Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security of Mobile Banking and Payments

A clear and emerging new channel in the space of banking and payments is mobile. A key challenge with gaining user adoption of mobile banking and payments is the customer s lack of confidence in security of the services. Understanding the mobile banking and payments market and ecosystem is critical in addressing the security challenges. There are new security risks introduced with mobile banking and payments that must be identified and mitigated. There are risks that have both an existing mitigation method as well as t...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Security of Mobile Banking and Payments

GIAC (GSEC) Gold Certification

Author: Vanessa Pegueros, vpegueros@gmail.com
Advisor: Johannes B. Ullrich, Ph.D.

Accepted: November 1, 2012

Abstract

A clear and emerging new channel in the space of banking and payments is mobile. A key challenge with gaining user adoption of mobile banking and payments is the customer's lack of confidence in security of the services. Understanding the mobile banking and payments market and ecosystem is critical in addressing the security challenges. There are new security risks introduced with mobile banking and payments that must be identified and mitigated. There are risks that have both an existing mitigation method as well as those that do not have a clear risk mitigation solution.

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

1. Introduction

There doesn't seem to be a week that something relative to mobile and/or mobile payments is not in the news. Mobile and everything mobile is the current hot area where new investments and new ideas are blossoming in the hopes of being part of the next "big thing" that generates healthy returns and wealth. Consumers are embracing mobile in their day to day lives and are more likely to forget their wallet at home than their mobile phone. With all this energy and momentum around mobile, as with any new next big thing, there are some areas of concern to consider.

A key area of concern for consumers and financial service providers is the security of mobile banking and payments. There are new technologies and new entrants as well as a complex supply chain that will increase the security risks. There is no real standard for technology that has captured the market and regulations relative some of the new entrants are non-existent. Customers have increased control of their device in terms of application downloads, OS updates and personalization of their devices. This will lead to new challenges relative to privacy and will take some time before the younger generation realizes the implications of privacy violations. Compounding the challenge is the fact that traditional security controls such as AV, firewalls, and encryption have not reached the level of maturity needed in the mobile space.

As with any emerging market area, these challenges will resolve over time. Until this are matures, there are measures that can be taken relative to customer education, service process rigor, payments technology and fraud preventive and detective controls that can mitigate the security risks.

2. Mobile Banking Definition

Mobile banking can be broken into three key areas: Informational, Transactional, and Service, Marketing & Acquisition

Within the area of informational there are functions such as balance and transaction history, loan, mortgage, and credit information, ATM and branch locators, as well as personal financial management (PFM) functions such as spending comparisons

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

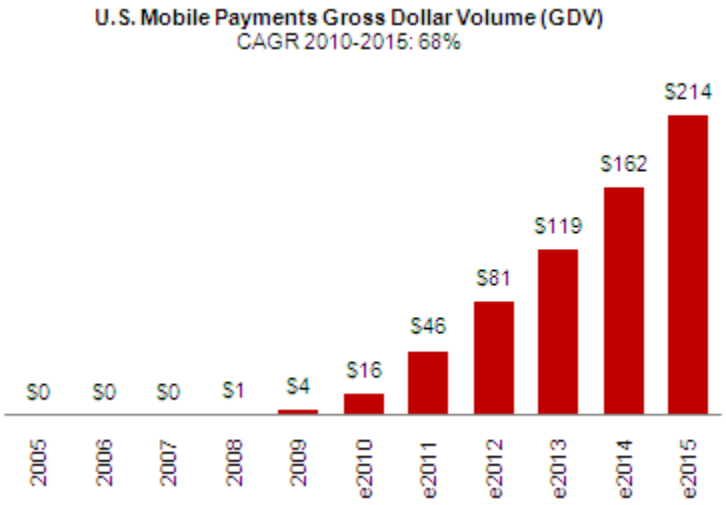
with peers or budget tools. Transactional services included account transfers, bill pay, person to person payments and remote deposit capture. Service features included functions that enhance the customer's experience including contact options, help information, and alerts. Additional service features include product renewal notifications, balance triggered savings offers, balance triggered credit offers, and location triggered travel insurance options. Finally, relative to marketing and acquisition, there are services such as mobile coupons/incentives, barcodes, new product information, customer research, cross selling and acquisition. The aspects of mobile that make it particularly appealing to marketing are the very personal nature of mobile devices and the "always on" aspect of customer use.

