Introduction To Secure Coding
Report

SECURITY RESEARCH ON A SOCIAL PAYMENT APP

Bu Proje Kapsamında Mobil Ödeme Uygulamalarının Güvenlik Konusu Araştırılmıştır.

Eskişehir Osmangazi Üniversitesi
Bilgisayar Mühendisliği Bölümü

Rapor Sahibi

152120131020 Sevda ÇİMEN

Ders Yürütücüsü
Dr. Uraz YAVANOGLU

Bilgisayar Mühendisliği Bölümü
ESKİEHİR OSMANGAZİ ÜNİVERSİTESİ
Güz Dönemi 2017

Özet

Apart from being used only for communication, mobile devices change our business life, our everyday life and our habits in many areas of our lives.These changes facilitate our lives and enable us to live a better life.With mobile apps, it's now possible to do almost anything you can think of.Among them, mobile payment technologies are taking place.Mobile payment technologies can also be used to define the next generation of commerce. Today's consumers are able to do these transactions with applications that pay with mobile wallets, gift cards, credit / debt or registered value accounts. "According to a 2015 study among mobile payment users in the United States," 20 percent is afraid of basic security concerns about mobile payments, the likelihood of someone cutting out payment information or other data, and about 13 percent of their phones being attacked "[1].ISACA is a non-profit organization dedicated to the development, adoption and use of globally accepted knowledge and practices for information systems.ISACA conducted a comprehensive survey of 2015 mobile payment security specialists with 900 member cyber security experts to investigate the biggest security risks.Only 23 percent of survey respondents said they believe mobile devices are safe enough to secure personal information, while 47 percent claimed that mobile payments are not secure.The overwhelming majority expected 87 percent, an increase in violations of mobile payment data next year [3].

As a result, when investigations are examined, the safety concerns for mobile payments are still of great importance and it can be said that the consumer complaints about the current situation have prevented mass acceptance.The proliferation of viruses and malware that affect mobile devices, especially with the real danger of lost or stolen devices, is causing consumer unease in terms of the reliability of personal information and documents.

There are a few different types of mobile payment systems that all work a bit differently. Some might require your phone to be near the other device receiving the payment, like with NFC (near-field communication) payments, while others just use the internet.

Most mobile payment systems can be identified in one of these categories:

1.Everyday Transactions

2.Point of Sale Payments

3.Closed Loop Mobile Payments

4.Carrier Payments

5.Mobile Payment Apps

The Mobile Network Operator provides the necessary infrastructure for the wireless WAN service. In addition, there are also regulators that are included in the monitoring of compliance.
There are two types of mobile payment systems between organizations:
1) Remote Payment Systems
On remote mobile payments, the customer first sends a payment request over a wireless network to the PSP using a remote wireless communication technology
2) Proximity Payment Systems
With proximity mobile payments, the customer usually credits the payment using a short-range wireless technology. To ensure the safety of the mobile payment system as a whole, each layer in the mobile payment system must be resistant to attacks such as man-in-the-middle, replay attacks, or impersonation attacks.There are several kinds of mobile payment process. Some of them are physical POS, android share, apple share and samsung share.Physical POS refers to such things as Apple, Samsung and Android Pay. The other share applications are the rendering platforms developed by Google, Apple and Samsung respectively.Even on these platforms there are some risks. But as days go by, the infrastructure under mobile payments becomes more robust and naturally can be regarded as completely safe now, due to most system tokenization. For example, the entrepreneur noted that a signal could not be attacked using the Samsung Pay icon, the KNOX security frame, and fingerprint authentication.Existing risks:
–1.Attacks caused by using public Wi-Fi,
–2.Phishing Attacks,
–3.Platform Selection Source Vulnerabilities,
–4.Mobile Malware
–5.Spyware Use.
In terms of reducing these risks, the security of the implementation is influenced by the formation of large demand differences in terms of self-sufficiency and reliability.That's why the PA-DSS standard is available for the development of mobile payment applications within the scope of some bases.Applications should avoid scams and provide customers with security in mobile wallets and payment applications.There are various options to verify the identity of mobile payments and to secure customer data in the mobile, contactless world.These are ;
User Solutions
Mobile Payment transactions can be taken by the user by taking the following factors into consideration.

1.Be sure to implement proper session management in the application.
2.Ensuring that the applications are safe to execute.
3.In practice, all trusted and untrusted (invalid user input, special characters, for example) confirm the validity of entries.
4.By enforcing the strong authentication mechanism in practice.
5.Using secure web services and Interfaces.
6.In case of loss or theft of the device, in possession
. **2) Hardware Solutions**
Some activities can be avoided, such as hardware solutions that can be received in the mobile device itself and SMS sending without permission. **3) Reseller-Based Solutions**
It is an obligation to evaluate the written application in terms of every risk, to keep up with the current deficits and to reach their solutions, to take the necessary precautions and then to present it to the user.

