Kötücül ve Casus Yazılımlara Karşı Elektronik İmzanın Sağlamış Olduğu Korunma Düzeyi

Gürol CANBEK, Şeref SAĞIROĞLU,

***Özet*—Kötücül ve casus yazılımlar, bilgi ve bilgisayar güvenliğine yönelik en ciddi ve oldukça tehlikeli tehditlerin başında gelmektedir. Bu bildiride; e-ticaret, e-devlet gibi pek çok güncel uygulamalarda etkinlik, güvenilirlik ve hız kazandırmak amacıyla uygulanıp yaygınlaşması beklenen ve planlanan elektronik imzanın, bu tür kötü niyetli yazılımlar karşısında sahip olduğu korunma ya da korunmasızlık düzeyi ele alınmıştır. Bu çalışmanın; gittikçe yaygınlaşmakta olan kötücül ve casus yazılımların, elektronik imzaların oluşturma ve kullanımı sürecine olan etkilerinin hiç bir şekilde göz ardı edilmemesi ve gerekli önlemlerin alınmasına olan acil ihtiyacı işaret etmesi açısından kayda değer sonuçlar sunduğu değerlendirilmektedir.**

***Anahtar Kelimeler*—E-imza, kötücül yazılım, casus yazılım, bilgi ve bilgisayar güvenliği, kişisel gizlilik**

The Level of Protection of E-sign Against Malware and Spyware

***Abstract*—Malware and spyware are the most critical, very dangerous and the foremost attacking structures against information and computer security. Electronic signature (e-sign) is expected and planned to be used widespread in order to provide efficiency, reliability, and rapidity in the applications such as e-commerce and e-government. In this paper, the level of protection and the level of vulnerabilities of e-sign against malicious software are studied. This paper concludes that it is necessary not to ignore the negative effects of malware on signature creation applications and it points out the urgent necessity to take measures noteworthy.**

***Keywords*—E-sign, malware, spyware, information and computer security, privacy**

I. GİRİŞ

Bilişim teknolojilerinin gittikçe geliştiği ve yaygınlaştığı günümüzde; insanların hayatları da bu teknolojileri en etkin bir şekilde kullanacak şekilde değişmektedir. İnternet'in yaygınlaşması sonucunda, kişiler ve kurum ve kuruluşlar arasında güvenli ve hızlı bir etkileşimi sağlamak amacıyla ortaya çıkan elektronik imza (e-imza); yakın zamanda insanların hayatını kökten etkileyecek bu tür teknolojilerden biri olarak gözükmektedir. E-imza, özellikle e-ticaret kapsamında firmadan müşteriye (B2C, business–to-consumer) ve firmadan firmaya (B2B, business–to–business) ticaret uygulamalarına ait ticaret sözleşmeleri ve hareketlerinde ve e-devlet kapsamında vatandaş ile devlet kurum ve kuruluşları arasındaki idari, hukuki ve mali iş ve işlemlerde önemli imkanlar vaat etmektedir. Gelişen kimi teknolojilerin daha önceden kullanıla gelen yerleşmiş köklü yapıların yerini aldığı düşünülürse; e-imzanın da ıslak imzanın yerini alacak güçlü bir aday olduğunu görmek gerekir. Her tür yenilikte olduğu gibi; bu süreç, doğal olarak kolay ve sorunsuz olarak gerçekleşmeyebilmektedir.

İnsanların kullanımına sunulan birçok yeni teknolojik altyapının sergilediği kolaylık ve kullanılışlığı gölgeleyebilecek en önemli etkenlerin başında, bilgi ve bilgisayar güvenliği gelmektedir. E-imzanın gerek kişisel ve gerek kurumsal alanda yaygınlaşabilmesi ve var olan geleneksel yapının yerini alabilmesi için yerine getirilmesi gereken en önemli şart, bu teknolojiye olan itimadın toplum içerisinde yaygınlaşması ve bir daha zarar görmeyecek şekilde sağlam bir biçimde yerleşmesidir. Günümüzde artan sayıda ülkede bir belgenin elektronik olarak imzalanmasının yasal sonuçları bulunmaktadır. Ülkemizde de bu durum, Ocak 2004 tarihinde kabul edilen 5070 sayılı Elektronik İmza Kanunu'na göre, "Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur" şeklinde açık olarak belirtilmektedir [1]. Bunun için e-imza kullanımında karşılaşılabilecek güvenlik tehdit ve risklerinin belirlenmesi ve bunlara karşı korunma sağlayacak güvenlik alt yapısının oluşturulması ve kullanıcılara sağlanması gerekmektedir. Bu konu hiçbir şekilde göz ardı edilemeyecek kadar önemlidir.

Bilgi ve bilgisayar güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme zemini oluşturma çabalarının tümüdür. Bunun sağlanması için, uygun güvenlik politikaları belirlenmeli ve uygulanmalıdır [2]. E-imza uygulamalarında, bilgi ve bilgisayar güvenliğinin bütün etkenleri ve kapsamıyla ele alınması gereklidir.