There are two different types of mobile payments to draw a distinction between throughout this paper. The first type of mobile payment is a mobile application (mobile wallet) that allows payment to be processed through the mobile carrier's network as in the case of Paypal or your Bank. A mobile wallet has several key components including ability to provision account information, payment origination and payment processing. The second type of mobile payment is through contactless technologies such as Near Field Communication (NFC) built into the phone. In the case of contactless technologies, the payment traverses the merchant's POS system and the relevant payment processing environment not relying on the mobile carrier's network.

2.1. Markets and Trends

As noted in the graph below, the revenue associated with mobile payments is expected to grow exponentially through 2015. The convenience of using the mobile device as the single method of payment will drive users away from the traditional "wallet" with numerous payment cards. The single wallet on the device (mobile wallet) will allow consumers to manage their finances through a single interface including prepaid cards, loyalty cards and traditional debit/credit cards. In addition, consumers will be able to conduct traditional forms of banking such as check deposit, checking balances, bill payment and transferring funds with their mobile device.

© 2012 The SANS Institute Author retains full rights.



(Aite Group, 2010)

The factors driving the increasing adoption of mobile banking are numerous including consumerization of Enterprise IT, generational use trends and smartphone growth. A key result of this this trend will be the extinction of the bank branch as it exists today.

Consumerization of Enterprise IT represents the growing trend of employees bringing their personally owned mobile device into the work environment and causing stress to the IT organizations in demanding access to the Enterprise environment through that device. This is a particularly challenging problem with the IT systems and processes that are not prepared to manage these devices. IT organizations struggle with issues such as applying and enforcing standard OS images, maintaining the patches and security controls and restricting unapproved applications on mobile devices. These issues continue to be a challenge for organizations as employees blend their personal and work life. Enterprises must address these issues as they can become victim to an unacceptable level of Compliance and IT risk.

Consumers are using their devices increasingly in their everyday life and activities. Based on a report done by the Federal Reserve, consumers are increasing using their phone for mobile banking activities.

Vanessa Pegueros, vpegueros@gmail.com

© 2012 The SANS Institute Author retains full rights.

Using Your Mobile Phone, Have You Done Any of the Following in the Past 12 months?

Activity	Percentage of respondents doing the Activity
Checked an Account Balance or Checked Recent Transactions	90%
Downloaded your bank's mobile bank application	48%
Transferred money between two accounts	42%
Received a text message alert from your bank	33%
Made a bill payment using your bank's website or application	26%
Located the closest in network ATM for your bank	21%
Deposited a check to your account using your phone's camera	11%
Manage your investments	2%

("Consumer and Mobile Financial Services," 2012)

From a generational perspective when looking at the age groups that utilize mobile banking the most, 37% of the usage is with 18-29 year olds and 36 % is with 30-44 year olds. ("Consumer and Mobile Financial Services," 2012) Businesses recognize that they will need to appeal to the needs of the younger generation and their desire to conduct daily activities including banking and payments on their mobile device.

2.2. Ecosystem and Competitive Landscape

The ecosystem of mobile banking is complex and this leads to some of the challenges when addressing issues of security. There are numerous players involved including:

Customers, merchants, banks, debit/credit card networks, clearing/settlement organizations, application providers, 3rd party payment providers, wireless carriers, and handset/chip manufacturers.

In order to understand the complexity, it is useful to walk through the different actors involved in credit card payments. The card holder is the consumer who applies for a credit card through some bank. The bank that issues and extends credit to the card holder is called the Issuer or Issuing Bank. The issuing bank assumes the liability of the card holder purchase. The merchant is the place of business whereby the cardholder uses their card to purchase goods or services offered by the merchant. The merchant must

© 2012 SANS Institute Author retains full rights.

obtain a merchant account prior to being allowed to process credit cards and receives this account through a merchant service provider or merchant bank (acquiring bank). The merchant service provider is responsible for all communications and relationships on behalf of the merchant to other players in the ecosystem. Processors provide a point of connectivity for the merchants to authorize and settle credit card transactions through appropriate payment networks. In some cases the merchant service provider and processor are part of the same company. Card associations are companies such as Visa, MasterCard, American Express and Discover. In the case of American Express and Discover they are the issuing bank, the merchant bank and the card association.

The other key complexity of the ecosystem is the mobile handset and wireless carrier component of the landscape. The diversity of handset manufacturers is growing and dynamic with some traditional players such and Nokia and Motorola losing market share and new players such as Samsung and Apple gaining significant market share. As noted in the chart below, In 1Q 2012, Samsung supplanted Nokia as the world's leader in device manufacturing and took over the top spot in the smartphone market from Apple. Blackberry a long time leader in the smartphone space declined to 2009 levels in terms of devices shipped. HTC remains a strong player in Asia/Pacific but has struggled somewhat in the US Market.