İçindekiler

Şekil Listesi

Bölüm 1

Giriş

Mobil cihazlar yalnızca iletişim kurmak amacıyla kullanılmasının dışında gelişen teknoloji ile iş hayatımızı,gündelik yaşamımızı ve hayatımızıdaki birçok alandaki alışkanlıklarımızı değiştirmektedir.Bu değişimler yaşantımızı— kolaylaştırarak daha kaliteli bir yaşam sürebilmemize olanak sağlamaktadır. Artık mobil uygulamalar ile aklınıza gelebilecek neredeyse herşeyi yapmak mümkün hale gelmiştir.Bunlar arasında mobil ödeme teknolojileri önemli yer kaplamaktadır.Mobil ödeme teknolojileri yeni nesil ticaretin tanımlanmasında da kullanılabilir.Günümüzün tüketicileri, mobil cüzdanlar, hediye kartları, kredi / borç veya kayıtlı değer hesaplarıyla ödeme yapan uygulamalarla bu işlemlerini rahatlıkla yapabilmektedir.Mobil cihazlar üzerinden tüketiciler bir web bankacılığı aracılığıyla güvenli finansal işlemler gibi çeşitli amaçlarla mobil ödeme uygulamalarına daha aşina hale gelmektedirler.Tüketici tarafında bu uygulamaların hayatımızı kolaylaştırmasının yanında hizmet sağlayıcılar ve parekendeciler için aynı durum geçerli degildir.Parekendeciler çeşitli zorluklarla karşı karşıya kalmaktadır. On yıllardır, perakende ödeme işlemleri, ödeme işlemcisine yetki için ulaşan bir mağaza içi satış noktası sistemi ile başlatılmıştır.Mobil ödemelerin ortaya çıkmasıyla birlikte müşteriler, POS işlemi gerektirmeyen bulut tabanlı mobil uygulamalar aracılığıyla ödemeleri başlatabilmektedirler ve bu durum göz önüne alındığında, mağaza yöneticiler, bulut tarafından başlatılan işlemlerin akışını başarılı bir şekilde yönetmek zorundadır.

Gelişmiş mobil ödeme çözümleri, bulut ödeme sağlayıcılarına hem yeni bulut tabanlı ödemeleri hem de POS'un başlattığı geleneksel ödemeleri etkinleştirmek için basit, güvenli ve uygun maliyetli bir platform sunar. E-ödeme sistemleri elektronik nakit kullanımını arttırdığı için kağıt para basmaya göre çok daha ucuz bir imkan sağlamasıyla hükümet ve finansal kuruluşlar tarafından büyük maliyet tasarrufu sağladığı gerekçesiyle savunulmaktadır.

Çoğu tüketici için mobil ödeme olanağı, çoklu kredi kartı ve bankamatik kartlarıyla geleneksel bir cüzdan taşımaktan daha fazla kolaylık sunar.Bununla birlikte, bir cep cüzdanının kullanılması risksiz değildir. Güvenlik önlemleri listenin başında gelmektedir.

"Amerika'daki mobil ödeme kullanıcıları arasında gerçekleştirilen 2015 araştırmasına göre, " yüzde 20'lik bir kesim, mobil ödemelerle ilgili temel güvenlik kaygısı, birinin ödeme bilgilerini veya diğer verileri kesme olasılığı olduğunu ve yaklaşık yüzde 13'ü telefonlarının saldırıya uğramasından korkmaktadır" [1].

ISACA, bilgi sistemleri için küresel kabul görmüş bilgi ve uygulamaların geliştirilmesi, benimsenmesi ve kullanılması için çalışan kar amacı gütmeyen bir kuruluştur.ISACA, 2015 Mobil Ödeme Güvenliği Uzmanları için en büyük güvenlik risklerini incelemek için 900 üyeli siber güvenlik uzmanını içeren kapsamlı bir anket düzenledi.Ankete katılan uzmanların sadece yüzde 23'ü, mobil cihazların kişisel bilgilerin güvenliğini sağlayacak kadar güvenli olduğuna inandıklarını söylerken ,yüzde 47 mobil ödemelerin güvenli olmadığını iddia etti.Ezici çoğunluk yüzde 87, önümüzdeki yıl mobil ödeme verisi ihlallerinde bir artış bekliyordu [2].

Sonuç olarak araştırmalar incelendiğinde, mobil ödemelere yönelik güvenlik kaygıları hala çok büyük önem taşıyor ve mevcut durumla ilgili tüketici rahatsızlığının kitlesel kabulü engellediği söylenebilir.Özellikle kaybedilen veya çalınan cihazların gerçek tehlikesiyle birlikte mobil cihazları etkileyen virüslerin ve zararlı yazılımların çoğalması,kişisel bilgi ve dökümanların güvenirliliği açısından tüketicilerde tedirginlik uyandırmaktadır.

Bölüm 2

Mobil Ödeme Sistemi

Tümü biraz farklı işleyen birkaç farklı mobil ödeme sistemi türü vardır. Bazıları telefonunuzun, ödemeyi alan diğer cihazın yakınında olmasını, örneğin NFC (alanın yakınında iletişim) ödemelerini gerektirirken diğerleri sadece internet'i kullanabilir.Çoğu mobil ödeme sistemi şu kategorilerden birinde tanımlanabilir:

Gündelik İşlemler:
Mobil ödemenin bir türü evinizdeki gibi her yerde gerçekleşir.Telefonunuzda bir uygulama açabilir ve istediğiniz kişiye istediğiniz herhangi bir nedenle ödeme yapabilirsiniz.Faturayı bölebilir, para gönderebilir veya iade işlemleri gerçekleştirebilirsiniz.Para genellikle banka hesabınızdan doğrudan alınır, ancak bazı hizmetler daha hızlı transferler için nakit paranın bir "cep cüzdanında" tutulmasına izin verir.