Elektronik imza oluşturan yazılım ve donanımlar olarak tanımlanan imza oluşturma uygulamalarını (İOU) güvenli hale getirmek için ortaya atılan yaklaşımların çoğu, kullanılan şifreleme algoritmaları ve akıllı kart içinde gerçekleştirilen

Gürol CANBEK, *Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, 06570 Maltepe, ANKARA, gurol44@gmail.com,*

Şeref SAĞIROĞLU, *Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, 06570 Maltepe, ANKARA, ss@gazi.edu.tr*

hesaplamaların güvenliği üzerine yoğunlaşmaktadır. Tamsayıların çarpanlarına ayrılması, ayrık logaritma ve eliptik eğrilere dayanan yöntemler ile bu konuda önemli aşamalar kat edilmiş olsa da; imza oluşturma uygulamasının çalıştığı ortam olan işletim sistemi ve bu ortam içinde bulunduğu diğer yazılımlar, gerek kullanıcılar tarafından gerekse bizzat bu yazılımları üreten firmalar tarafından göz ardı edilmektedir [3]. Avrupa Standartlaştırma Komisyonu'nun (CEN, European Committee for Standardization) 2004 yılında hazırlamış olduğu rapora göre; normal olarak imza oluşturma uygulaması ile aynı ortamda çalışan, fakat elektronik imza oluşturma sürecine doğrudan dahil olmayan sistemler, uygulama programları, çevre birim ve haberleşme kanalları "güvenilmez" olarak ele alınmalıdır [4]. Bu açıdan bakıldığında elektronik imza oluşturma uygulamalarının karşı karşıya olduğu en büyük güvenlik tehlikelerinin başında, kötücül ve casus yazılımlar gelmektedir.

Bu bildiride e-imza oluşturma uygulamaları ve kötücül ve casus yazılımlar arasındaki etkileşim ele alınmıştır. Bu çalışma ile gittikçe yaygınlaşan kötücül yazılımlar karşısında, e-imza oluşturma uygulamaların sergilediği korunma düzeyi veyahut sahip oldukları korunmasızlık ve zayıflıklar işaret edilerek; bu konuda gereken önlemlerin alınmasına yardımcı olmak hedeflenmektedir.

İkinci bölümde, elektronik imza genel hatları ile ele alınmış ve getirmiş olduğu yenilikler ve kullanım alanları aktarılmıştır. Üçüncü bölümde, bilgi ve bilgisayar güvenliğine karşı gerçekleştirilen en önemli saldırılardan, kötücül ve casus yazılımlar tanıtılmış ve bu yazılımların sebep olduğu zararlar ve sergiledikleri karakteristikler özetlenmiştir. Dördüncü bölümde, kötücül ve casus yazılımlar ile e-imza yaklaşımları arasındaki ilişki ve etkileşim ele alınmıştır. Bu yazılımların ne şekilde e-imza güvenliğini sekteye uğratabileceği de işaret edilmiştir. Sonuç bölümünde, yapılan çalışma değerlendirilmiş ve saptanan sonuçlar aktarılmıştır.

II. Elektronik İmza (E-İmza) ve İmza Oluşturma Sürecindeki Genel Güvenlik Ölçütleri

E-imza, 2000 yılı Amerikan E-SIGN (Electronic Signatures in Global and National Commerce, Küresel ve Ulusal Ticaret Elektronik İmza) yasasında "bir kayıt ile mantıksal olarak ilişkilendirilmiş veya bu kayda eklenmiş elektronik ses, simge veya sürecin; bir kişi tarafından, o kaydı imzalamak amacıyla uygulanması veya benimsenmesi" olarak tanımlanmaktadır.

E-imza ile güncel teknolojiler kullanılarak, işlemleri güvenli bir şekilde yapmak; iş verimliliğini arttırmak; iş akışını hızlandırmak; bürokrasiyi azaltmak; dünya ile hızlı bir şekilde bütünleşmek; küresel pazarlara açılmak; kağıttan elektronik belgelemeye geçişi sağlamak mümkün olabilecektir [5].

E-imza, gelişmiş teknolojiler kullanarak, elektronik ortamda gönderilen veya alınan bir bilginin, bunu gönderen kişi veya kuruma ait olduğunun "doğrulanmasını"; bu bilginin başkaları tarafından değil de bildiğimiz kişiler tarafından gönderildiğinin "belirlenmesini"; bilgiyi gönderenin gönderdiğini ve bilgiyi alanların aldıklarını "inkar edememesini"; bilginin içeriğinin "değiştirilememesini"; bilgiyi oluşturan verinin başkaları tarafından bir şekilde elde edilmesi durumunda içeriğinin bu kişiler tarafından "anlaşılamamasını" garanti eden elektronik haberleşme vasıtası olarak açıklanabilir. Bu ifadeler, e-imzanın sağlamış olduğu şu güvenlik unsurlarına karşılık gelmektedir: kimlik kanıtlama, inkâr edememe, bütünlük ve gizlilik.

