başka bir yöntem olan keylogger adı verilen klavye ve ekran görüntülerini kopyalayabilen programlar vasıtasıyla ulaşabilmektedirler.

İnternet kullanan banka müşterilerinin veya internet üzerinden ticaret yapan kullanıcıların çevrimiçi işlem şifrelerinin çalınması keylogger, yani klavye tuş girdilerini kayıt eden yazılımlar vasıtasıyla da yapılmaktadır. Kullanıcıların bilgisayarlarına yerleştirilen keylogger adlı yazılım, bilgisayarda yapılan her türlü işlemlerin bir kaydını tutar, bu kayıtlar klavyeden girilen bilgilerin yanı sıra ekran görüntüleri de olabilir. Bu kayıtlar ya sistemde bir txt (metin) dosyası olarak tutulur ya da klavye girdileri e-posta ile saldırgana (hacker) gönderilir.

Bu çalışmada keylogger, screen logger saldırılarını önleyen güvenli bir sanal klavye geliştirilmiştir. Geliştirilen sanal klavye sayesinde internet bankacığında dolandırıcılık işlemlerine maruz kalan kullanıcıların güvenliği üst düzeye çıkartılmıştır.

Çalışmanın önemini vurgulamak adına üçüncü bölümde kullanıcıların güvenliğini etkileyen kötücül yazılımlar ayrıntılı olarak anlatılmıştır.

## 3. KÖTÜCÜL YAZILIMLAR (MALWARE)

Kötücül yazılım (malware, İngilizce "malicious soft-ware"in kısaltılmışı), bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış istenmeyen yazılımların genel adıdır [2]. Kötücül yazılımlar, kullanıcının haberi olmadan veya kullanıcıyı yanıltarak sistemlere yetkisiz bir şekilde bulaşmaktadır [6]. Kirli yazılım scumware) olarak da ifade edilen kötücül yazılımlar, hemen hemen her programlama veya betik (script) dili ile yazılabilmekte ya da birçok dosya içinde taşınabilmektedirler.

Virüsler, solucanlar (worm), Truva atları (Trojan horse), arka kapılar (backdoor),mesaj sağanakları (spam), kök kullanıcı takımları (rootkit), korunmasızlık sömürücüleri (exploit), klavye dinleme sistemleri (keylogger), görüntü yakalama sistemleri (screen logger), tarayıcı soyma (browser hijacking) ve casus yazılımlar (spyware) en genel kötücül yazılımlardır.

Genel olarak tüm kötücül yazılımlar; yaşam döngüsü, kendi kendini çoğaltma, özerklik, bulaşma mekanizması, ayrık veya virüs özelliği taşıma, korunma mekanizması açısından farklı karakteristikler sergileyebilmektedir. Kötücül yazılımlar, yaşam döngüsünde harhangi bir aşamada farklı davranışlar sergileyebilecekleri gibi, kendi kendini çoğaltmayacak tek bir amaca yönelik çalışmaktadır. Kullanıcının araya girmesine ihtiyaç duyabilecekleri gibi tamamen özerk bir yaklaşıma sahip olmakta; kötü niyetli kişiler tarafından bizzat elle hedef bilgisayar sistemine kurulabilmekte, kendisini saptayacak veya yok edecek korunma yapılarına

karşı direnç gösterebilmekte, çeşitli taktiklerle bu tür programları atlatabilmektedir [6]. En temel kötücül yazılımlar, gelişme süreçleri açısından karşılaşılan ilk kötücül yazılım olmaları dışında; belirgin karakteristik özellikleriyle bilgi ve bilgisayar güvenliğine karşı önemli tehditler içeren ve oldukça yaygın bir şekilde kullanıcıların maruz kaldığı yazılımlardır. Aşağıdaki kısımda kötücül yazılımlar kısaca açıklanmıştır.

### 3.1. Bilgisayar Virüsleri (Computer Viruses)

Virüsler, en tehlikeli ve en eski kötücül yazılım olarak kabul edilmektedirler. Organizmalardaki hücrelere bulaşan küçük parçacıklar olarak tanımlanan biyolojik virüslerden esinlenerek adlandırılan bilgisayar virüsleri, kendi kopyalarını çalıştırılabilir diğer kodlara veya belgelere yerleştirilerek yayılan ve kendi kendine çoğalan programlardır[7,8].

### 3.2. Bilgisayar Solucanları (Computer Worms)

Bilgisayar virüslerine benzer bir yapıda olan solucanlar, virüsler gibi bir başka çalıştırılabilir programa kendisini iliştirmez veya bu programın parçası olmazlar. Solucanlar, yayılmak için başka bir programa veya virüslerde olduğu gibi insan etkileşimine ihtiyaç duymayan, kendi kendini çoğaltan bir yapı arz ederler [9]. Bir solucanın yayılmasında kullandığı en yaygın yöntemler arasında, e-posta, FTP ve HTTP gibi Internet hizmetleri bulunmaktadır[10].