Satış Noktası Ödemeleri:
Bunlar, hizmeti veya iyi ürünü satın aldığınız yerde gerçekleşir.Birçok mağazada POS mobil ödeme sistemleri bulunur; bu işlem, telefonunuza kart okuyucuda dokunmanız veya faturayı anında ödemek için telefonunuzdaki bir düğmeye basmanız son derece kolaydır.

Kapalı Döngü Mobil Ödemeler:
Bu mobil ödeme türleri, bir şirkete özeldir.Örneğin, Herhangi bir yemek veya sipariş online menüden, telefonunuzu kullanarak bir şey satın almanızı sağlar.Hatta mağazadaki hattı atlayabilir ve siparişinizi hızlı bir şekilde almak için doğrudan bir mobil siparişi belirleyen satıra geçebilirsiniz.

Taşıyıcı Ödemeleri:
Her cep telefonu ödeme kabiliyetine sahip bir telefon bir cep telefonu operatörü kullandığından, telefonunuzdan herhangi bir şey için ödeme yapmanıza izin veren ancak cep telefonu faturasını alıncaya kadar ödemeniz gereken bazı hizmetler bulunmaktadır.Bunlar bazen bağışlarla metinde yapabileceğiniz görülebilir.

Mobil Kart Okuyucu:
Bazı şirketler, bir bankamatik veya kredi kartından ödeme kabul etmek için kullanılabilen telefonunuza veya tabletinize takılan küçük bir cihaz sunar.Bu, küçük işletmelerde veya hatta ödemeleri ödeme koşullarında kabul eden bireyler için vazgeçilmezdir.
Mobil Ödeme Uygulamaları
Büyük app store platformlarında daima mobil ödeme uygulamaları piyasaya sürülüyor. Bazı telefonların cihazın içine yerleştirilmiş bir mobil ödeme özelliği bile olan çok popüler hale gelmektedir.

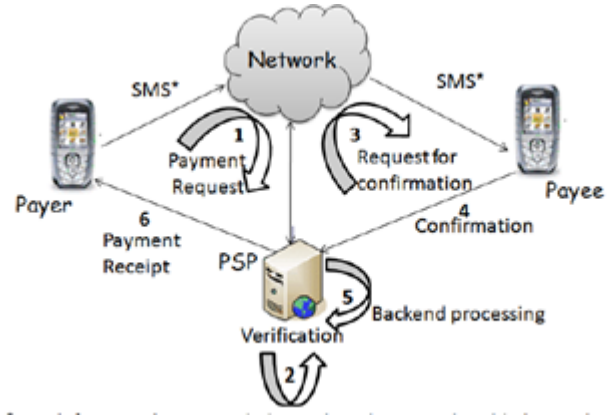
Bir mobil ödeme sistemi tipik olarak beş ana aktörü kapsar.Bunlar;
1) Mali Hizmet Sağlayıcı (Financial Service Provider (FSP)
2) Ödeme Hizmeti Sağlayıcı (Payment Service Provider (PSP))
3) Mobil Ağ Operatörü (Mobile Network Operator (MNO))
4) Ödeme yapan
5) Alıcı
dahildir.
Bir Mali Hizmet Sağlayıcı genellikle bir bankadır ve iki taraf arasında bir işlemi gerçekleştirmek için gerekli olan arka uç işlemeyi yapmaktan sorumludur.
Bir Ödeme Hizmeti Sağlayıcı, Mali Hizmet Sağlayıcı ile ödeyici / alacak arasındaki iletişimi ödeme yazılımı ve kullanıcı arayüzleri sağlayarak kolaylaştırır.
Mobil Ağ Operatörü, kablosuz WAN hizmeti için gerekli alt yapıyı sağlar.Buna ek olarak, uyumluluğun izlenmesinde yer alan düzenleyiciler de bulunmaktadır.

Kuruluşlar arasındaki mobil ödeme sistemleri iki tiptir:
1) Uzaktan Ödeme Sistemleri
2) Yakınlık Ödeme Sistemleri.

2.1 Uzaktan Ödeme Sistemleri

İlk aşamada, ödeme yapan kişi ve alacaklı kişi uzak konumlarda, ör. bir müşteri evinden bir perakende mağazasına bir sipariş verir.İkincisinde, ödeme yapan kişi ve alacaklı kişi aynı çevrede, ör. bir müşteri (ödeme yapan), bir satış makinesinden (alacaklı) bir fincan kahve alır. Şekil 1'de gösterildiği gibi, aşağıdaki adımlar genellikle bir uzak mobil ödeme sistemi kullanılarak bir işlemi gerçekleştirir:

Uzak mobil ödemelerinde,müşteri ilk önce uzak bir kablosuz iletişim tek-

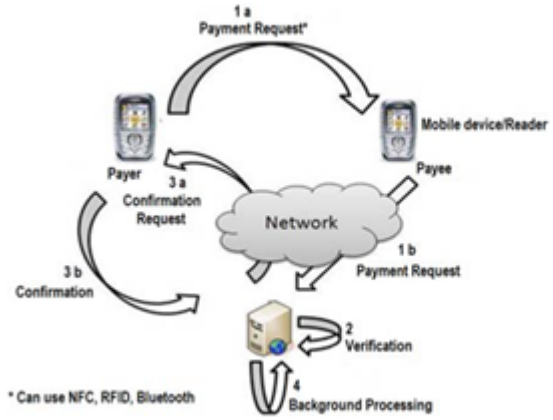


Şekil 2.1: Uzak Mobil Ödeme Sisteminin Temel Mimarisi [9]

nolojisini kullanarak bir kablosuz ağ üzerinden ödeme talebini PSP'ye gönderir.PSP daha sonra bu talebi alacaklıya iletir.