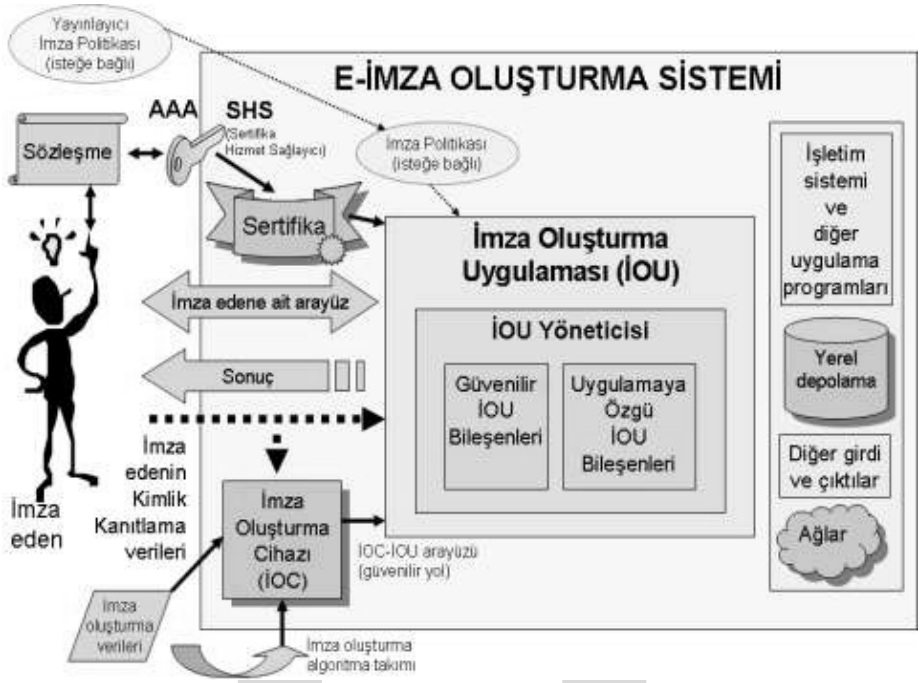
E-imzada bu unsurların sağlanması için, özetleme fonksiyonları veya açık anahtar altyapısı gibi, günümüz bilgi işlem güç ve kapasitesi ile çözülmesi veya kırılması neredeyse imkansız olan şifreleme algoritmaları kullanılmaktadır [6]. Bu açıdan e-imza; şifrelenmiş bilgilerin şifresini kırmak veya çözmek için yapılan, kaba kuvvet, sözlük, ortadaki adam, salt şifreli metin, bilinen düz metin, seçilen düz metin veya şifreli metin saldırıları gibi kriptoanaliz yöntemlerinin kullanıldığı kriptografik saldırılara karşı son derece etkin bir korunma sağlayabilmektedir [7].

E-imza oluşturmanın ön plana çıkan bu mekanizması dışında çok sayıda bileşen ve etkin bulunmaktadır. İmza oluşturma bu bakış açısı ile ele alındığında, bu sürecin tüm öğeleri ile oluşturduğu modelin, tamamının güvenlik açısından ele alınması gereklidir.

Şekil 1'de e-imza oluşturma sürecinin işlevsel modeli gösterilmektedir.

Bu modelden de görülebileceği gibi imza oluşturma işlevleri ile bilgi nesne ve arayüzlerinin hepsi ile ilgili güvenlik hususları söz konusu olabilir. Süreç çok sayıda noktada güvenlik riski ve tehdidi altındadır. Bu noktalardaki korunmasızlık ve zayıflıklardan yararlanan kötücül ve casus yazılımlar, e-imza oluşturma sürecinin güvenliğini tehlikeye sokabilirler.

E-imza oluşturma süreci, güvenlik açısından en geniş çerçevede ele alındığında; çevre etkenleri bakımından iki farklı ortamda, iki farklı güvenlik seviyesine gereksinim duyulmaktadır. Ev ve işyeri gibi ortamlarda e-imza oluşturmada, halka açık ortamlarda e-imza oluşturmadan daha fazla düzeyde güvenlik tedbirine ihtiyaç duyulacaktır. Dolayısıyla, örneğin ev kullanımı için tasarlanmış bir imza oluşturma sisteminin halka açık ortamlarda kullanılması risklidir.



Şekil 1. E-imza oluşturma işlevsel modeli [4]

E-imza oluşturma süreçlerinin güvenlik gereksinimlerini ele alan çeşitli çalışmalar bulunmaktadır. ESIGN Uzman Grubu tarafından, CEN/ISSS için 2001 yılında hazırlanmış olan "Güvenilir İmza Oluşturma Cihazı" raporunda, imza oluşturma sürecini oluşturan güvenlik ortamı ayrıntıları ile mercek altına alınmıştır [8]. Rapora göre, gizliliği temin edilmiş olan şifre veya özel (gizli) şifre anahtarları gibi, imza edenin bir elektronik imza oluştururken kullandığı benzersiz veri olarak tanımlanan İmza Oluşturma Verileri (İOV); dışarı aktarımında bütünlüğü korunmuş olan şifre veya genel (açık) şifre anahtarları gibi, bir elektronik imzayı doğrulamak amacıyla kullanılan İmza Doğrulama Verileri (İDV); PIN kodu gibi girdi olarak sağlanan kimlik kanıtlama verisi veya kullanıcının biyometrik karakteristiklerinden türetilen kimlik kanıtlama verisi anlamına gelen ve uç kullanıcı tarafından imza oluşturma işlemi sırasında girilen Kimlik Kanıtlama Doğrulama Verileri (KKDV) ve uç kullanıcının teşhis edilmesi ve kimliğinin kanıtlanması için kullanılan referans PIN kodu ve biyometrik kimlik kanıtlama referansı olarak tanımlanan Referans Kimlik Kanıtlama Verileri (RKKV) e-imza oluşturma işleminin güvenlik ortamının varlıkları olarak tanımlanmaktadır. Bu güvenlik ortamının özneleri ise; uç kullanıcı veya yönetici ve imza oluşturma sürecini tehdit eden saldırganlar olarak belirlenirse; İOV'nin güvenilir bir biçimde sistemin içerisine aktarıldığı ve sertifika üretme uygulamasının güvenilir biçimde imza edenin adının kimlik kanıtlamasını yaptığı varsayımından hareket edildiğinde, güvenlik tehditleri aşağıdaki şekilde sınıflanmıştır:

ÇİZELGE 1.
E-İMZA GÜVENLİK TEHLİKELERİ

Güvenlik Tehdidi	Açıklama
Fiziksel korsanlık	Fiziksel ortamdaki korunmasızlıkların istismarı
İOV ifşası	İmza oluşturma verilerinin depolanması ve kopyalanması
İOV türetilmesi	İmza oluşturma verilerinin türetilmesi
İOV yayınlaması	İmza oluşturma verilerinin yayınlanması
İmza kalpazanlığı	Elektronik imzanın sahtesinin oluşturulması
İmzanın inkârı	Geçerli elektronik imzanın ret ettirilmesi
İDV kalpazanlığı	İmza doğrulama verilerinin sahtesinin oluşturulması

Söz konusu raporda e-imza oluşturma sürecinde ulaşılması gereken hedefler şu şekilde belirtilmiştir:

- Süreç sırasında ve sonunda ortaya çıkan emarelerden yararlanılarak bir sonuca ulaşılmasını önleyecek veya en azından belirli sınırlar içinde tutacak tasarımın hazırlanması ve uygulanması;
- İlklendirme aşaması ile kullanımda olduğu zamanda ortaya çıkabilecek kusurların saptanabilmesi ve ihraçtan sonra güvenilir yok etme yöntemlerinin sağlanması;
- İOV ve İDV arasındaki uyuşmanın temin edilmesi;
- İDV'nin aslına uygunluğunun sağlanması;
- Kurcalanmışlığın saptanması;
- Kurcalanmaya karşı direnç gösterilmesi;

- İmza oluşturma cihazları arasındaki İOV'nin güvenli naklinin sağlanması;
- İOV ve İDV'nin sadece yetkili kullanıcılar tarafından başlatılmasının temin edilmesi;
- İmza oluşturma verilerinin benzersizliğinin sağlanması.

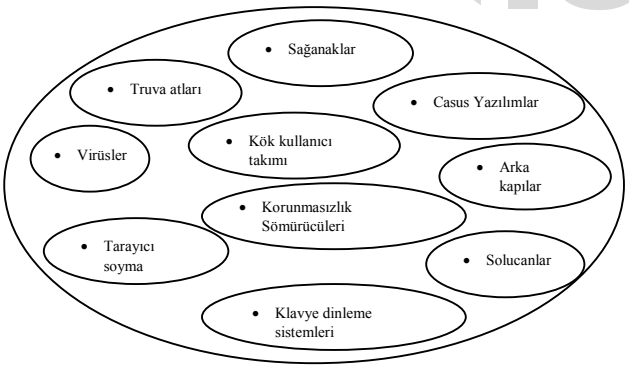
Bütün bu amaçlara ulaşabilecek e-imza oluşturma sürecine ait bir güvenlik politikasının hazırlanması ve uygulanabilmesi, çok geniş kapsamda ve titiz bir biçimde yürütülecek araştırma ve çalışmalar istemektedir.

Yukarıda bahsedilen tehditleri oluşturacak ve istenilen amaçlara ulaşmayı zorlaştıracak en önemli uygulanabilir saldırı türleri arasında son günlerde gittikçe yaygınlaşan kötücül ve casus yazılımlar gelmektedir. Bölüm 2'de bu yazılımlar tanıtılmaktadır.

III. KÖTÜCÜL VE CASUS YAZILIMLAR

Bilgisayar teknolojilerinin gelişmesi ile son zamanlarda bilgi ve bilgisayar güvenliği konusunda en ciddi tehditlerin başında kötücül yazılımlar gelmektedir. Kötücül yazılım (malware, İngilizce "malicious software"in kısaltılmışı), bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış istenmeyen yazılımların genel adıdır [9]. Aslında ana bir tür kötücül yazılım olan fakat bütün kötücül yazılım türleri arasında daha fazla ön plana çıkan ve bir çok kötücül yazılım türünü bir şekilde kapsayan casus yazılım (spyware), kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır. "Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma" adlı çalışmada, hali hazırda mevcut olan bütün ana ve ikincil kötücül ve yazılım türleri ele alınmıştır [10]. Bu çalışmada e-imza ile kötücül ve casus yazılımlar arasındaki etkileşim ve ilişkiler incelenirken söz konusu makaleden yararlanılmıştır ve bu yazılımlar hakkında ayrıntılı bilgiler için bu çalışmaya başvurulması önerilir.

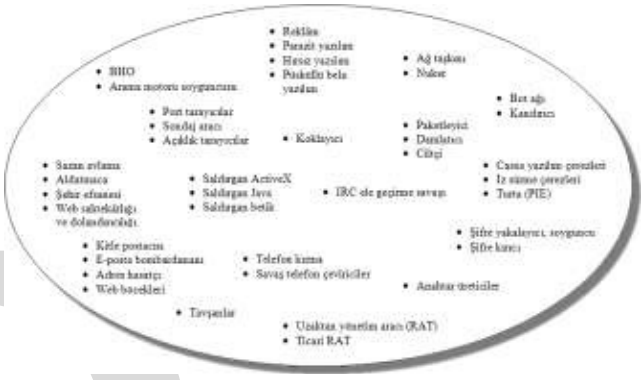
On ana kötücül yazılım türü Şekil 2'de gösterilmektedir.