### 3.3. Truva Atları (Trojan Horses)

Yunan antik şairlerinden Homeros'un yazmış olduğu Odise adlı eserde: Yunanlıların Truva şehrini on sene boyunca kuşatmalarına rağmen şehri ele geçirememişlerdir. Bunun üzerine içine bir kaç düzine askerin saklandığı dev boyda bir atı hediye olarak kalenin içine sokmayı başardıkları ve gece geç vakitte at içinde saklanan askerlerin kalenin kapılarını içerden açarak şehrin ele geçirilmesini sağladıkları yazılmaktadır [11]. Tarihte birçok örneği görülen bu gizleme hilesini kullanan kötücül yazılımlar, bu efsanenin ismi ile anılmaktadır. Truva atları meşru yazılım gibi gözüken kötücül yazılımlardır. Son zamanlarda tersi de geçerli olan örnekler bulunsa da; Truva atları, virüsler gibi kendi kendine çoğalmayan yazılımlardır. Bir Truva atı faydalı bir programa "bohçalanabileceği" (bundling) gibi; kullanıcıları, faydalı bir işleve sahip olduğunu ikna edip, bizzat kullanıcı tarafından çalıştırılmaları ile de etkinleştirilirler[12].

### 3.4. Casus Yazılımlar (Spyware)

Casus yazılımlar, virüs ve solucanlardan farklı olarak hedef sisteme bir kez bulaştıktan sonra kendi kopyasını oluşturarak daha fazla yayılmaya ihtiyaç duymazlar. Casus yazılımın amacı kurban olarak seçilen sistem üzerinde gizli kalarak istenen bilgileri toplamaktır. Bu bilgi kimi zaman bir kredi kartı numarası gibi önemli bir bilgi bile olabilir [13]. Bunun dışında, ticari firmalar Internet üzerindeki kullanıcı alışkanlıklarını saptamak amacıyla casus yazılımları Internet üzerinde yayabilmektedirler [14]. Kullanıcıların haberi olmadan sistemlere bulaşabilen casus yazılımlar, kişisel gizliliğe karşı gerçekleştirilen en önemli saldırılardan biridir [9].

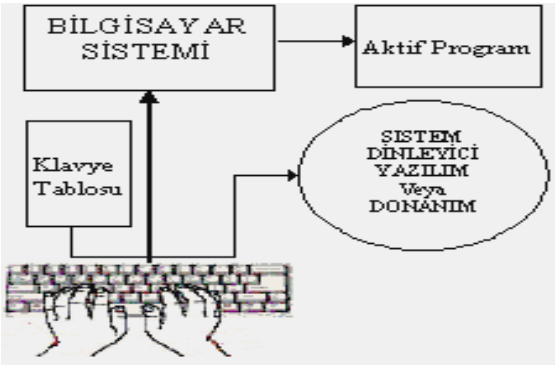
### 3.5. Arka Kapılar (Backdoor)

Bilgisayar üzerinde sıradan incelemelerle bulunamayacak şekilde, normal kimlik kanıtlama süreçlerini atlamayı veya kurulan bu yapıdan haberdar olan kişiye o bilgisayara uzaktan erişmeyi sağlayan yöntemler, arka kapı olarak adlandırılmaktadır. Bir sisteme sızmak için oldukça zahmetli bir çaba harcayan korsanlar, daha sonra aynı sisteme erişmek için daha kolay bir yolu sisteme eklemek isterler. En sık karşılaşılan arka kapı yöntemi, hedef sistemde, dinleme ajanı iliştirilmiş bir kapıyı (port) açık tutmaktır. Bu açıdan bakıldığında, bu tür bir açığa maruz kalındığından

emin olmak için, sistemde mevcut bulunan bütün kapılar, 1'den 65535'e kadar, iki kere (bir kez TCP bir kez de UDP için) taranmalıdır [15]. Arka kapılar kimi zaman, sistemi geliştiren programcı tarafından test edilen sisteme erişmek amacıyla kullanılan fakat daha sonra unutulan açıklar olarak karşımıza çıkmaktadır. Bu durumun bir şekilde farkına varan kötü niyetli kişiler, bu yapıları kullanabilirler. Hatta bu tip arka kapılar bazen programcı tarafından kasten bırakılabilmektedir [16].