2.2 Yakınlık Ödeme Sistemleri

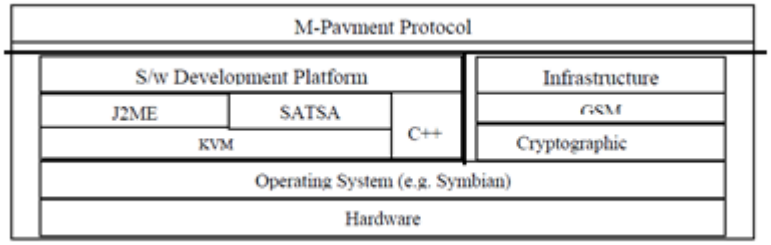
Yakınlık mobil ödemelerinde, müşteri genellikle kısa menzilli bir kablosuz teknoloji kullanarak ödeme talebini alacaklıya gönderir.Alacaklı, daha sonra bu ödeme talebini bir kablosuz ağ üzerinden PSP'ye iletir.



Şekil 2.2: Yakınlık Mobil Ödeme Sisteminin Temel Mimarisi [9]

Bu sınıflandırmanın yanı sıra mobil ödemeleri, ilgili ödeme değerine (Mikro ve Makro ödemeler) ve kullanılan şarj yöntemine (Ödenen, Önceden Ödemeli

ve Öde Şimdi) dayalı olarak da sınıflandırılabilir [9].



Şekil 2.3: Bir mobil ödeme sisteminin farklı katmanları [9]

Bir bütün olarak mobil ödeme sisteminin güvenliğini sağlamak için, mobil ödeme sistemindeki her katmanın, man in-the-middle, tekrarlama (replay) saldırıları veya kimliğe bürünme saldırıları gibi saldırılara karşı dayanıklı olması gerekir.

Bölüm 3

Güncel Mobil Ödeme Yöntemleri

Malların ve hizmetlerin ödemesini gerçekleştirmek için bir mobil cihazın kullanılması, sadece dijital ödemelere yönelik paradigma kaymasını temsil eder ve perakende mağazalardan alışveriş yapmak veya mobil "dijital cüzdan" kullanarak para aktarmak isteyen tüketiciler tarafından yönlendirilir.

3.1 Mobil Ödeme İşlem Döngüsü

Her teknoloji ile birlikte insanlar onu kullanmak için takip etmesi gereken bir dizi protokolü getirir. Mobil ödeme risklerini anlamak, PIN cetvellerinin mobil cüzdanla ilişkili verileri kabul etmesini, doğrulamasını ve iletilmesini analiz etmeyi içerir.
1. Kasiyer emri çalar ve ödeme talebinde bulunur
. 2. Müşteri, işlemin kimliğini doğrulamak için parmak izini tarar veya bir şifre girer.
3. Müşteri akıllı telefonu NFC destekli PIN pad'ine bağlar.
4. Akıllı telefon içindeki bir çip, PIN pad'iyle veri alışverişinde bulunur ve satın alım işlemi tamamlanır.
5. Bu durumda, en büyük endişelerden biri, mobil cüzdanın PIN pad'ine bilgi aktarma şekli olmasıdır

3.2 Mobil Ödeme İşlem Türleri ve Uygulamaları

3.2.1 Fiziksel Pos ile Ödeme

Herkesin bildiği üzere alıcının kredi kartının, satıcının pos cihazından işleme tabi tutulması ile gerçekleştirilen tahsilat. Alıcının, kredi kartı işleme tabi tutulurken kendisinin belirlemiş olduğu şifreyi pos cihazına giriyor olması güvenlik açısından bir avantaj. Ancak bunun haricinde, özellikle cari hesap tahsilatları için, bir çok dezavantajı bulunuyor fiziki pos ile tahsilat yapmanın. Güvenlik açısından artı kazandıran şifre giriş işlemi aslında bu dezavantajların başında yer alıyor. Fiziki pos cihazına şifrenin girilmesi için alıcının mutlaka pos cihazının bulunduğu ortamda bulunması gerekiyor. Bu da uzakta olan bir müşterinin tahsilatını tamamen imkansız hale getiriyor.

3.2.2 Mobil Pos ile Ödeme

Fiziki pos ile kredi kartı tahsilatını tercih edenler için doğacak en önemli dezavantajı uzakta olan bir müşteriden yapılacak tahsilatın mümkün olmaması olarak belirttim. Bu gibi durumlar için de fiziki poslara taşınma özelliği eklenerek yeni bir yöntem oluşturuldu. Taşınabilir yani mobil poslar ile uzakta olan müşteriye ulaşarak kredi kartı ile pos cihazı işleme sokuluyor ve tahsilat gerçekleşiyor. Mobil poslar, fiziki poslardan farklı olarak sadece veri özelliği bulunan mobil hatlar ile çalışıyor.