Top Five Worldwide Smartphone Vendors, Shipments, and Market Share, Q1 2012 (Units in Millions)

Vendor	1Q12 Unit Shipments	1Q12 Market Share	1Q11 Unit Shipments	1Q11 Market Share	Year-over-year Change
Samsung	42.2	29.1%	11.5	11.3%	267.0%
Apple	35.1	24.2%	18.6	18.3%	88.7%
Nokia	11.9	8.2%	24.2	23.8%	-50.8%
Research In Motion	9.7	6.7%	13.8	13.6%	-29.7%
HTC	6.9	4.8%	9.0	8.9%	-23.3%
Others	39.1	27.0%	24.5	24.1%	59.6%
Total	144.9	100.0%	101.7	100.0%	42.5%

("Worldwide Smartphone Market Continues to Soar," 2012)

Vanessa Pegueros, vpegueros@gmail.com

© 2012 SANS Institute, Author retains full rights.

In addition to the hardware diversity, the variety of operating systems on these devices continues to grow. RIM has continued to decline in market share since the advent of iOS and Android and no longer holds the number one spot with approximately 4% of the total market. Android continues to have numerous versions within the marketplace and shows no signs of decreasing. iOS is well controlled both from a hardware and software perspective. Microsoft seems to have finally developed a mobile OS worth talking about in Windows 7 and with the advent of Windows 8 may finally be able to capture some relevant market share. As the tablet space grows, there will likely be a further acceleration to mobile banking. While the technologies struggle for dominance, so do the various companies in this space.

The carriers have a strong customer connection and control the mobile device services as well as the payment process for that service with the customer. They are attempting to gain a more significant presence in this ecosystem through partnerships such as ISIS. In 2010 AT&T, Verizon and T-Mobile entered into a joint venture (ISIS) to establish a mobile payments network. The device technology they chose to use was Near Field Communications (NFC) explained later in this paper.

Traditional financial institutions such as banks have key advantages including the customer relationship, their focus on fraud and security which reduces the risks to customers, and an imbedded infrastructure and mature processes. Financial services are motivated to maintain these advantages and gain revenue share in emerging payments areas. A starting point for many banks is launching their branded mobile wallets. Based on a 2012 study by Forrester, Chase, Citibank, Bank of America and Wells Fargo lead the way relative to mobile banking functionality. (Wannemacher, 2012) Some of the key recommendations made to banks to continue their growth in mobile banking were to continue to use the mobile channel (SMS, dedicated mobile websites, native mobile apps, and tablets) to engage and interact with their customer base through service and value add products, continue to make the enrollment and login experience user friendly, and to ensure that mobile banking is integrating across their digital footprint thereby leveraging the rich information about the customer and having their experience feel more integrated.

Vanessa Pegueros, vpegueros@gmail.com

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Card associations are partnering with other members of the ecosystem to extend their footprint in the ecosystem. Discover partnered with Paypal to launch a person to person (P2P) payments solution to address a need identified through their personal financial management (PFM) application. Visa acquired Fundamo which provides mobile financial services in emerging markets and gave Visa access the area of the unbanked and under-banked population.

There are new vendors sitting within the processor space such as Intuit, Square, and LevelUp. LevelUp is essentially a middleware component that accomplishes aggregated transactions and minimizes fees. Square provides software and a small credit card swiper that connects to the 3.5mm headset jack of the device.

Within the application space there are numerous new companies developing mobile payment applications. A key advantage of these new entrants includes innovative customer solutions. Paypal is providing apps to mobile devices and the APIs to developers so that the Paypal apps can be added to new applications. PayPal facilitates payment methods between individuals and on-line merchants. Through this positioning Paypal can control the relationship between customer and merchants while cutting out the traditional financial service institutions. Google has developed Google wallet an app and payment system that utilizes NFC to combine deals and discounts with digital payments.