### 3.6. Klavye Dinleme Sistemleri (Keyloggers)

Ortaya çıkan ilk türleri açısından ve en temel işlevi bakımından, kullanıcının klavye kullanarak girdiği bilgileri yakalayıp, tutan ve bunları saldırgana gönderen casus yazılımlardır. Saldırganlar istedikleri zaman bunlara ulaşıp yazılan her tür bilgiyi görebilirler. Bu yolla e-mail şifresi, kredi kartı numarası gibi hayati önem taşıyan bilgiler çalınabilir. Son zamanlarda birçok keylogger program bilgisayardan anlık görüntüler yakalayabilmekte ve bu sayede o anda ne yapıldığını, şifrelerin nereye yazıldığını da kolaylıkla gösterebilmektedirler. Ayrıca bazıları bu bilgileri e-posta yoluyla da gönderebilme yeteneğine sahiptir. Mutlaka dikkat edilmesi gerekmektedir. Klavye Dinleme Sistemleri, Şekil 1'de verilmiştir.




Şekil 1. Klavye dinleme sistemleri
(Figure 1. Keyloggers)

Keylogger türü yazılımlar sisteme 2 şekilde girebilir.

- Kötü niyetli kişiler tarafından yazılan ve işletim sistemlerinin açıklarından yararlanılarak hedef bilgisayarın kısmen veya tamamen yönetici haklarını saldırgana teslim eden truva atı (trojan) adlı yazılımlar aracılığıyla keylogger yazılımları sisteme yüklenebilir.
- Keylogger yazılımı bilgisayara kullanıcı tarafından yüklenebilir.

Keylogger yazılımlara örnek olarak:

- iSpyNow
- Perfect Keylogger
- Phantom

gibi yazılımlar verilebilir.

### 3.7. Görüntü Yakalama Sistemleri (Screen Logger)

Screen Logger da key logger ile aynı temel mantığa dayanır. Ancak Screen Logger programlar ile taşınabilen data yalnız klavyenizde yaptığınız tüm vuruşlarla sınırlı olmayıp ekran görüntülerinizi de içerir. Fare ile ekranda bir noktaya tıklamanız ile beraber aynı anda Screen Logger, adeta ekranın tamamının ya da küçük bir bölümünün (genellikle fare merkezli olarak küçük bir dörtgenin) o anki resmini çekerek bunları Internet ortamında sabit bir adrese iletir.

### 3.8. Kök Kullanıcı Takımları (Rootkit)

UNIX işletim sistemlerinde yönetici anlamına gelen "root" isminden gelen kök kullanıcı takımları, saldırganın bir sistemin kontrolünü ele geçirdikten sonra, bilgisayar sistemine eklenen yazılımlardır. Takımda yer alan araçlar arasında, kayıt (log) girdilerini silerek veya saldırgan işlemlerin gizleyerek, saldırının izlerini temizleyen araçlar ve saldırganın sisteme daha sonraki girişlerini kolaylaştıracak arka kapıları düzenleyen araçları sayılabilir [15,17]. ps komutu saldırgana ait kötücül işlemlerin saklamak için; ls komutu gizlenmesi gereken dosya ve dizinleri saklamak için; du komutu saldırgan program ve kök kullanıcı takımları tarafından kullanılan disk alanını saklamak için değiştirilmektedir [18]. Çekirdek seviyesinde kök kullanıcı takımları, işletim sistemine çekirdek (kernel) seviyesinde çengel (hook) attıklarından, fark edilmeleri oldukça güçtür. UNIX ve türevi işletim sistemleri dışında Windows 2000 ve NT sistemleri için de kök kullanıcı takımları Internet üzerinde rahatlıkla elde dilebilmektedir [13].

### 3.9. Korunmasızlık Sömürücüleri (Exploits)

Belirli bir güvenlik korunmasızlığını hedef alan türde saldırılar üretebilen kötücül yazılımlardır. Bu tür yazılımlar sadece bu korunmasızlığın varlığını bütün dünyaya göstermek amacıyla yazıldığı gibi; ağ solucanları gibi zararlı programların bulaşma yöntemi olarak da kullanılabilirler. Bir açıdan bakıldığında korunmasızlık sömürücüleri, ilgili olduğu işletim sistemini veya programı üreten firmanın bu tür açıkları kapatmak için harekete geçirten bir etkendir [19].

### 3.10. Şifre Yakalayıcılar ve Şifre Soyguncular (Password Capture and Password Hijacker)

Sistemde girilen şifreleri yakalayıp kaydetmeye yönelik çalışan casus programlardır. Bu tür programlar konak içinde çalışabileceği gibi ağ üzerindeki paketler içinde hesap ve şifre bilgilerini saptayıp, elde edebilmektedirler [13].

### 3.11. Şifre Kırıcılar (Password Cracker)

Kaba kuvvet ve sözlük tabanlı deneme yanılma yöntemlerini de içeren; bir şifreyi veya şifreli bir dosyanın şifresini çözen araçlardır [20,21]. Şifre kırıcılar, güvenlik yöneticileri tarafından meşru bir biçimde, kullanıcılar tarafından tanımlanmış olan zayıf şifrelerin bulunması ve bu şifrelerin değiştirilmesinin, daha güvenilir bir sistem oluşturmak için, kullanıcıdan talep edilmesi için de kullanılabilmektedir [22].