3.2.3 Mobil Uygulamalar ile Ödeme

Çoğu fiziksel POS ödemeleri çoğu akıllı telefonda bulunan Near Field Communication (NFC) teknolojisini kullanarak çalışır ve çoğu akıllı telefonda bulunanbu teknoloji temassız bankamatik / kredi kartınızdaki aynı teknolojidir. NFC, 10 cm'ye kadar mesafelerde veri aktarımına izin veren ISO / IEC 18092 standardında kablosuz iletişim teknolojisidir [5].

Google Cüzdan

Sabit bir şekilde popülerlik kazanan Google Cüzdan, bugün itibariyle yalnızca birkaç el cihazını desteklemekte.Yeni mobil cihazların çoğuna dahil olan bir NFC çipi gerektiriyor.Bu ödeme sistemini kurmak oldukça basittir. Kullanıcıların bir PIN numarası oluşturmaları ve kart bilgilerlerini uygulamaya

girmeleri gerekir. Ardından, telefonun arka yüzü, ödeme için verilen terminale karşı vurulmalıdır.Kullanıcının telefonunu kaybetmesi durumunda, Google Cüzdan hesabını kapatmak için uygulamanın yerleşik bulut bağlantısını kullanabilirler.

PayPal

PayPal ile mobil bir ödeme yapmak çok kolay ve kullanışlıdır.Tüm kullanıcıların yapması gereken, PayPal hesabını telefonlarıyla bağlamak, bir PIN kurmak ve ardından ilgili bir ödeme terminalinde ödeme işlemini tamamlamaktır.PayPal, istenmeyen sorunları önlemek için birkaç güvenlik önlemi uyguladığından, yalnızca bir telefon numarası ile ödeme yapmayı hayal etmek güvensiz görünse de, aslında oldukça güvenlidir. Bu sistem birçok kullanıcı arasında popülerlik kazanmaktadır.

Android Pay

Android Pay, google tarafından geliştirilen bir ödeme platformudur. Android işletim sistemine sahip telefon, tablet ya da saatlere tanımlanan kredi kartları ile market, giyim vb. alışverişlerde ödeme yapma imkanı sağlar.Yapılan her türlü alışverişte ödemelerin rahatlıkla ve güvenle yapılabileceği Android Pay uygulaması, NFC (Near Field Communicaion) sistemi ile çalışır. Bu sistem kişinin kredi kartı bilgilerini satıcının cihazına ulaştırarak ödeme yapmayı gerçekleştirir. Son derece güvenli olan NFC sistemi Android kullanıcılarının bilgilerini kesinlikle açıktan paylaşamaz ve kredi kartı bilgileri de üstün güvenlik önlemleri ile korunur. Ayrıca Android Pay ile Android uygulamalarını da satın alabilirsiniz.

Apple Pay

Apple Pay Apple'ın 2014 yılında ortaya çıkarttığı ve "Güvenli, Basit ve Çok Kullanışlı" sloganıyla adını öne çıkaran Apple Pay iOS cihazlar için gerek güvenlik gerek kullanışlılık ve gerekse optimizasyon bakımından bir numaralı temassız ödeme yöntemidir. Ödeme işlemini yaparken de gelişmiş güvenlik önlemlerine sahip olan Apple Pay, iPhone için ödeme işlemi sırasında TouchID (parmak izi) girişinizi ister ve Apple Watch için ise deri teması özelliğini kullanır.Buna ek olarak da NFC(Near Field Communicaion) sistemi ile de çalışmaktadır.

Samsung Pay

Samsung Pay Samsung tarafından sunulan kablosuz ödemelere adanmış yeni bir araçtır. Şu an için, mobil ödeme, bazı yeni akıllı telefon ve saatlerde bulunan NFC çipi ile çalışmaktadır.Samsung, mobil ödemelere adanmış bu süreci hızlandırmak için çalışıyor, bu şekilde, Kore bir süre önce mobil ödeme sistemi geliştiren bir şirket ile anlaşmıştır ve böylece her yerde mevcut olan manyetik POS cihazlarından ödeme yapılması mümkün olacaktır.Bu teknoloji MST (Manyetik Güvenli İletim)olarak adlanıyor ve yeni Samsung Galaxy S6 ve 6S Edge telefonlarına dahil edilmiştir. Samsung telefonlara sahip kullanıcılar Manyetik POS ve NFC ile mobil ödeme yapabilecekler. Samsung Pay ile yapacağınız ödemelerinizi 2 şekilde yapabilmektedir. Bunlar NFC sistemi ve Manyetik Güvenlik Aktarımı (MST) sistemi.
1. NFC sisteminde ödeme yapacağınız cihaza telefonunuzu ya da tabletinizi yaklaştırarak ödemenin yapılması sağlanıyor.
2. MST sistemi ise eski tip POS cihazlarında ödeme yapılabilmesini sağlamaktadır.