Şekil 2. Ana kötücül yazılım türleri [10]

Bu kötücül yazılımların her biri, çok farklı amaçlar için, çok farklı yöntemler kullanmaktadır. Ayrıca, bu yazılımlar oldukça yaygın olarak karşılaşılan ve gerek kişisel, gerekse kurumsal çapta önemli maddi ve manevi zararlara sebep olan yapılardır.

Daha alt türde kötücül yazılımlar da Şekil 3'de topluca sınıflandırılmış halde gösterilmektedir.



Şekil 3. Sınıflandırılmış ikincil kötücül yazılım türleri [10]

Kötücül yazılım ve casus yazılımların elektronik imza oluşturma sürecinde oluşturdukları güvenlik açıkları ve bu yazılımlar ile süreç arasındaki etkileşim ve ilişki takip eden bölümde ele alınmıştır.

IV. E-İMZA OLUŞTURMA SÜRECİNDE KÖTÜCÜL VE CASUS YAZILIM SALDIRILARI

Literatürde, sınırlı kapsamda da olsa bazı kötücül yazılım türlerinin e-imza oluşturma sürecine olan olumsuz etkileri ele alınmıştır. Spalka, Cremers ve Langweg tarafından Almanya'daki e-imza oluşturma uygulamalarının (İOU) en tehlikeli kötücül yazılım türlerinden biri olan Truva atları ile nasıl sekteye uğratılabileceği örnekler ile gözler önüne serilmektedir [11]. Yazarlar, inceledikleri e-imza oluşturma uygulamaları üreticilerinin en önde gelenlerinin bile, Truva atlarına karşı özel bir önlem almadıklarını ve bunun oldukça zahmetli ve maliyetli olduğunu, bizzat kendi ağızlarından duyduklarını ifade etmektedirler. Bu, durumun ciddiyetini göstermek açısından kayda değerdir. Bu çalışmanın imza oluşturma uygulamaları ile ilgili bir diğer önemli tespiti de; bu uygulamalarda geliştirilen koruyucu tedbirlerin saldırıları önlemekten ziyade uygulamanın kolay kullanımını önlemeye yönelik olduğu şeklinde gözlemdir. Yapılan çalışmada Truva atları kullanılarak e-imza oluşturma sürecinde kullanılan PIN numaralarının elde edilmesinin ve imzalanan belgenin kullanıcının haberi olmadan değiştirilmesinin mümkün olabileceği gözler önüne serilmiştir.

Kötücül ve casus yazılımların elektronik imza oluşturma sürecine olan olumsuz etkilerinin ayrıntılarına geçmeden önce; e-imzanın, hali hazırda oldukça yaygın olan bazı kötücül yazılımların hareket alanlarını oldukça kısıtladığı, hatta neredeyse imkânsız hale getirdiğini belirtmek gerekir. E-

imzanın, tanımı gereği kimlik kanıtlama, inkâr edememe, bütünlük ve gizlilik güvenlik unsurlarını yerine getirmesinden dolayı; bu noktalardaki korunmasızlıkları istismar eden kötücül yazılımlar e-imza kullanıldığında bertaraf edilmektedir. E-imzanın etkisiz hale getirdiği ya da caydırdığı kötücül yazılım türleri şunlardır:

- Mesaj sağanakları (spam)
- Sazan avlama (phishing)
- Aldatmaca (hoax)
- Web sahtekârlığı ve dolandırıcılığı (web scam and fraud)
- E-posta bombardımanı (mail bomber)
- Kitle postacısı (mass mailer)
- Adres hasatçı (e-mail harvester)
- Web böcekleri (web bugs)

Söz konusu kötücül yazılımların çoğunlukla e-posta aracılığıyla gerçekleştirilen saldırılardır. Bu tür kötü niyetli e-posta iletilerini alan kullanıcıların, iletiyi gönderen kişinin kimliğini kesin bir doğrulukla tespit etmesi mümkün olmadığından çeşitli şekillerde kandırılması ve zarara uğratılması mümkündür.

Örneğin, ülkemizde de son aylarda çok sık bir şekilde rastlanan sazan avlama yönteminde kullanıcılar, sanki bir bankadan veya buna benzer bir kuruluştan bir e-posta alıyormuş gibi yanıltılmakta ve kredi kartı bilgileri gibi önemli ve kişisel verileri yönlendirilen sahte bir İnternet sitesi ile elde edilebilmektedir. Aldatmaca, web sahtekârlığı ve dolandırıcılığında da sahte e-posta adresleri kullanan dolandırıcıların gerçek kimliklerine erişmek mümkün olamamaktadır. Bu tür kötü niyetli e-posta iletileri e-imza ile imzalanmamışsa kullanıcılar tarafından dikkate alınmayarak sorunun daha etkili bir şekilde çözülmesi mümkün olmaktadır. Bu noktada, sahte e-imza ile bu tip e-postaların imzalanmasının çok zor hale getirilmiş olmasının şart olduğunu da hatırlatmak yerinde olur.