### 3.12. Web Böcekleri (Web Bugs)

İz sürme böceği (tracking bug), piksel etiketi (pixel tag), web feneri (web beacon) veya temiz GIF (clear GIF) olarak da bilinen web böceği, HTML tabanlı bir e-posta mesajını veya bir web sayfasını kimlerin, kaç kez görüntülediği ve mesajla ne kadar süre ilgilendiği gibi bilgileri elde etmek amacıyla kullanılan ilginç ve sıradan kullanıcı tarafından pek bilinmeyen bir tekniktir. [23]. Bu tür bir mesajı açan kişi, en azından kendi e-posta adresinin geçerli ve kullanılan bir adres olduğunu karşı tarafa ifşa etmektedir. Bu şekilde ileride birçok mesaj aynı e-posta adresine gönderilebilir. Web sayfaları ve e-postalar dışında Microsoft Word, Excel ve PowerPoint gibi ofis programı belgelerinde de web böceği uyarlamasının gerçekleştirilmesi mümkündür[24].

### 3.13. Sazan Avlama (Phishing)

Dilimizde kullanılmak amacıyla "sazan avlama" olarak bir karşılık önerilen phishing, kimlik hırsızlığı (identity theft) adı verilen banka hesap numaraları, kredi kartı numaraları gibi kişisel bilgilerin, banka gibi resmi bir kurumdan gerçekten gönderilen resmi bir mesaj gibi gözüken

e-postalarla kişilerden elde edilmesidir. Sosyal mühendisliğin bir uygulama alanı olan bu tür sahte epostalarını alan kişi, istenilen gizli bilgileri göndererek, bu bilgilerin kötü niyetli üçüncü şahısların eline geçmesine ve akabinde oluşabilecek zararlara maruz kalınmasına neden olacaktır [25]. Amerika'da 57 milyon insanın farklı teknikler kullanılarak sazan avlamaya maruz kaldığı ve sazan avlama sebebi ile 2003 yılında 500 milyon $'lık bir kayıp ortaya çıktığı rapor edilmiştir [26].

### 3.14. Web Sahtekârlığı ve Dolandırıcılığı (Web Scam and Fraud)

Internet üzerinden veya e-posta ile yapılan bir dolandırıcılık türüdür. Genellikle İngilizce olarak yazılmasına karşın ileride ülkemizde de bu tür sahtekârlıklara rastlanacağı tahmin edilmektedir. Kişileri maddi veya manevi zararlara uğratacak türde etkileri olan ve Internet üzerinde yapılan girişimler web sahtekârlığı olarak adlandırılmaktadır. Nijerya yatırımı (Nigerian investment), saadet zinciri ya da piramit entrikası (pyramid schemes) ve mektup zinciri (chain letters) en sık rastlanan web sahtekârlıklarındandır. Ülkemizde de örneklerine rastlanan mektup zinciri, gönderilen kişiye maddi zarara uğratmaz; fakat bu kişi aldığı mesajı örneğin 10 kişiye göndermezse pek yakında kötü bir felakete uğrayacağı şeklinde korkutularak zincirin devamı sağlanır. Bu tür mesajlar hiçbir şekilde ciddiye alınmamalıdır [27].

### 3.15. Casus Yazılım Çerezleri (Spyware Cookie)

Sitelerin Internet üzerinde daha kullanışlı bir hizmet vermek amacıyla kullandıkları çerezler, kötü amaçlara da hizmet verebilmektedir. Kişisel kullanıcı bilgilerinin elde edilmesi ve paylaşılması amacıyla bu çerezler kullanılabilmektedir.

## 4. UYGULAMANIN GELİŞTİRİLMESİ (DEVELOPMENT OF APPLICATION)

Son dönemde İnternet ortamında artış gösteren dolandırıcılık olaylarına karşı bir takım ek önlemler alınmıştır. Genellikle dolandırıcılık girişimleri;

- Kullanılan e-mail adreslerine gönderilen virüslü program'ların çalıştırılması
- İnternet üzerinde faydalı veya eğlenceli gözüken bazı oyun ya da programların bilgisayara indirilmesi
- Sohbet odaları bağlantısı sırasında bilgisayara virüslerin yüklenmesi, aracılığı ile Kullanıcı Kodu ve şifrenin bilgisayar klavyesinden tıklanması sırasında veya bu girişlerin ekran görüntülerinin kaydedilmesi yöntemi ile gerçekleştirilmektedir.

