İnternet Bankacılığında Akıllı SMS İçin Üç Yollu El Sıkışma

Onur Gök[1] H.Engin Demiray[2]

[1,2]Bilgisayar Mühendisliği Bölümü, Kocaeli Üniversitesi, Kocaeli
[1]e-posta: ogok@kocaeli.edu.tr [2] e-posta: hedemiray@kocaeli.edu.tr

Özetçe

İletişim ve bilişim sektöründeki hızlı gelişim ve zamanın en değerli olduğu gerçeği, bankaların da bu gelişime ayak uydurma çabaları ve müşterilerine daha hızlı ve kaliteli hizmet vermeleri için İnternet bankacılığı önemli alternatif yol olmuştur. Bu alternatif bankacılık hizmeti sayesinde, banka müşterileri zaman ve mekandan bağımsız tüm bankacılık hizmetlerini gerçekleştirmeleri hem müşteri hem banka açısından büyük kolaylıklar sağlamıştır. Bu kolaylıklarla beraber, internet altyapısının getirdiği bazı güvenlik riskleri de mevcuttur. Bu risklerden bir tanesi de banka müşterisinin kimlik doğrulamasıdır. Kimlik doğrulama işlemleri için, bankalar internet bankacılığı sistemleri kapsamında günümüze kadar farklı metotlar uygulanmıştır. Bu metotlardan bazıları sadece müşterinin belirlediği şifreler, müşteriye verilen rast gele şifre üreten anahtarlar, cep telefonuna gelen şifreler olmuştur.Günümüzde en yaygın olarak kullanılan metot iki kademeli kimlik doğrulamasıdır. Birinci adımda kullanıcının belirlediği şifre, ikinci adımda bankanın müşterinin cep telefonuna gönderdiği SMS onay şifresinin kullanılarak internet bankacılığı sistemine girilmesi şeklindedir. Bu yöntemde SMS onay şifresinin müşteriye veya üçüncü kişilere ulaşıp ulaşmadığı konusunda bir kontrol yapılmamaktadır. Bu sebeple güvenlik açığı ortaya çıkmaktadır. Bu çalışmamızda bu güvenlik zafiyetini ortadan kaldırmak için bir onay mekanizması yöntemi önerilmiştir. Önerilen çalışmada, bilgisayar ağlarında bağlantı kurmak için kullanılan 3 yollu el sıkışma benzetimi yapılmıştır.

1. Giriş

Türkiye'de faaliyet gösteren bankaların birçoğu müşterilerine internet üzerinden de hizmet vermektedir. Günümüzde İnternet Bankacılığı; bankalar, ve müşterileri açısından önemli bir yer tutmakta olup, işlemlerin hızlı bir şekilde sonuçlandırılması ve maliyetler açısından her iki tarafa da fayda sağlamaktadır. Türkiye Bankalar Birliği üyesi olan ve İnternet Bankacılığı hizmeti veren 25 bankadan alınan bilgilere göre; Aralık 2008 itibariyle internet bankacılığı yapmak üzere sistemde kayıtlı olan ve en az bir kez sisteme giriş yapmış toplam müşteri sayısı 12.580.671'dir.

Internet Bankacılığı, işlem maliyetinin düşüklüğü, kolaylığı, ürün çeşitliliği, hızlı bilgi değişimi gibi avantajlarıyla hem bankalar hem de tüketiciler için en cazip dağıtım kanalı olarak dikkat çekmekte ve bütün dünyada hızla yayılmaktadır [1].

İlk İnternet Bankacılık hizmeti 1997 tarihinde verilmeye başlanmıştır. Oldukça yeni olan bu dağıtım kanalında ilk yıllarda kayıtlı dolandırıcılık işlemi azdı. İnternet bankacılığının büyük bir hızla yaygınlaşması ile beraber, tüm dünyada olduğu gibi, ülkemizde de internet üzerinden yapılan dolandırıcılık girişimlerinde artış gözlemlenmektedir. Son dönemde, bu konudaki yasal boşluklar internet bilgi hırsızları (hacker) tarafından fark edilmiş kötü niyetli girişimler ve saldırılar başlamıştır. İnternet bankacılığı dolandırıcılık eylemlerindeki ortak kurgu; müşterinin özel bilgilerinin, kullanıcı bilgisayarından çeşitli yöntemlerle çalınması ve bu bilgilerin kullanılarak müşteri adına internet üzerinde işlem yapılmasıdır .