Bölüm 4

Riskler

Mobil ödeme ile ilgili risklerin çoğunun müşterilerin bunları nasıl kullandıklarına bağlıdır.ISACA'nın 2015 yılında 900 güvenlik uzmanını ile mobil cüzdan güvenlik tehditlerini belirlemek için yaptığı araştırma da mobil ödeme uygulamalarının yol açtığı tehditlerin de belirlenmesinde rol aldı.Bu tehditler katılımcıların kamu Wi-Fi, çalınan cihazlar ve kimlik avı kullanımını cep telefonu ödeme güvenliğindeki en büyük üç tehdit olarak kullandıklarını belirtti [2].Dolayısıyla tüketicilerin cihazlarını nasıl kullandıklarının farkında olmaları gerekmektedir. Gün geçtikçe de mobil ödemelerin altındaki altyapı daha sağlam hale gelmektedir ve şu an çoğu sistem tokenization nedeniyle doğal olarak tamamen güvenli sayılabilmektedir. Örneğin, girişimci, Samsung Pay'ın simgeleştirmeyi, KNOX güvenlik çerçevesini ve parmak izi kimlik doğrulamasını kullanarak bir sinyal saldırıya uğramadığını kaydetti. Cep telefonu ödemelerinin güvenliği konusundaki yanlış anlamalar, sektördeki büyümenin büyük kısmını engelledi, ancak bu algı değiştikçe daha fazla tüketicinin daha akıllı telefonlarıyla daha hızlı ödeme yapabilmelerini sağlayacaktır.

4.1 Kamuya Açık Wi-Fi Kullanımı

Kamuya açık wi-fi'ye dokunmak, dışarıda olduğunuzda iyi bir çözüm gibi görünebilir. Sorun şu ki, halka açık Wi-Fi, bilgisayar korsanlarının sizin güvenceye almamış verilerinize erişiminin tehlikeye girmesine neden olmaktadır. Kendinizi korumak için VPN ve SSL bağlantıları kullanabilirsiniz. Bu hizmetler kullanılmadığında paylaşımı ve wi-fi'yi kapatmak da birçözüm olarak uygulanabilir.

4.2 Savunmasız Ödeme Teknolojileri

bilgisayar korsanları herhangi bir güvenlik açığını kullanarak mobil cihazınız, giyilebilir araç veya ev otomasyonunuza saldırabilmektedir. En son ödeme teknolojisinin tüm güvenlik açıklarını anlayıp her biri için ayrı önlemler aldığını varsaymak pek dogru olmayacaktır.Buyüzden kullanıcı tarafından alınabilecek olam önlemler her uygulama ve akıllı cihaz için alınmalıdır.Bu önlemler şu şekilde sıralanabilir:
1. Güçlü bir şifreye sahip olmak ve sık sık değiştirmek
2. İki faktörlü kimlik doğrulama
3. Verileri şifreleme
4. Yazılım güncellemelerini derhal yüklemek
5. Yalnızca güvenli olduğunu bildiğiniz sitelerde alışveriş yapmak
gibi temel güvenlik önlemlerini takip ederek kişisel bilgiler güvende tutulabilmektedir.

4.3 Kimlik Avı(Phishing) Saldırıları

Kimlik avı dolandırıcılıkları bir e-postanın veya web sitesinin sizden bilgi çalmaya çalıştıkları dolandırıcılık tipidir.Kimlik avı, insan hatası yüzünden hala etkili bir saldırıdır. Kimlik avı e-postalarını engelleyen bir yazılım kullanılsa bile, yasal bir e-posta bu engelden geçebilir.Bu yüzden gelen e-postalar kaynağı bilinmeden veya güvenilir olduğu belirlenmemiş kaynak tarafından gönderiliyorsa açılmaması bu saldırıarı önleyebilir.

4.4 Platform Seçimi Kaynaklı Güvenlik Açıkları

Bir mobil ödeme planının ne kadar güvenli ve güvenli olursa olsun, şemayı uygulamak için seçilen platformdaki güvenlik açıklarından dolayı güvende olmayabilir. Birçok araştırmacı, J2ME'yi kullanarak m-ödeme sistemleri için prototip geliştirdi.Fakat bazı Java özellikli telefonlarda, kullanıcının yetkilendirmesine gerek duymadan SMS mesajları gönderen kötü amaçlı bir yazılım olan MIDlet yazmak üzere kullanılabilecek bir güvenlik açığını bulunmaktadır. Bu, kullanıcının, bir işlemi başlatmak için bir SMS mesajı (ödeme ağ geçidine) göndermesini gerektiren bazı SMS tabanlı şemaların güvenliğini etkileyebilmektedir.SMS mesajı gönderen kullanıcının telefonuna kötü niyetli bir MIDlet kurulmuşsa, kullanıcının onayını almadan bir işlemi başlatmak mümkün olacaktır [9].

4.5 Mobil Zararlı Yazılımlar ve Casus Yazılım Kullanımı

Mobil zararlı yazılım dünyasının solucanlar veya virüsler tarafından değil, truva atları tarafından yönetildiğini göstermektedir [9]. Bunun temel nedeni, Truva atlarının herhangi bir yayılım vektörüne ihtiyaç duymaması ve yalnızca onları indirip yüklemek için kullanıcının merakına güvenmesidir.Zararlı yazılım içerdiğinden habersiz olan kullanıcı uygulamayı yükledikten sonar bu tür yazılımlar mobil ödeme için gerekli olan SMS doğrulama kayıtlarına kadar ulaşabilmekte ve büyük bir risk oluşturmaktadırlar.Böyle bir casus yazılıma bir örnek, vahşi doğada olan Flexispy 'dir [10].Belli bir süre için SMS tabanlı bir mobil ödeme sisteminde, kötü niyetli bir saldırgan bu tür casus yazılımlarda ufak değişiklikler yapabileceği ve bir kullanıcı tarafından yapılan tüm işlemleri izleyebileceği için, bu zararlı yazılım kullanıcının gizliliğini ciddi şekilde etkileyebilir. PbStealer ismiyle bir başka casus yazılım, kullanıcının telefon defterindeki tüm kayıtları çalabilmektedir [11]. Bu casus yazılım, telefon defterini sıkıştırarak bellek alanından tasarruf edebilecek bir yardımcı program olarak taklidi eder. Bununla birlikte, telefon rehberini sıkıştırmak yerine, tüm girdileri bir metin dosyasına kopyalar ve bu dosyayı menzil içindeki herhangi bir Bluetooth cihazına gönderir.