3. Key Technologies

3.1. Mobile Elements

In understanding the security risks of mobile banking, it is useful to understand the general hardware and system software of a mobile device. The most prevalent technology relative to mobile devices and the associate wireless carriers today is based on 2G technology (GSM/EDGE) and 3G technology (UMTS/HSPA) standards. The latest technology currently being rolled out by major carriers is Long Term Evolution (LTE) which doesn't currently meet the requirements to be considered 4G (speeds of up to 100Mbps for a moving user and 1Gbps for a stationary user) but is being marketed as 4G. The basic components of a wireless network include the spectrum for the wireless interface, the antennas and radio processing equipment located at the base station or cell

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

sites, and the connectivity (T1, microwave) from the cell site back to the mobile switching center that contains the voice and data processing equipment. The security elements for 3G technology include encryption on the air interface and mutual authentication between the user and the network (involving the HLR and USIM).

Turning to the mobile device itself, the basic mobile software framework consists of the kernel, libraries, the application framework, and finally the applications themselves. The kernel layer or operating system layer contains memory management programs, security settings, device drivers and power management software. The middleware layer includes main libraries and services such as data storage, virtual machines and multimedia libraries. Libraries are a set of instructions that tell the device how to handle different kinds of data. For example, the media framework library supports playback and recording of various audio, video and picture formats. The application framework includes programs that manage the devices basic functions like resource allocation, phone applications, switching between processes or programs and keeping track of the phone's physical location. Finally, you have the applications themselves which are the predominant space end users interact.

To build an application, a developer must be familiar with the device programming language. The developer will need access to the device software developer kit (SDK). The SDK gives the developer access to the device's application programming interface (API). The SDK includes several tools, including sample applications and a phone emulator. Emulators are programs that duplicate the features and functions of a specific system or device. When the developer finishes building an application, they can test it out on the emulator to see how the app will perform on actual hardware.

A key component of the device security is the operating system. The 3 most compelling OS' are Android, iOS, and the yet to be launched Windows phone 8. While RIM had been a large Enterprise player, it is losing market share quickly. Since 2009, the RIM market share has dropped from 20% to approximately 4% in 2012. According an IDC's study published in May 2012, Android shipments during 1Q 2012 totaled 89.9 million units, up 145% from 36.7 million in the first quarter of 2011. iPhone shipments were up 88.7% over the first quarter last year to 35.1 million units, giving Apple 23% of

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

the smartphone market in the first quarter compared to Google's 59% share. ("Worldwide Smartphone Market Continues to Soar," 2012) Windows Phone 8 is scheduled to launch sometime in the Fall 2012.

3.2. Payments Technology

The primary elements of mobile payments technology include NFC, SE, and TSM.

The use of Near Field Communications (NFC) for mobile payments is governed by the ISO 18092 standard and has the following attributes:

- Is limited to a 424 kilobits per second data transfer rate,
- Supports communication ranges up to approximately 0.2 meters
- Offers no native encryption

Under the typical scenario, NFC communications are established automatically when two compatible devices are brought within range of each other; however, the NFC technology in mobile computing and other devices used for mobile wallet transactions is typically tuned for a much shorter range, on the order of a few millimeters.

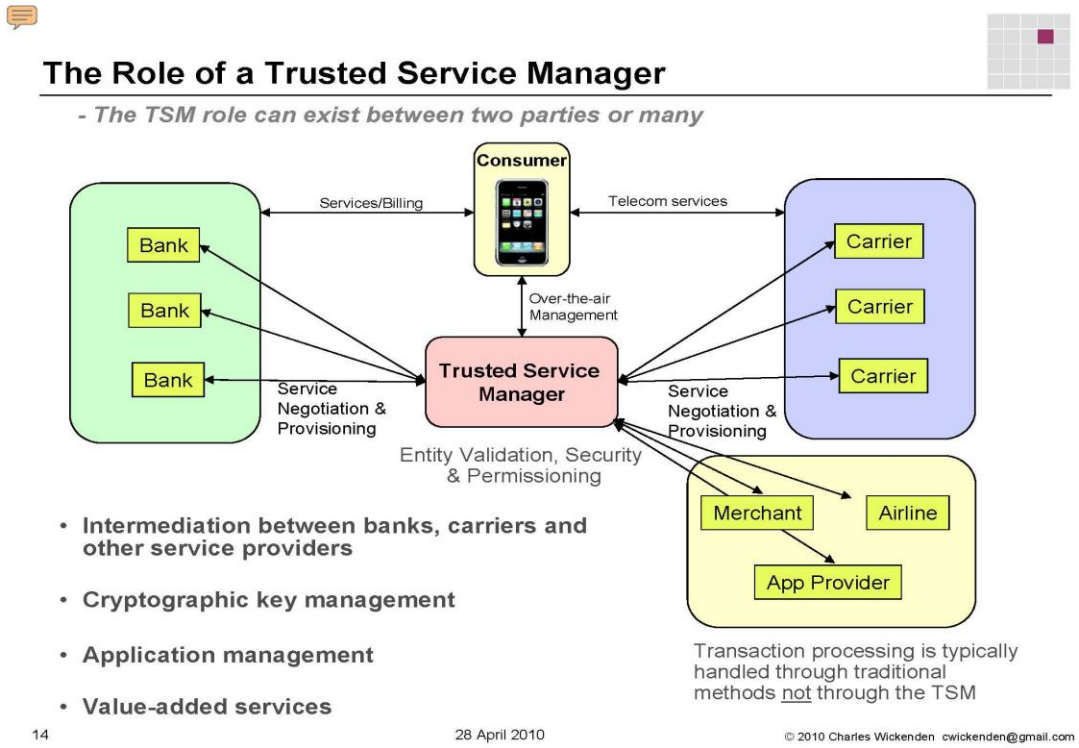
Since NFC offers no native encryption, mobile payments using NFC must be coupled with a Secure Element (SE) which is a cryptographic module in the mobile device. The exact implementation of a SE in the mobile device has still not been standardized and there are 3 competing options: 1) build it into a chip on the mobile device 2) implement it into the existing SIM chip 3)implement through micro SD cards. ISIS and MasterCard are leveraging the SIM approach while Google wallet is using phone that have built in modules.