Kötücül yazılımlar arasında e-imza oluşturma sürecine olumsuz etkileri olan türler ile ilgili açıklamalar aşağıda maddeler halinde sunulmuştur.

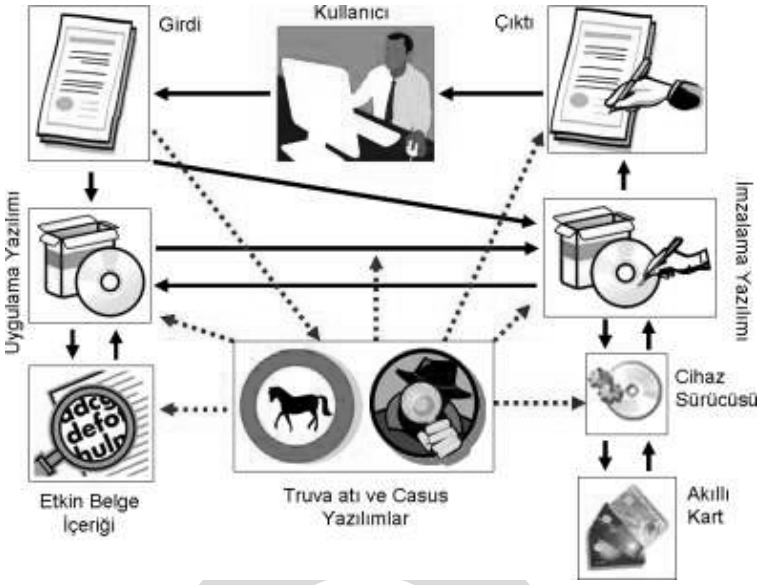
Bilgisayar Virüsleri (Computer Viruses): En tehlikeli ve en eski kötücül yazılım olarak kabul edilen virüslerin e-imza oluşturma süreçlerinde önemli etkileri söz konusudur [10]. İmza oluşturma uygulamasına (İOU) ait .EXE, .DLL gibi çalıştırılabilir modüllerine virüs bulaşması sonucu uygulama hatalı şekilde çalışabilir. Özellikle e-posta programlarına bulaşan makro virüsleri gerek PIN numaralarını elde etmek gerekse imzalanan asıl belgede tahrifat yapmak için kullanılabilir.

Bilgisayar Solucanları (Computer Worms): Solucanlar, yayılmak için başka bir programa veya virüslerde olduğu gibi insan etkileşimine ihtiyaç duymayan, kendi kendini çoğaltan bir yapı arz ederler [10]. Solucanlar bulaştığı bilgisayardan elde edilen elektronik imzalı e-postaları, başka kişilere göndermek için kullanılabilir. Şimdiden Windows işletim sisteminin güvenlik sistemini atlatmak için uygulama sayısal sertifikalarını taklit eden bilgisayar solucanları ortaya çıkmıştır [12]. Bu ileride elektronik imzayı taklit eden bilgisayar solucanlarının da ortaya çıkabileceğinin bir işareti olarak kabul edilebilir.

Truva Atları (Trojan Horses) ve Casus Yazılımlar (Spyware): Truva atları meşru yazılım gibi gözüken kötücül yazılımlardır. Casus yazılım, kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır. Bu yazılımlar e-imza oluşturma sürecinde değişik nokta ve arayüzlere saldırılarda bulunabilir. E-posta programı gibi uygulama yazılımları ile imzalama yazılımı arasındaki arayüz, imzalama yazılımı ile akıllı kart arasındaki cihaz sürücüleri ve uygulama yazılımındaki etkin belge içeriği Truva atları ve casus yazılımlar tarafından hedeflenebilir [11]. Şekil 4'de bir e-imza oluşturma sürecinde Truva atları ve casus yazılımların saldırabileceği arayüzler gösterilmektedir. Bu arayüzlerin hepsinin güvenliğinin artırılması ve korunmasızlıkların kapatılması, işleyişin güvenilirliğinin temini için gereklidir. Bu arayüzlerinde çoğunun diğer kötücül yazılım türleri tarafından da kullanılabileceği göz önünde tutularak çözümlerin geliştirilmesi gereklidir.

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. Kişisel bilgisayar içine yerleşmiş olan bir arka kapı çeşitli şekillerde e-imzanın kötüye kullanılması için kullanılabilir. Arka kapı için bir başka önemli konu, İOU üreticilerinin yazılımlarına arka kapı yerleştirme olasılığıdır. Bu özellikle devlet ve askeri alanda kullanılacak İOU yazılımlarında çok önemli bir konu olabilir. Bu yazılımların yurt dışından değil de; tamamen yerli kaynaklar kullanılan güvenilir üreticilerden temin ve idame ettirilmesi ülke güvenliği açısından gereklidir.