Kötü niyetli bir saldırgan, bu casus yazılımın hassas verilerini kullanıcının telefonundan çalmak için değiştirebilir .Kısa süre önce ,kullanıcının onayı olmaksızın premium telefon numaralarına SMS mesajları gönderebilen ve böylece kullanıcıya maddi hasar verebilen başka bir Trojan (Viver) keşfedildi [12].Bu tür Truva atları, bir işlemi başlatmak ve yetkilendirmek için SMS mesajları kullanan gibi mobil ödeme sistemlerinin güvenliğini ciddi şekilde etkileyebilir.Yukarıdaki bilgiler, mağdurun cihazından SMS mesajları (veya başka herhangi bir veri) sızlayan / çaldığı / gönderdiği kötü amaçlı yazılım yazmanın mümkün olduğunu göstermektedir.

Bölüm 5

Güvenliğin Sağlanması

Uygulamanın güvenliğini kendi sağlaması hem tercih edilmesi hem de güvenilirlik açısından büyük talep farkları oluşmasında bir etkendir.Bu yüzden mobil ödeme uygulamalarının güvenliğinin bazı temeller kapsamında geliştirilmesi için PA-DSS standardı bulunmaktadır.Ödeme Uygulamaları Veri Güvenliği Standardı (PA-DSS), yazılım tedarikçilerinin PCI DSS uyumluluğunu destekleyen güvenli ödeme uygulamaları geliştirmelerine yardımcı olmak için tasarlanmış bir dizi gereksinimdir. PA-DSS, ödeme kartı sahibinin verilerini bir yetkilendirme ya da çözümün bir parçası olarak saklayan, işleyen veya ileten üçüncü taraf uygulamaları için geçerlidir. Tüccarlar tarafından kendi bünyelerinde kullanılmak üzere geliştirilen yazılım uygulamaları yalnızca PA-DSS'den muaftır ancak PCI DSS'ye uymak zorundadır. PA-DSS uyumluluğunu sağlamak için bir yazılım sağlayıcısı, başvurusunu bir PA-DSS Kalifiye Güvenlik Testi Denetçisi tarafından denetlenmelidir. PA-DSS gereksinimleri şunları içerir:
1. Tam manyetik şerit, kart doğrulama kodu veya değeri veya PIN bloku verileri bulundurmayın.
2. Güvenli parola özellikleri sağlayın.
3. Saklanan kart hamiline ait verileri koruyun.
4. Uygulama etkinliğini günlüğe kaydet.
5. Güvenli uygulamalar geliştirin.
6. Kablosuz iletimleri koruyun.
7. Zayıf noktaları ele alan uygulamaları test edin.
8. Güvenli ağ uygulamasını kolaylaştırın.
9. Kart sahibi bilgilerini İnternet'e bağlı bir sunucuda saklamayın.
10. Güvenli uzaktan yazılım güncellemelerini kolaylaştırın.
11. Uygulamalara güvenli uzaktan erişimin kolaylaştırılması.
12. Hassas trafiği genel ağlar üzerinden şifreleyin.
13. Tüm konsol dışı yönetimsel erişimi şifreleyin[4].

Bölüm 6

Güvenlik Çözümleri

Mobil ödemelerin hızlı ve kolay olması gerekir. Fakat bu uygulamaların dolandırıcılığı önleyecek ve müşterilere mobil cüzdanlarda ve ödeme uygulamalarında güvenliği de sağlaması gerekmektedir.Mobil ödeme işlemlerinin kimliğini doğrulamak ve mobil, temassız dünyadaki müşteri verilerini güvence altına almak için çeşitli seçenekler bulunmaktadır. Fakat temelde taşınabilir aygıtlardan Uygulama Sunucusuna güvenli veri aktarımı gerçekleştiginden emin olunarak ve yerel el cihazlarında veri depolama güvenliğini sağlayamak da güvenlik önlemi alınmasını belirli bir oranda sağlayabilmektedir.

6.1 Kullanıcı Çözümleri

Mobil Ödeme işlemleri kullanıcı tarafından aşağıdaki etkenler gözetilerek de güvenceye atına alınabilir.
• Uygulamada uygun oturum yönetimini uygulayacağından emin olunarak.
• Uygulamaların güvenli yürütülebilir olduğundan emin olunarak.
• Uygulamada tüm güvenilir ve güvenilmeyen (Geçersiz kullanıcı girdileri, örneğin özel karakterler) girişlerin geçerliliğini onaylayarak.
• Uygulamada güçlü kimlik doğrulama mekanizmasının uygulanmasını sağlayarak.
• Güvenli web hizmetleri ve arayüzler kullanarak.
• Cihazın kaybolması ve çalınması durumunda mobil cihaz güvenlik garantisine sahip olunarak. [13]

6.2 Donanımsal Çözümleri

Mobil cihazın kendi içerisinde alınabilecek donanımsal çözümler ile izinsiz SMS gönderimi gibi bazı etkinlikler önlenebilir.