The Trusted Service Manager (TSM) handles transactions from a single financial institution to act as an interface to the payments ecosystem. Key functions include:

- Management of business rules, authentication
- Connect MNOs and service providers
- Guarantee end-to-end security; manage secure element key
- Application life cycle management for MNO, hand-set & customers
- End-to-end customer support

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.



4. Key Security Risks

A major challenge for the adoption of mobile banking technology and services is the perception of insecurity. In the survey conducted by the Federal Reserve, 48% of respondents cited their main reason for not using mobile banking was "I'm concerned about the security of mobile banking". In the same study, respondents were asked to rate the security of mobile banking for protecting their personal information and 32% rated it as somewhat unsafe and very unsafe, while 34% were not sure of the security. These statistics represent a significant barrier to the use of mobile banking products and services. ("Consumer and Mobile Financial Services," 2012)

When you analyze the security risks of the mobile space, many of these feelings are not necessarily irrational. The lack of maturity of the mobile banking space brings many risks in the areas of new technologies, new inexperienced entrants in the ecosystem and a complex supply chain with risks in secure integration of the complex ecosystem. Many of these new entrants are innovative and dynamic with minimal experience or

© 2012 The SANS Institute Author retains full rights.

attention to security as a discipline. These risks are most evident in the mobile application development and mobile hosting areas. New privacy risks are brought to light with personal data collected by the applications and information about the customer's physical location. Finally, customers are largely uneducated or have a high risk tolerance and unfortunately may opt into services that put their security and privacy in jeopardy.

The security risks associated with mobile devices are very similar to any other computing device with a few key exceptions:

- Mobile devices have a smaller form factor and therefore are more susceptible to loss or theft
- Mobile devices are more personal and there will be a tendency for users to use devices in a more personal and confidential way
- Security controls and tools available have not matured to accommodate the constraints of limited processing power and limited battery life

The key risks to the mobile device include:

- Malware
- Malicious applications
- Privacy violations relative to application collection and distribution of data
- Wireless carrier infrastructure
- Payments infrastructure/ecosystem
- SMS vulnerabilities
- Hardware and Operating System vulnerabilities
- Complex supply chain and new entrants into the mobile ecosystem
- Lack of maturity of Fraud tools and controls

4.1. Mobile Device and Application Vulnerabilities

Malware is becoming a growing challenge with mobile devices and according to a report by Juniper, the amount of malware targeted at mobile devices rose by 155% in the past year. (Morgan, 2012) Ninety nine percent of the malware growth was in two

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

categories: spyware and SMS Trojans. Malware has been specifically troublesome for the Android platform with malware increasing exponentially from 400 identified samples in June 2011 to 13000 in December 2011. (Jackson, 2012) According to a Kaspersky Lab report, malware targeted at mobile devices increased 6.4 times in 2011, with the overwhelming majority of detected mobile backdoors targeting Android devices. ("Mobile malware increased six-fold in 2011," 2012)

A key vector by which malware gets to the mobile device is through malicious applications. The integrity of applications is key risk relative to mobile devices. There are various malicious applications posing as legitimate applications that users download and then become infected. In April of 2012, it was discovered that a malicious version of the Instagram app (popular free photo sharing application) for Android was being pushed to Russian Android users offered from a web site that appeared to be the legitimate download site. ("Malware disguised as new Instagram Android app," 2012)

Compounding the risk of application integrity is jail breaking. Jail breaking is a form of privileged escalation that allows a user to gain root access of a device which allows access to all files, hidden files or protected files on the device. Once a device is jail broken the user can install any application they wish on the device without going through the sanctioned store of the device manufacturer. Jail breaking also enables the user to utilize the phone on a different wireless carrier since carriers often lock a device onto their network.