Klavye Dinleme Sistemleri (Keyloggers): Kullanıcı ile klavye arasında bulunan insan-makine arayüzünde gerçekleştirilen ortadaki adam saldırıları, klavye dinleme sistemi (keylogger) olarak adlandırılmaktadır [9]. Temel işlevi açısından klavye dinleme sistemi, klavye kullanırken basılan tuş bilgilerini çeşitli yöntemlerle gizli bir şekilde yakalayan ve bunları bir yerde depolayıp yine kullanıcının bilgisi dışında başka kişilerin kullanımına sunan casus yazılım olarak tanımlanabilir. Tuş bilgilerini elde eden kişi, kullanıcının bilgisayarını kullanırken şifre ve önemli kişisel bilgiler dâhil yazdığı her şeyi ele geçirmiş olacaktır. Klavye dinleme sistemleri, tuş bilgilerini kullanarak bilgi edinme dışında; fare tıklamaları, ekran görüntüleri, pano değişimleri, İnternet ve bilgisayar kullanımı ile ilgili izleme gibi değişik yöntemleri de kendi içerisine dâhil etmektedir. Klavye dinleme sistemleri e-imza kullanımı sırasında gerek klavyedeki tuşlar kullanılarak; gerekse bazı İOU yazılımları ile beraber sunulan sanal klavye ile fare kullanılarak girilen PIN kodlarının elde edilmesini sağlayabilir. Bu kodu elde eden kötü niyetli kişiler, akıllı kartı ile kullanılan bilgisayarı bir süreliğine ele geçirdiğinde kullanıcı adına imzalanmış e-posta gönderebilir.



Şekil 4. E-imza oluşturma uygulamasında Truva atı ve casus yazılımlar tarafından hedef alınan arayüzler

Kök Kullanıcı Takımları (Rootkit): Saldırganın bir sistemin kontrolünü ele geçirdikten sonra, bilgisayar sistemine eklenen yazılımlar olarak tanımlanan kök kullanıcı takımlarında yer alan araçlar arasında, kayıt (log) girdilerini silerek veya saldırgan proseslerini gizleyerek, saldırının izlerini temizleyen araçlar ve saldırganın sisteme daha sonraki girişlerini kolaylaştıracak arka kapıları düzenleyen araçları saymak mümkündür [10]. Çekirdek seviyesinde kök kullanıcı takımları, işletim sistemine çekirdek (kernel) seviyesinde çengel attıklarından, fark edilmeleri oldukça güçtür. Bu araçlar imza oluşturma sürecinde kötü amaçlar ile kullanılabilir.

Korunmasızlık Sömürücüleri (Exploit): Sömürücüler, belirli bir güvenlik korunmasızlığını hedef alan türde saldırılar üretebilen kötücül yazılımlardır. Gerek işletim sisteminde; gerekse bizzat İOU yazılımlarında var olan korunmasızlıklar kullanılarak imza oluşturma sürecine müdahale edilebilir. Bu, özellikle İOU yazılım üreticilerinin çok dikkat etmesi gereken bir konudur. Bu yazılımlarda bulunabilecek arabellek taşması (buffer overflow), CGI betikleme (scripting) hataları, SQL zerki (SQL injection) ve şifreleme hataları gibi yazılım kusurları kötü niyetli kişiler tarafından kullanılabilir. Bu yazılımların üretiminde sıkı güvenlik standart ve yöntemleri uygulanmalı ve yazılımların testlerinin geniş kapsamlı olarak yerine getirilmesi gereklidir.

Uzaktan Yönetim Aracı (Remote Administration Tool, RAT): Bu araçlar, saldırgana hedef makine çevrim içi olduğu zaman, makineye sınırsız erişim hakkı veren en tehlikeli kötücül yazılımlardan biridir. Saldırgan, bu araçları kullanarak imzalanmış sahte e-postalar gönderebilir.

Şifre Kırıcılar (Password Cracker): Kaba kuvvet ve sözlük tabanlı deneme yanılma yöntemlerini de içeren; bir şifreyi veya şifreli bir dosyanın şifresini çözen araçlar olarak tanımlanan şifre kırıcılar, özelikle PIN numaralarını elde etmek için kullanılabilir.

E-imza oluşturma sürecinde yukarıda ele alınan ana kötücül yazılım türleri dışında; diğer alt türlerinde e-imza oluşturma sürecinde önemli tehditlerin olabileceği düşünülmektedir. Şekil 3'de gösterilen bu türlerin de kapsamlı bir şekilde ele alınması; var olan ya da olması muhtemel güvenlik riskleri ve korunmasızlıkların belirlenmesi ve bunlara karşı alınabilecek önlemlerin saptanması gereklidir. Bu çalışmanın bu tür çalışmalara temel sağlayacağı değerlendirilmektedir.

V. SONUÇ VE DEĞERLENDİRME

E-imza'nın gittikçe yaygınlaşacağı ve birçok süreçte kullanılacağı gözükmektedir. Bu açıdan e-imza alt yapısının tüm kapsamıyla irdelenmesi gereklidir. E-imza'nın kullanımı ile ilgili her türlü aşamada güvenlik, çok boyutlu olarak ele alınması gereken bir husus olarak karşımıza çıkmaktadır. Bu çalışmanın en önemli bulgusu, ortaya konulan zengin kötücül ve casus yazılımların, e-imza kullanımına yönelik çok ciddi bir tehdit olması, olarak kabul edilebilir.