Kimlik hırsızlığı (identity theft), bir başkasına ait kişisel bilgilerin yetkisiz olarak kullanılması suretiyle işlenen dolandırıcılık yöntemidir [2].

Kimlik hırsızlığında dolandırıcıların en çok kullandığı yöntemler şöyle sıralanabilir:

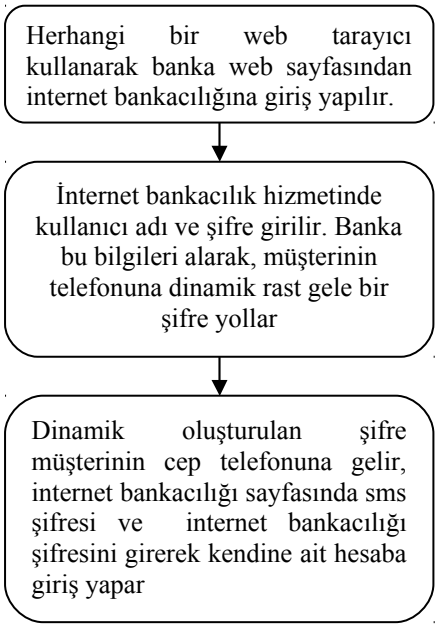
- Tuş kaydediciler (keylogger),
- Ekran kaydediciler (Screenlogger)
- Oltalama (Phishing)
- Casus yazılım (Spyware)
- Sosyal mühendislik.

Kimlik hırsızlığı yöntemlerine bakıldığı zaman, bu yöntemlerin genellikle kullanıcının tedbirsiz ve dikkatsizliklerinden kaynaklandığı görülmektedir. İnternetteki tehlikelerden haberi olmayan bir kullanıcı, internet bankacılığında geleceğin mağdurlarından biri olarak görülebilir[3].

Bir banka müşterisinin, internet bankacılığı sistemini kullanabilmesi için, banka sisteminin müşteri kimliğini doğrulaması gerekmektedir. Bu doğrulama, sadece bankanın ve müşterinin bildiği bilgilerin sorgulanması ile olmaktadır. Müşterinin bilgisayarından girdiği kişisel bilgiler banka sisteminde saklı kişisel bilgilerle karşılaştırılıp, yetkili müşteri tarafından yapılıp yapılmadığı sistem tarafından kontrol edilerek girişe izin verilmektedir. İnternet bankacılığı işlemlerinde kişisel bilgilerin doğrulanmasında, güvenliğin sağlanması için geliştirilen teknikler arasında, güvenlik ihtiyacına göre parola, şifre, para çıkışlarında ikinci bir işlem şifresi, ortak belirlenen cep telefonlarına Mesaj, Akıllı SMS, IP Kısıtlaması, Tek Kullanımlık Şifre, Akıllı Anahtar, Elektronik İmza gibi tekniklerden bir kaçı uygulanabildiği gibi, güvenlik ihtiyacına göre bunların kombinasyonundan oluşan kademeli bir anlayışı da uygulandığı görülmüştür.

Günümüzde kullanılan kişisel bilgilerin doğrulanmasında kullanılan yöntemlerinden birisi de akıllı SMS'dir. Bu yöntemde müşteri bankanın internet hizmetini kullanmak istediğinde, bankanın web sayfasından sisteme giriş yapmak için kullanıcı adı (hesap numarası da olabilir) ve internet şifresini kullanmakta, bu şifre ile giriş yaptıktan sonra cep

telefonuna bankanın ürettiği rast gele dinamik bir şifre gelmektedir. Belli bir zaman aralığında bu şifreyi web sayfasında kullanarak internet bankacılığı sistemine giriş yapılabilmektedir.