Jail breaking exposes the device to increased security risk as the standard device protections are now possibly compromised by actions of the user or an uncertified application. Additionally, the warranties of the device may be nullified when a device is jail broken. Despite these risks, the efforts to overcome the manufacturer's impediments to jail break persist. In May 2012, an un-tethered jailbreak (Absinthe 2.0) for iOS 5.1.1 became available for download. (Essers, 2012) Un-tethered jailbreaks allow devices to remain jail broken even after reboot.

There also exist vulnerabilities related to specific mobile device manufacturers and OS versions. Similar to the traditional computer space, OS vulnerabilities are being

© 2012 The SANS Institute Author retains full rights.

discovered fairly routinely. The difference in the mobile space is that there is no dominant OS and therefore is a more complex environment to address OS vulnerabilities. In addition, end users are in control of the patching of their devices and this fact leaves the security of the device at great exposure since some end users will be diligent and some will not in terms of updating their OS.

Short Message Service (SMS) is susceptible to misuse including redirection, hijacking and spoofing. In early 2012, a programmer developed a program that could allow anyone to launch social engineering attacks, spoofing SMS with the purpose of obtaining valuable information and potential even money. (Kovacs, 2012) The SMS channel can also be compromised by malware as was the case with a malicious application posing as a free well known Android application. The malware was dubbed Android.Opfake designed solely to surreptitiously "send SMS texts to premium-rate numbers," until the smartphone owner's account balance was maxed out. (Schwartz, 2012) Another fake Gmail Android application called DDSpy was capable of intercepting and uploading SMS messages, call logs, and vocal records to a remote server. (Danchev, 2012)

4.2. Privacy

Privacy of user information is a particularly challenging issue as mobile devices are much more personalized and tied to the user's identity than a traditional computer. Risks related to legitimate applications passing user data to other applications or 3rd parties in an unauthorized manner is gaining more attention in the public arena. One recent case included EU customer personal data being sent to a US based advertiser. In this situation several Android applications were accused of breaking EU data protection laws by passing personal information to a US advertising firm named MobClix without user's explicit permission. (Worth, 2012) There can also be security vulnerabilities associated with the OS that give unauthorized access to user information or content. In early 2012, there was a vulnerability discovered on both iOS and Android that gave applications access to the user's photo library without permission. (Chen, 2012) Geo-location is additional information that can be gathered by the application and shared in an unauthorized manner. This is a particularly challenging issue since many apps ask the

© 2012 The SANS Institute Author retains full rights.

user permission to use their location data; unfortunately it is not clear all the ways that application may use the data.

4.3. Wireless Carrier

In addition to the internet, mobile devices have another key network involved in the processing of mobile communications. The wireless carrier is the primary interface to the mobile device. The radio component of the mobile device communicates to the cell sites. The cell sites then communicate through dedicated circuit or microwave to the mobile switching center (data center) which contains both the voice processing and data processing equipment and systems. The switching center contains the gateway to the Internet and other carrier networks. If there is a security weakness in any part of this network, it can put the customer's data at risk.

4.4. Payments Technology

The payments infrastructure can also have vulnerabilities that lead to security risk. This can come in the form of POS vulnerabilities or the actual complex ecosystem previously noted in the Ecosystem and Competitive Landscape portion of this paper. In the Black Hat conference held this year, security researchers exposed vulnerabilities in three POS devices and were able to steal credit card information and PIN numbers.

As mentioned previously, NFC does not have native encryption capabilities and therefore is vulnerable to security exploits if not properly implemented. RF signal which NFC works from has the potential to be read or intercepted up to several meters away with the proper equipment without needing line of sight. Appropriate encryption will provide adequate protection against eavesdropping.

The keys stored on the secure element can be vulnerable to exposure if the keys are not protected properly from unauthorized access and use. Mobile payment applications employ a pin or password that is required to unlock the data in the secure element. The strength of the pin chosen by the customer will be one factor in determining the strength of the mobile payment application protections. Secure elements built into the SIM or device benefit from additional protections provided by the mobile device OS which prohibits applications to access the secure element.