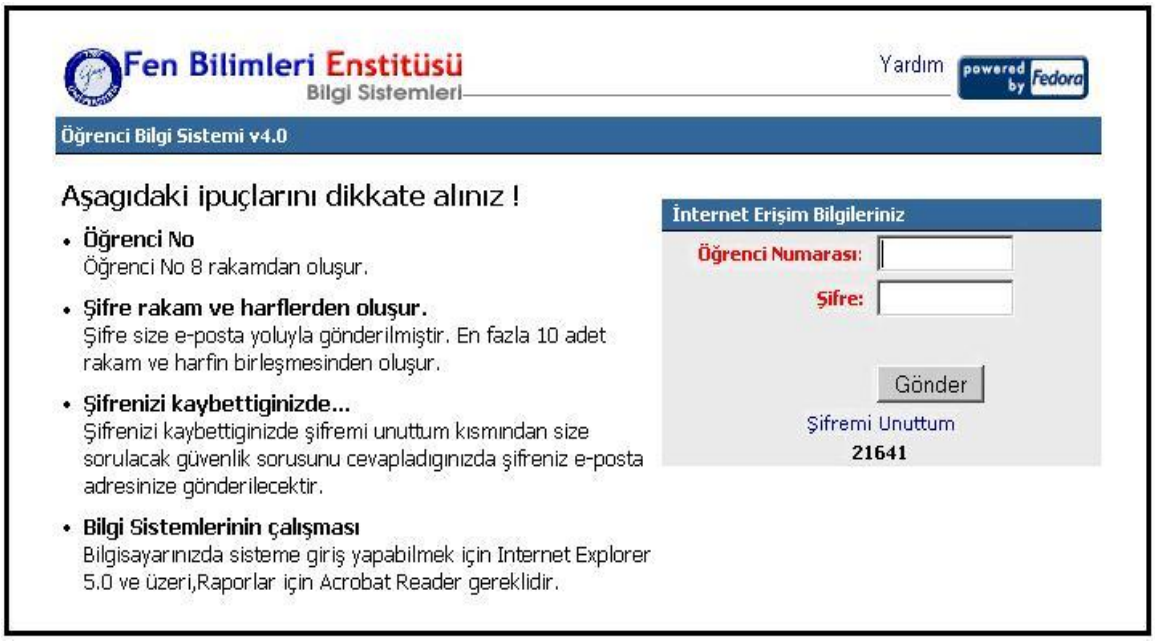
Sanal klavye, bilgisayardaki fiziksel klavyeyi kullanmadan, bilgisayarın fare'sini kullanarak ekrandan şifre girişini sağlayan ek bir güvenlik önlemidir. En çok kullanım yerleri internet bankacılığı uygulamalarıdır.

Sanal Klavye, bilgisayara bilginiz dışında yüklenebilecek ve şifre bilgilerini çalmaya yönelik olan "keylogger" programlarına karşı korunmak amacı ile geliştirilmiştir. Bu tip programların yüklü olduğu bilgisayarlarda, kullanıcının klavyede basmış olduğu her tuş bu program aracılığıyla kaydedilmektedir. Özellikle genel kullanıma açık, Internet cafe gibi yerlerde bu nitelikteki programların bilgisayarlara yüklenmiş olma riski fazladır. Fare kullanılarak Sanal Klavye ile şifre girişi yapıldığında, gerçek klavye kullanılmadığı için programın şifreyi yakalaması mümkün olmamaktadır.

Bu makalede kötücül yazılımlara karşı geliştirilmiş bir sanal klavye uygulaması gerçekleştirilmiştir. Yapılan uygulama sayesinde key logger, truva atları, casus yazılımlar vb. kötücül yazılımların girilen şifreyi edinmesi engellenmiştir. Diğer birçok sanal klavyeden farklı olarak sanal klavyedeki sürekli değişen tuş yerleri ile screen logger programları ile şifrenin tespiti imkânsız hale getirilmiştir. Ayrıca klavyeye verieln bir

özellikle ile tuşlara tıklamadan üzerinde bekleyerek şifre girişi sağlanmıştır.

Uygulamanın test edilmesi için, sanal klavye Fen Bilimleri Enstitüsü'nün öğrenci bilgi sisteminin girişine yerleştirilmiştir. Bu sayfanın web adresi https://www.fbe.gazi.edu.tr/ogrenci/bbg/ dir. Ayrıca, Şekil 2'de resmedilmiştir.




Şekil 2. Şifre giriş ekranı
(Figure 2. Password entry screen)

Sanal klavye uygulaması java script dili kullanarak gerçekleştirilmiştir. Hemen hemen tüm web tarayıcıların tüm sürümlerinde çalışmaktadır. Klavyenin biçimsel özellikleri ise CSS kullanılarak gerçekleştirilmiştir ve tüm sitelerde küçük renk ve font değişiklikleri ile kullanılabilmesi sağlanmıştır. Şekil 3'te sanal klavyenin ekranda görüntüsü yer almaktadır.