Çalışmada; e-imza oluşturma ve kullanım süreçleri irdelenmiş ve güvenlik riskleri işaret edilmeye çalışılmıştır. E-imzanın; bir yandan, mesaj sağanakları (spam), sazan avlama (phishing), aldatmaca (hoax), web sahtekârlığı ve dolandırıcılığı (web scam and fraud), e-posta bombardımanı (mail bomber), kitle postacısı (mass mailer), adres hasatçı (e-mail harvester) ve web böcekleri (web bugs) gibi çok sayıda kötücül yapılara karşı etkili korunma sağlarken; diğer yandan, bilgisayar virüsleri, solucanları, Truva atları, casus yazılımlar, arka kapılar, klavye dinleme sistemleri, kök kullanıcı takımları, korunmasızlık sömürücüleri, uzaktan yönetim araçları ve şifre kırıcılar için iştah açıcı bir hedef olduğu çeşitli örneklerle ortaya konulmuştur. Kötücül ve casus yazılımların sahip olduğu bu olumsuz potansiyelin, e-imza üreticileri ve kullanıcıları tarafından göz ardı edildiği izlenimi, bazı örneklerle desteklenmektedir. Bu yaklaşımın bir an önce terk

edilip; gerek üretici, gerekse kullanıcı tarafında gerekli olan önlemlerin alınması, e-imzanın geleceği açısından son derece önemlidir. Aksi taktirde; e-imza, çok şey vaat eden fakat ortaya çıkacak kullanıcı hatası, kötüye kullanım ve yasadışı vakalar sonucunda, kullanıcılar tarafından itimat edilmeyen ve rağbet görmeyen bir araç haline gelebilir.

E-imza kanunun ortaya çıkabilecek veya casusluğu önleyecek birçok hususu içerisinde barındırdığı da göz ardı edilmemelidir. E-imzanın interneti olmayan ve özel tasarımlı odalarda üretileme zorunluluğu bu çalışmada sunulan birçok açığında önüne geçmektedir. Fakat bu açıkların tamamen ortadan kaldırmadığını da hatırlatmakta fayda vardır. Kullanıcı kendi özel anahtarını sadece kendine ait olan bir kart veya cihaz içerisinde taşıması önemli bir farkındalık ve güvenlik sağlasa da burada güvenliği sağlayan PIN numarasının casus yazılımlarla elde edilmesi ise en büyük açıklardan birisini de oluşturabilecektir. Casus yazılım vasıtasıyla kişinin imzalama PIN kodunu elde ettiğinde artık en zor olan kısmı geçmekte ve kişinin kartını bir şekilde elde ederek büyük bir güvenlik açığı oluşturabilmektedir.

E-imzaya yönelik donanım ve yazılım geliştiricilerin dikkat edecekleri en önemli hususlardan birisi de kötücül ve casus yazılımlara karşı ürettikleri donanım ve yazılımları sürekli test ederek kullanıcılarına bu bilgileri sunmalıdırlar. Donanım ve yazılım geliştiricilerinin yanında; e-imza ile ilgili en önemli kurum olarak karşımıza çıkan elektronik sertifikaları üreten hizmet sağlayıcısının, standartlara ve ilgili kanunlara ne kadar uyduğunun, sık sık denetlenmesidir. Elektronik imza veya mobil imza kullanan kişilerin de mutlaka kötücül ve casus yazılımların farkında olarak sistemleri kullanmaları ve riskleri en aza indirmek amacıyla üzerlerine düşen kullanım sorumluluklarını üstlenmeleri gerekmektedir.

Teknolojik gelişme sürecinde çok önemli getirileri olan e-imzanın güvenlik alt yapısının, bu tür risklere karşı yapılacak araştırma ve çalışmalarla bir an önce kuvvetlendirileceği öngörüsüyle; bu çalışmanın, özellikle ülkemizde e-imzanın gelişimi ve yaygınlaşması sürecine önemli katkıda bulunması temenni edilmektedir.

VI. KAYNAKLAR

[1] "Elektronik İmza Kanunu", Resmi Gazete, Sayı: 5070, 23 Ocak 2004.
[2] Canbek, G., Sağıroğlu, Ş., "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", Gazi Üniversitesi, Politeknik Dergisi, Cilt: 9 Sayı: 3 s. 165–174, Ankara, 2006
[3] Spalka, A., Cremers, A. B., Langweg, H., "Trojan Horse Attacks on Software for Electronic Signatures", 2002.
[4] CEN/ISSS WS/E-Sign Workshop (2004). "Security Requirements for Signature Creation Applications". CEN Workshop Agreement CWA 14170:2004 Version 2.1.5.
[5] Sağıroğlu, Ş., Alkan, M., "Her Yönüyle E-İmza", Grafiker Yayınları, Ankara, 2005.
[6] Canbek, G., Sağıroğlu, Ş., "Şifre Bilimi Tarihine Genel Bakış–II", Telekom Dünyası, 36–44, Haziran, 2005.
[7] Canbek, G., Sağıroğlu, Ş., "Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme", Erciyes Üniversitesi, Fen Bilimleri Enstitüsü Dergisi, Cilt 23, No: 1–2, s. 1–12, Kayseri, 2007.
[8] ESIGN Workshop - Expert Group F, "Protection Profile — Secure Signature-Creation Device Type1", CEN/ISSS, Version: 1.05, EAL 4+, 28 July 2001.
[9] Canbek, G., Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Eylül 2005.
[10] Canbek, G., Sağıroğlu, Ş., "Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma", Müh. Mim. Fak. Dergisi, Gazi Üniversitesi, Cilt 22, No: 1, 121–136, Ankara, Mart 2007.
[11] Spalka, A., Cremers, A. B., Langweg, H., "Trojan Horse Attacks on Software for Electronic Signatures", Informatica 26, 191–203, 2002.
[12] Keizer, G., "Kama Sutra Spoofs Digital Certificates", Techweb, 24 Ocak 2006.