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Once unlocked, the secure element is vulnerable to unauthorized access. Mobile payment applications provide mitigation for this vulnerability by implementing inactivity timeouts to automatically re-lock the secure element. Conceptual methods have been proposed whereby an attacker could trick a device into keeping the NFC and secure element active after a transaction, and thus unlocked. Such an attacker would still need to gain physical possession of the device in order to complete a fraudulent transaction.

A possible drawback to the mobile wallet and secure element solution is that a single pin unlocks all of the accounts stored in the wallet. This is in contrast to plastic cards, where each card can be set to use a different pin. Mobile wallets could thus present greater exposure to loss in the event that a mobile wallet device and its single pin are compromised

A key process for mobile payments is the ability to securely provision, de-provision, and re-provision secure elements. You must maintain security during each of these processes as each presents a possible opportunity for attackers to intercept sensitive account information.

5. Risk Mitigation

There are various measures that can be taken to address the security challenges of mobile banking and payments. As a summary, the table below lists the major risks and the suggested mitigation.

Risk	Suggested Mitigation	Comments
Mobile more susceptible for loss or theft	• Customer Education • Implementation of remote wipe, passcode and automatic lock out	
Users more likely to store personal and sensitive information on mobile device	• Customer education • Device encryption • Ensure applications don't store customer sensitive data locally	
Malware	• Mobile malware protection • Don't jailbreak your device	Products in this space lack maturity
Malicious	• Customer education	

Vanessa Pegueros, vpegueros@gmail.com

© 2012 The SANS Institute Author retains full rights.

Applications	• Use only reputable sites to download apps • Ensure that apps are tested for security	
Privacy Violations	• Customer education • Security testing of applications and data handling	
Wireless carrier infrastructure	• Vet the security of the carrier infrastructure and services through targeted questions	A complex infrastructure that leaves the consumer with little control over the risks. Enterprise customers have a greater opportunity to vet the security.
Payment systems infrastructure	• Ensure the point of sale device vulnerabilities are addressed • Utilize EMV where possible	A complex infrastructure that leaves the consumer with little control over the risks. Enterprise customers have a greater opportunity to vet the security.
SMS vulnerabilities	• SMS should not be used as a channel for money movement and other high risk transactions	
Hardware and OS Vulnerabilities	• Ensure that software updates are being pushed to devices	Hardware and OS vulnerabilities are difficult for anyone but the manufacturer and OS provider to address
Complex Supply Chain and New Entrants in the Mobile ecosystem	• Implement a 3rd party vendor security program	
Lack of Maturity in Fraud tools and controls	• Extend current online fraud tools and controls are extended to the mobile channel • Secure provisioning/de-provisioning	

Vanessa Pegueros, vpegueros@gmail.com

© 2012 The SANS Institute Author retains full rights.

Several of these risks have common mitigation suggestions and it is important to discuss several of these mitigation controls in more depth.

5.1. Customer Education

One of the less technical areas of risk mitigation includes an effort around strong customer education. There should be an established and well understood method of communication with customers. Customers should understand that any deviations from this established communication channel cannot be trusted. This will reduce the risks of customers falling victim to attacks such as phishing. Customers should also have an established way to communicate relative to suspected fraud and understand how their banking company will communicate to them.

There should be a basic customer education program relative to security including addressing issues such as the importance of passwords, the structure of strong passwords, ensuring that their device locks after a designated period of time, importance of updating their operating system and the installed applications, the dangers of a "jail broken" device, and implementing encryption and anti-virus whenever possible. Additionally, if remote wipe is implemented by their carrier, the customer should be encouraged to implement the ability to remotely wipe their device in the event that it is lost or stolen.

Finally, customers should be educated on the importance of downloading from reputable sites as well as understanding the behavior of the application in terms of what data is gathered and shared with potentially other services or applications.

5.2. Device and Application

Major app providers are taking action to control the integrity of their applications. Earlier this year, Google announced that it would implement an automated scanning process designed to keep malicious applications out of the Android market. The service called "Bouncer" scans for spyware and Trojans and looks for suspicious behaviors. Apple puts strict controls on its app store, requiring all developers to register and authenticate. (Mills, 2012)

Vanessa Pegueros, vpegueros@gmail.com

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Relative to the development of a mobile applications there are some key recommendations should be followed. Clear text credentials and any customer confidential data should not be stored on the device. Customer confidential information should be masked, truncated, redacted or otherwise rendered incomplete. Communication by the mobile banking app through the internet should employ secure transmission protocols such as HTTPS. Additionally, customer data exchanged with 3rd party vendors should be encrypted (in transmission and storage) or rendered incomplete. Additionally, applications should time out after 15 min of inactivity; pins required in the mobile application should not be less than 6 characters and should lock after 10 incorrect entries.