Şekil 3. Sanal klavye görüntüsü 1
(Figure 3. Virtual keyboard screenshot 1)

Yukarıdaki şekilde herhangi bir tuşa basıldığı zaman klavyede bulunan tüm karakterler Şekil 4'te görüldüğü gibi yıldız (*) karakterine dönüşecek ve sonra kendiliğinden tüm rakam ve harflerin yerleri Şekil 5'te görüldüğü gibi karışacaktır.


Şekil 4. Sanal klavye görüntüsü 2
(Figure 4. Virtual keyboard screenshot 2)


Şekil 5. Sanal klavye görüntüsü 3
(Figure 5. Virtual keyboard screenshot 3)

Yukarıda anlatıldığı gibi, klavye üzerindeki bütün rakam ve harfler otomatik olarak değişmiştir. Bu durum mevcut sanal klavyelerde bulunmamaktadır. Özellikle de her tuş basımında karakterlerin * şekline dönüşmesi ve karakterlerin yerinin değişmesi screen logger programlarını da etkisiz hale gelmiştir.

Ayrıca, kullanıcı her şifre alanına tıkladığında sanal klavye ekranın farklı bölgesinde açılacaktır. Bu sayede ekranda fare' nin tıklandığı yerin piksel değerlerine bakarak hangi karaktere tıklandığını tahmin etmeye çalışan casus yazılımlar etkisiz hale gelecektir.

Gerçekleştirilen Sanal Klavye 2 farklı şekilde kullanılabilir.

Tıklayarak Giriş: Sanal Klavye üzerinden istenilen harfleri/rakamları tıklamak suretiyle giriş yapılabilir.

Harf/Rakam Üzerinde Bekleyerek Giriş: Tuşlara tıklama yapmadan farenin oku harfler/rakamlar üzerinde 1.5 saniye bekletildiğinde, şifre giriş kutusunun yanında 1 saniye boyunca kırmızı renkte uyarı verilecek ve o harf/rakam tıklanmış gibi şifre hanesine otomatik olarak yazılacaktır.

Kullanıcı kodundaki veya şifredeki küçük harfleri girmek için "Küçük Harf" butonuna, büyük harfleri girmek için ise "Büyük Harf" butonuna basarak klavyenin istenilen durumda kullanılması sağlanabilir.

Şifre girişinde, hatalı yazılmış karakterleri silmek için "Sil" düğmesini kullanılabilir.

Sanal klavye'nin sağ üst kısmında bulunan sabitle butonu yardımı ile klavyedeki karakterleri Şekil 6'da görüldüğü gibi Q klavye tuş dizilimine göre sabitleyerek şifre girilebilir. Ancak bu durumda screen logger ile tıklanan tuşların yerlerin tahmin edilmesi mümkün olacağından tavsiye edilmez. Güvenlik için sanal klavyeyi karıştır metodu ile kullanılması önerilir.


Şekil 6. Sanal klavye görüntüsü 4
(Figure 6. Virtual keyboard screenshot 4)

Kullanıcının klavye kullanımında karşılaşabileceği sorunlarda kendisine yardım edecek bir yardım sayfası da hazırlanmıştır. Gerçekleştirilen uygulama tarayıcının görüntülediği html sayfası, sayfaya ait renk kodlamaları ve arka plan görünümü için css kodu ve işlemin gerçekleştirilmesini sağlayan javascript kodlarından oluşmaktadır. Anlaşıldığı gibi asıl önemli işlevi gerçekleştiren sanalklavye.js adlı javascript dosyasıdır. Modülerlik açısından daha okunabilir dosya oluşturmak için tüm işlemler fonksiyonlar yardımıyla gerçekleştirilmiştir. Bu dosyada 23 tane değişken ve 25 tane fonksiyon kullanılmıştır. Örneğin, herhangi bir tuşa basıldığında sanal klavyede * karakterlerinin oluşmasını sağlayan fonksiyon aşağıda verilmiştir.

```
function HideShowLetters(isState) {
      var mystrn
      var tempStr
      for(var i=0;i<kybrdCntrl.length;i++)
      {
            if (isState =="0"){
                  mystrn=  "thisform.kpbtn"  +  kybrdCntrl[i]  +  ".value  =
'*';"
            }
            else
            {
                  tempStr = kybrdCntrlValues[i];
                  if (i==0 && newSbt)
                        tempStr=kybrdCntrlValues[4];
                  if (i==1 && bk == 'b')
                        tempStr=kybrdCntrlValues[5];
                  mystrn= "thisform.kpbtn" + kybrdCntrl[i] + ".value = '" +
tempStr + "';";
            }
            eval(mystrn);
      }
      for(var i=0;i<kybrd.length;i++){
            if (isState =="0"){
                  mystrn= "thisform.kpbtn" + i + ".value = '*';"
            }else{
                  mystrn= "thisform.kpbtn" + i + ".value = thisform.kpbtn"
+ i + ".alt;"
            }
            eval(mystrn);
  }

  }
```

Diğer fonksiyonlar ve işlevleri de Tablo 1'de belirtildiği gibidir.