Şekil 1: Uygulanan internet bankacılığı adımları

Şekil 1'de internet bankacılığı sisteminde, akıllı SMS kullanımının amacı, müşterilerin web sayfasına girmek için kullandıkları statik şifre ve kullanıcı adının 3. kişiler tarafından internet ağı üzerinden keylogger, screenlogger, truva atı, phishing gibi yöntemleri ile ele geçirilme ihtimaline vardır. Bu durumu engellemek için internet bankacılığı sistemlerinde Akıllı SMS yüksek oranda bir çözüm olmuştur. Yukarıda bahsedilen internet ağı kullanılarak yapılan kimlik hırsızlıklarını etkisiz hale getirmek için, internet bankacılığı sistemine girmek isteyen müşteriye farklı bir alt yapı olan GSM kullanılarak dinamik bir şifre gönderilmektedir. Bu sayede kimlik hırsızlarının bu bilgiye ulaşmaları engellenerek, sadece cep telefonuna giden SMS şifresini bilen müşterinin internet bankacılığı sistemine girmesi sağlanır.

Günümüzde bu güvenlik mekanizmasına rağmen, kimlik hırsızlığı ile ilgili farklı metotlar yapıldığı görülmüştür. Müşterinin kimlik bilgileri ve telefon numarası elde edilerek, GSM kartı bloke edildiği, akıllı SMS'lerini, kopyalanan aynı telefon numarasına sahip başka bir telefona yönlendirildiği ve bu sayede internet bankacılığı şifresi ve akıllı SMS şifresi ile müşterilerin hesaplarına girilip boşaltıldığı tespitleri yapılmıştır. Gönderilen akıllı SMS'in müşteriye ulaştığı bilgisi böyle bir açığı engelleyecektir. Bankanın gönderdiği SMS'in istekte bulunan müşteri tarafından alındığı bilgisini bankaya iletmesi durumunda yukarıdaki anlatılan durum için bir çözüm olacaktır. Bu çözüm, bilgisayar ağlarında iki üç bilgisayar arasında iletişime geçmeden önce bağlantı kurmak için kullandığı üç yollu el sıkışma mantığına benzemektedir. Müşteri ilk olarak internet bankacılık sistemine girerek 1. yolu oluşturacak, banka müşteriye SMS ile dinamik şifre göndererek 2. yolu oluşturacak, müşteri dinamik şifreyi kendisinin aldığını bankaya SMS ile ileterek 3. yol oluşmuş olacaktır.

2. Üç Yollu El Sıkışma ve Uygulamaya Benzetimi

İnternet ağlarında iki uç bilgisayarın birbiri ile haberleşmesi için tanımlanmış protokol olan TCP'de, bilgisayarlar haberleşmeye başlamadan önce birbirleri ile bağlantı kurmak için Tomlinson[4] tarafından önerilen 3 yollu el sıkışma mantığını kullanır[5]. Bu mantığa göre, bağlantı kurmak isteyen istemci , bağlantı kurulmak istenen sunucuya İSTEK mesajı gönderir ve belli süre bekler. Sunucu eğer müsaitse istemciye KABUL mesajını iletir. Sunucu KABUL mesajının istemciye gittiğini öğrenmek için belli bir süre istemciden KABUL mesajının ulaştığına dair ULAŞTI mesajı bekler , ULAŞTI mesajı bu süre içerisinde sunucuya ulaşırsa her iki bilgisayar bağlantı kurma işlemi yaparlar.

Şekil 2: İnternet ağlarında TCP bağlantı kurma

İnternet bankacılığı için kullanılan Akıllı SMS yönteminde, müşterinin SMS'i aldığına dair bankaya cep telefonu üzerinden göndereceği ULAŞTI mesajı tam bir bağlantı kurulmasını sağlayacaktır. Fakat burada ULAŞTI mesajının içeriği önem kazanacaktır. Bu mesajın içeriği, müşteriyi tanımlaması gerekecektir. Bu nedenle, mesaj içeriği 3. kişilerin eline geçemeyecek sadece banka ve müşteri tarafından bilinen statik veya dinamik, donanımsal veya yazılımsal bir bilgi olması gerekecektir. Mesaj içeriğinin nasıl olması gerektiği ile ilgili birden fazla çözüm yolu olabilir. Bu çözüm yolları şu şekilde sıralanabilir:

- Donanımsal bilgi: cep telefonu IMEI numarası
- Müşteri bazlı bilgi: Müşterinin bankadan elden aldığı veya banka kartı ile ATM'den alabileceği akıllı cevap şifresi
- Yazılımsal bilgi: Bankanın üreteceği , cep telefonlarına yüklenebilecek bir yazılım olacaktır. IMEI numarası, akıllı cevap şifresi (sadece müşterinin bildiği) oluşan 2 anahtarlı kriptolanmış bilgi.

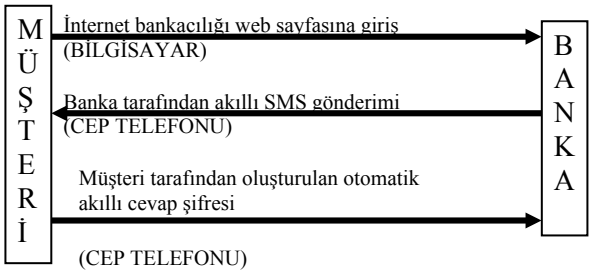
5070 sayılı Elektronik İmza Kanunu'nda yer alan şekliyle elektronik imza; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar.

Elektronik imza kavramı çok genel bir tanım olup kişilerin elle atmış olduğu imzaların tarayıcıdan geçirilmiş hali olan sayısallaştırılmış imzaları, kişilerin göz retinası, parmak izi ya da ses gibi biyolojik özelliklerinin kaydedilerek kullanıldığı biyometrik önlemleri içeren elektronik imzaları veya bilginin bütünlüğünü ve tarafların kimliklerinin doğruluğunu sağlayan

sayısal imzaları içermektedir. Sayısal imza, imzalanan metine göre farklılık gösterir ve içeriğin matematiksel fonksiyonlardan geçirilerek eşsiz olduğu düşünülen bir değer bulunması sureti ile elde edilir. Yani kişilerin, elle atılan imzada olduğu şekilde tek imzası yoktur; bunun yerine imzalamada kullanılan anahtarları vardır. 5070 sayılı Elektronik İmza Kanunu'nda ve bu metinde geçen "elektronik imza" kavramı sayısal imzayı işaret etmektedir.

Uluslararası Mobil Cihaz Kodu (IMEI: International Mobile Equipment Identity): Her bir GSM telefon cihazına üretim aşamasında IMEI numarası yüklenmektedir. IMEI numarası her bir cihazın kimlik numarası olup tek ve benzersizdir.

Günümüzde internet bankacılığı işlemlerinde E-imza, cep telefonlarına gönderilen akıllı mesaj olarak kullanılmaktadır. Tek ve benzersiz olan IMEI numarası bir E-imza uygulaması olarak kullanılması temelinde üç yollu el sıkışma mantığı ile müşteri ve banka arasında bağlantı kurmak daha güvenilir bir yol olacağı düşünülmektedir.



ŞEKİL 3. İnternet bankacılığında üç yollu el sıkışma

Müşteri, herhangi bir bilgisayardan bankasının internet bankacılığı sistemine giriş yapmak istediğinde, web sayfası üzerinden müşteri numarası ve parola kullanarak bağlantı isteğinde bulunur. Bağlantı isteği bankanın sisteminde yorumlanır. Banka müşterinin kayıtlı olduğu cep telefonuna akıllı SMS ile bir şifre gönderir. Kimlik doğrulama işlemi için, müşteriden cevabı cep telefonu üzerinden bekler. Müşterinin mesajı aldığına dair donanımsal, yazılımsal veya müşterinin girdiği alındı şifresini GSM üzerinden Sms yoluyla göndermesi ile internet bankacılığı sisteminde oturum açmak için izin alır. Bankanın sistemine giden alındı mesajı ile birlikte, müşteri internet bankacılığına girmek için parola ve akıllı SMS şifresini sistemde girerek, oturum açabilir.