1. Multi-Tenant SIM
Multi-Tenant SIM, birden fazla servis sağlayıcının, ödeme kimlik bilgilerinin güvenli, özel kurulum ve yönetimi için el cihazının SIM kartındaki alanı paylaşmasına izin verir.
2. Embedded Secure Element
Embedded Secure Element, SIM kart yoksa bile kimlik bilgilerini sabit aygıta mobil cihazda depolayarak son derece güvenli bir çözüm sunar.
3. Micro SD
SD çözümleri, telefonunuza ve gerektiğinde güvenli bir öğeyi bağlayabileceğiniz anlamına gelir. Çözümün esnekliği, gerektiğinde güvenlik ve diğer ödeme uygulamalarını enjekte edebileceğiniz anlamına gelir. **4. Trusted Execution Environment (TEE)**
Trusted Execution Environment (TEE) (Güvenilir Yürütme Ortamı), hassas verileri depolayan, işleyen ve koruyan bir mobil aygıt işlemcisinde güvenli bir alan sağlar.TEE, koruma, gizlilik, bütünlük ve veri erişimi hakları için 'güvenilir uygulamalar' kullanmaktadır. **5. Tokenized payment credentials**
Tokenized payment credentials(Simgeleştirilmiş ödeme kimlik bilgileri), ödeme işlemlerinde, mağazada veya çevrimiçi olarak ve bulutta saklanan hassas kimlik bilgilerinin yerine kullanılır. Bunlar, HCE özellikli cihazlar, Güvenli Öğeler, TEE gibi her tür cihaza kurulabilir

6.3 Satıcı Tabanlı Çözümler

Yazılan uygulamanın her risk açısından değerlendirilmesi,güncel açıkların takip edilerek bunların çözümlerine ulaştırılması ve gerekli önlemlerin alınarak ardından kullanıcıya sunulması ile satıcı firmanın güncel yazılımlar kullanarak mobil ödeme güvenliğini sağlamasında üzerine düşen yükümlülüktür.
"Veri saklama risklerinin şiddeti büyük ölçüde ürüne bağlıdır. Örneğin Android Pay, kullanıcıların kredi veya bankamatik kartı bilgilerini asla iletmez; kart numaralarını temsil etmek için simgeleri kullanır. Aslında, uygulama kredi kartı numaralarını bile saklamaz ve bir kullanıcının gönderdiği her kart için bir belirteç oluşturur" [6]. Apple Pay benzer bir süreç kullanmaktadır. Bir müşteri bir ödeme kartını Apple Pay'a girdiğinde, uygulama verileri şifreler ve Apple'ın sunucularına gönderir. Apple, kartın ödeme ağını tanımlamak için verileri çözer ve yalnızca kart düzenleyicisinin ve yetkili sağlayıcıların açabileceği bir anahtarla yeniden şifreler. Ardından, bu bilgiyi bankaya gönderir; bu, bir aygıt hesap numarası oluşturur ve Apple'a gönderir. Apple, aygıt hesap numarasını şifresini çözmez ve müşterinin telefonundaki güvenli öğeye(secure element) gönderir [13].

References

[1] Statista, “Mobile payment security concerns in the United States in 2015, https://www.statista.com/statistics/244322/mobile-payment-security-concerns-of-us-consumers/

[2] ISACA, ”2015 Mobile Payment Security Study Global Survey”, http://www.isaca.org/Pages/mobile-payment-security-study.aspx?cid=pr_1110000&appeal=pr

[3] PA-DSS (Payment Application Data Security Standard), Maggie Sullivan, http://searchsecurity.techtarget.com/definition/PA-DSS-Payment-Application-Data-Security-Standard

[4] The Mobile Money Revolution,Part 1: NFC Mobile Payments,ITU-T Technology Watch Report May 2013

[5] Chip PIN Çözümleri Android Pay açıklaması,28 Eylül 2016 , https://t.co/WDS4f6HQr5

[6] Mobile Payment Services: Security Risks, Trends and Countermeasures,Suhas Desai Practice Head – Cloud Mobile Security

[7] Security, Security Issues in Mobile Payment Systems, Shivani Agarwal1*, Mitesh Khapra1, Bernard Menezes1 and Nirav Uchat1

[8] Mobile Malware Evolution: An Overview, Part 1. (Online), http://www.viruslist.com/en/analysis?pubid=200119916.

[9] F-Secure Malware Information Pages: Flexispy.A. (Online), http://www.f-secure.com/vdescs/flexispy_a.shtml

[10] F-Secure Virus Descriptions: Pbstealer.A. (Online , http://www.f-secure.com/v-descs/pbstealer_a.shtml

[11] F-Secure Malware Information Pages: Trojan:SymbOS/Viver.A. (Online) , http://www.f-secure.com/vdescs/trojan_symbos_viver_a.shtml.

[12] Security, MobilityHow Secure are Mobile Payments?Datacap Systems inc. February 1, 2017 , https://www.datacapsystems.com/blog/2017/2/1/how-secure-are-mobile-payments