Tablo 1. Fonksiyonlar ve işlevleri
(Table 1. Functions and duties)

| | |
|---|---|
| function browserDetect() | Tarayıcının versiyonunu kontrol eder. |
| function hideKeypad() | Sanal klavyeyi saklar. |
| function ClickRadio(rvalue) | |
| function showKeypad(thisObj) | Sanal klavyeyi görünür yapar |
| function startDrag(e) | Sanal klavye, fare ile sürüklenmeye başlarken x,y pozisyonlarını alır. |
| function drag(e) | Sanal klavye, fare ile sürüklenirken farenin yeni konumu için sanal klavyeyi konumlandırır. |
| function endDrag() | Sanal klavyenin fare ile sürüklenmesi bittiğinde Sanal klavye referans nesnesini siler. |
| function nextElement() | Finds next password textbox |
| function girisClick() | giris_click event handler |
| function ClickEvent(keyvalue,kindex) | Sanal klavye tuşlarına basıldığında şifre alanına tuş değerinin yazılması sağlar. |
| function CallOverEvent(keyvalue,kindex,keyobj) | Sanal klavye tuşları üzerinde beklendiğinde şifre alanına tuş değerinin yazılması sağlar. |
| function BtnCptChange() | Karıştır/Düzenle tuşunun başlığını düzenler |
| function SetMixButtonCaption() | |
| function changeLetters() | Büyük/Küçük harf çevrimi yapar. |
| function changeActLetter(actLet) | Tek bir harf için küçük büyük harf çevirimi yapar. |
| function CallOutEvent(keyvalue,keyobj) | Sanal klavye tuşları üzerinde beklendiğinde başlatılan şifre alanına tuş değerinin yazılması işlemini bitirir |
| function AddPass(keyvalue,kindex) | Şifre alanına tuş değerinin yazılmasını sağlar. |
| function DeletePass() | Şifre alanına girilen en sağdaki değeri siler. |
| function disableImages() | Kullanıcı girişe bastığında tüm resim butonların pasif edilmesini sağlar. |
| function SubmitForm() | sanal klavye üzerinden siteye girişe izin verir. |
| function SKYardim() | Sanal Klavye Yardım sayfasını açar. |
| function SanalKlavye() | Sayfa ilk açıldığında Sanal klavye'nin oluşturulması, büyük/küçük harf ve karıştır/düzenle işlemlerinde sanal klavyenin yeniden dizayn edilmesi işlemlerini yapar. Javascript dosyasındaki en uzun ve en önemli fonksiyondur. |
| function vk_GetCookie(name) | |
| function vk_getCookieVal(offset) | |

## 5. SONUÇLAR (RESULTS)

Bu çalışmada, bilgi ve bilgisayar güvenliğini tehlikeye sokan kötücül ve casus yazılımlar araştırılmış, incelenmiş, sınıflandırılmış ve karşılaşılabilecek tehlikeler göz önüne serilmiştir. Bilgisayar kullanıcılarının karşılaşabilecekleri tehlike ve tehdidin boyutlarını ayrıntılı bir biçimde sunmak, bu çalışmanın diğer bir önemli katkısı olarak değerlendirilmektedir. İnceleme sonucunda; bilginin ve teknolojinin iç içe olduğu, baş döndürücü bir hızda gelişen elektronik ortamlarda, her zaman yanı başımızda olacak bilişim korsanları gibi kötü niyetli kişilerin ve sistemlerin açığını bulmada, bu açıkları kullanıp sistemlere izinsiz erişmede, sistemlere ve sistemi kullanan kişilere, kişisel veya kurumsal zarar vermede hemen hemen her yolu denemeye çalıştıkları tespit edilmiştir. Bu saldırılara ve tehditlere karşı tedbir alınabilmesi için, bu tür yazılımların ve kullandıkları yöntemlerin sürekli olarak incelenmesi gerektiği, elde edilen bulgular arasındadır.

Dünyada ve ülkemizde kötücül ve casus yazılımların yaygın olarak kullanımda olduğu, fakat kullanıcıların bu tehlike ve tehditlerinden çoğunlukla haberdar olmadığı anlaşılmıştır. Kişisel veya kuramsal her hangi bir zararla karşılaşılmaması için, konuya gereken önemin verilmesi, bilgi birikiminin arttırılması, hassasiyet gösterilmesi ve gereken önlemlerin alınması gerekmektedir.