Cep telefonun tek ve benzersiz olan fiziksel adresi(IMEI) sayısal imza olarak kullanılarak, kimlik hırsızlığının azaltılması sağlanacaktır. Bunun yanında bankaların internet bankacılığı sistemine müşterilerin cep telefonu IMEI numaralarını kayıt edilmeleri gerekmektedir. Bu hem bankalara hem müşteriye ek bir yük getirmesi dezavantaj olarak görülebilir. Bunun yanında müşterinin de sms olarak alındı cevabı göndermesi müşteriyi uğraştırması veya zamanını alması bir dezavantaj olarak görülebilir fakat gelişen bilişim sistemi ile birlikte cep telefonu üzerinde geliştirilebilecek uygulamalarla bu yük azaltılabilir. Sayısal imza için ek bir donanım için maliyet de düşünülürse, cep telefonlarının sayısal imza için kullanılması sadece bankacılık işlemleri için değil, internet ortamında sayısal imza gerektiren diğer tüm uygulamalar için de bir anahtar olması mantıklı bir seçim olabilir.

3. Sonuçlar

Ocak 2010 tarihinden itibaren BDDK tarafından zorunlu hale getirilen elektronik imza, internet bankacılığı hizmetlerinde, cep telefonlarının dolaylı olarak elektronik imza gibi kullanılması gibi durumu ortaya çıkarmıştır. Bankalar ve GSM firmaları birbirlerinden farklı kurumlardır ve hizmet yönleri farklı olduğu için, internet bankacılığında güvenlik için cep telefonu kullanılmasında bazı boşluklar ortaya çıkmaktadır. Akıllı SMS, internet bankacılığı dolandırıcılıkları için büyük oranda çare olmuş fakat kullandığı GSM hizmetlerindeki farklılıklardan kaynaklanan (sim kart kopyalama gibi) açık meydana gelebilmektedir. Yaptığımız çalışmada bu açığın kapatılması için bir öneri yapılmıştır.

Müşterinin bankaya gönderdiği Akıllı SMS ulaştı mesajının temelinde, tek ve benzersiz olarak kullanılan IMEI numarası vardır. IMEI numarasının sayısal imza olarak kullanılması sadece banka işlemleri için değil, elektronik ortamda tüm diğer işlemler için bir sayısal imza olarak kullanılması tercih edilebilecek bir metot olarak düşünülmüştür.

Cep telefonları internet bankacılığı işlemleri için bir bakış açısıyla donanımsal anahtarımız olmuştur. Önümüzdeki yıllarda, bu anahtarın sadece internet bankacılığı gibi güvenlik isteyen mekanizmalar için değil, tüm internet işlemleri içinde bir nevi Elektronik imza gibi kullanılması için IMEI numarası, parmak izi tarayıcı gibi, TC kimlik numarası gibi bilgiler donanım üzerine yazılımsal olarak gömülerek , uygulama çeşitliliği artırılabilir.

4. Kaynakça

[1] Usta, R., "Tüketicilerin Internet Bankacılığını Kullanmama Nedenleri Üzerine Bir Araştırma", Doğuş Üniversitesi Dergisi, 6 (2) 2005, 279-290 (2005).

[2] Kocamaz, C., "Kimlik Hırsızlığına Karşı Web Tarayıcıların Kullanımı Kimlik Hırsızlığı", www.sayisaldelil.net, Erişim Tarihi:02/10/2009 (2009).

[3] Ayvaz Reis, Z., Gülseçen, Z., Bayrakdar, B., "Güvenli Internet Bankacılığı Eğitim Sistemi :GIBES, Akademik Bilişim Konferansı, 2010

[4] Raymond S. Tomlinson, "Selecting Sequence Numbers," INWG Protocol Note 2, IFIP Working Group 6.1, August 1974. Also in Proceedings of the ACM SIGCOMM/SIGOPS Interprocess Communications Workshop, (Santa Monica, CA, March 24–25, 1975), and ACM Operating Systems Review, Volume 9, Number 3, July 1975, Association for Computer Machinery, New York, 1975.

[5] Kurose, J.F. & Ross, K.W. (2010). Computer Networking, 5th ed. Boston, MA: Pearson Education, Inc.