Bu çalışmada, sahip oldukları karakteristiklerinin, kullanım amaçlarının, var olan çeşitlerinin ve kullandıkları yöntemlerin özetlendiği en genel kötücül yazılımlar arasında yer alan; virüsler, solucanlar, Truva atları, arka kapılar, kök kullanıcı takımları, korunmasızlık sömürücüleri, klavye dinleme sistemleri, görüntü yakalama sistemleri, tarayıcı soyma ve casus yazılımlardan bahsedilmiştir.

Ayrıca, gerçekleştirilen uygulama sayesinde İnternetten girilen bilgilerin (e-posta, şifre, kredi kartı no) güvenilirliği üst seviyelere çıkmıştır. Bu uygulamayla birlikte, Key loger, screen loger vs yazılımlarla şifrelerin çalınma olasılığı ortadan kalkmaktadır. Tüm şifreli giriş ekranlarında kullanılabilir. Ccs dosyasındaki küçük değişikliklerden sonra tüm sitelere uyumlu hale gelebilir. Web Sitesine SSL desteği verildiğinde güvenlik daha üst seviyelere çıkmaktadır.

**KAYNAKLAR (REFERENCES)**

1. Canbek G., Sağıroğlu Ş., (2006). Bilgi ve Bilgisayar Güvenliği, Ankara, Ağustos 2006.
2. Canbek, G., (2005). Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, 13, 31-32, 43, 50, 58, 154, Eylül 2005.
3. Calder, A., Watkins, S., (2003). It Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799, Kogan Page, 14, 163, September 1, 2003.
4. Thompson, R., (2005). The Four Ages of Malware, Infosecurity Today, 47-48, March/April, 2005.
5. Internet: Internet Bankacılığı ve Güvenlik, http://www.tbb.org.tr/turkce/guvenlik/internet%20bankaciligi%20ve%20guvenlik, Haziran 2009.
6. Heiser, J.G., (2004). Understanding Today's Malware, Information Security Technical Report. Vol. 9, No. 2, 47-64, April-June 2004.
7. Peikari, C., Fogie, S., Maximum Wireless Security, Sams Publishing, 153, 164, December 18, 2002.
8. Skoudis, E., Malware: Fighting Malicious Code, Prentice Hall PTR, 13, 96, 123-125, 149-151, 179, November 7, 2003.
9. Gustin, J., Cyber T., Marcel D., (2003). 26-27, October 15, 2003.
10. Russell, D., Gangemi, Sr. G.T., Computer Security Basics, O'Reilly, 82, July 1, 1991.
11. Thompson, D.P., (2004). The Trojan War: Literature and Legends from the Bronze Age to the Present, McFarland & Company, 33, January 6, 2004.
12. Internet: Trojan Programs, VirusList, (2005). http://www.viruslist.com/en/virusesdescribed?chapter=152540521, Eylül 2005.
13. Hansen, J.B. and Young, S., (2003). The Hacker's Handbook, CRC Press, 72-74, 126, 530, 714, November 24, 2003.
14. Conway, R., Cordingley, J., (2004). Code Hacking: A Developer's Guide to Network Security, Charles River Media, 55-56, 92, May 1, 2004.
15. Cole, E., (2001). Hackers Beware: The Ultimate Guide to Network Security, Sams Publishing, 104-108, 191-193, 544, 550, August 13, 2001.
16. Hansche, S., Berti, J., and Hare, C., (2003). Official (Isc) 2 Guide to the Cissp Exam, CRC Press, 590, December 15, 2003.

17. Bishop, M.A.,(2002). Computer Security: Art and Science, Addison-Wesley Professional, 724-725, December 2, 2002.
18. Tipton, H.F., Krause, M., (2003). Information Security Management Handbook, CRC Press, 132, 1254-1255, December 30, 2003.
19. Russell, R., (2001). Hack Proofing Your Network, Syngress Publishing, 78, January 1, 2001.
20. Poole, O., (2002). Network Security: A Practical Guide, Elsevier, 69-71, December 9, 2002.
21. Pipkin, D.L., (2002). Halting the Hacker - A Practical Guide to Computer Security, Prentice Hall PTR, 52, August 26, 2002.
22. Bace, R.G., (1999). Intrusion Detection, Sams Publishing, 151, December 22, 1999.
23. Mena, J., (2004). Homeland Security Techniques and Technologies, Charles River Media, 47-48, May 10, 2004.
24. Vacca, J.R., (2005). Computer Forensics – Computer Crime Scene Investigation, Charles River Media, 489-490, May 1, 2005.
25. Bennett, J., (2004). Digital Umbrella: Technology's Attack on Personal Privacy in America, Brown Walker Press (FL), 47-50, September 1, 2004.
26. Gralla, P., (2005). Windows XP Hacks, O'Reilly, 152- 157, April 1, 2005.
27. Internet: Consumer Online: Home > Scams > Major Scams, http://www.consumer.org.nz/topic.asp?docid=253&category=&subcategory=&topic=Scams&title=Major%20Scams&contenttype=summary, Eylül 2005.