Combating mobile malware is best addressed through following some key guidelines. The first relates to not jail breaking your device and if you are an Enterprise, don't allow jail broken devices on your network. Second, only download applications from trusted application sites. Again if you are an Enterprise do not allow users to download from unapproved sites. Finally, ensure that users are doing OS updates and application developers are sandboxing the applications. Sandboxing prevents the application from interacting with other applications on the device as well as limiting the applications interaction with the OS to the necessary interfaces. Implementation of software such as antivirus on mobile devices is still relatively immature and the bandwidth and battery life consumed by these types of software may be prohibitive from the customer perspective.

An emerging area to assist in the challenges with mobile applications security is hardware based virtualization. According to Basso (2011), "By the end of 2012, 90% of smartphones will ship with ARMs Trustzone's virtualization capabilities." (p.3) Trustzone is a standard component of ARM's system on a chip (SoC) architecture. The partitioning supported by hardware virtualization can be used to isolate sensitive data and instructions inside personal devices, providing a more trustable platform for corporate applications, mobile payments or other m-commerce capabilities provided the application supports it. TrustZone can also be used by the smartphone OS to support device security or provide secure services that can be used by multiple applications. As stated by Basso (2011), " TrustZone uses hardware to partition the microprocessor and SoC into "trusted" and "untrusted" execution paths. All instructions and data are "flagged" to determine

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

which path they follow. The flag acts as a hardware switch between the domains, which ARM calls "trusted" and "normal." A software monitor intercepts microprocessor transactions and accesses to/from system resources (such as peripherals) to determine the domain to which they belong. Effective isolation of the trusted domain is critical. The smartphone's user OS runs entirely in the normal domain. The trusted domain runs a separate, thin and secure kernel, where trusted applications can be installed." (p. 4-5) In addition to these device mitigation measures, there are emerging solutions in the payments space to address the security of mobile banking.

5.3. EMV

The Europay, MasterCard and Visa (EMV) also known as chip and pin has been in operation within Europe since 2004 as a payment standard and since it was introduced in the UK, face to face card fraud has decreased 69%. In August 2011, Visa announced a program to encourage the adoption of EMV technology with merchants by October 2015. (Litan, 2011) Part of the program would require that terminals must be enabled to support contact and contactless payments including mobile contactless payment based on Near Field Communications (NFC) Technology. EMV has been widely adopted within Europe and Asia and has yet to be adopted in the U.S. EMV has many advantages in increasing security and reducing fraud. EMV can be employed as either online or offline authorization. Online authorization is verified immediately via online with the card issuer. Offline authorization (also called chip and pin) requires a pin to unlock the card.

With traditional credit cards (magstripes) static data authentication is utilized. With static data authentication, there are two cryptographic key pairs an issuer pair and a certificate authority pair. The terminal uses the CA public key to get the Issuer public key. The terminal then uses the issuer's public key to calculate a hash value with the static data (account no, expiration date, etc...). The terminal conducts the same hash exercise with the card presented and if the hashes are equal, the card is accepted as valid.

EMV utilizes dynamic data authentication where there are three cryptographic key pairs: issuer, CA and card. The terminal uses the issuer's public key to obtain the card public key. The terminal then sends a random number to the card. The card encrypts the random number with the card's private key and sends it to the terminal. The

© 2012 The SANS Institute Author retains full rights.

terminal decrypts the number with the cards public key to get the random number. If the random numbers match, the card is accepted as valid.

EMV addresses three key areas beyond magstripe:

- counterfeit cards
- skimming
- off line interceptions, man in the middle attacks are prevented since each transaction contains unique, encrypted data

EMV can be employed with NFC and will provide the same benefits and protections for contactless payments.

5.4. Vendor Management

For many companies they must rely on a 3rd party vendor to assist them in the development of a mobile payment application as they do not possess the core competencies to do so themselves. Many of these 3rd party vendors are new entrants into the mobile banking and payments ecosystem and may not prioritize security and compliance in their product offerings. There must therefore be renewed diligence relative to ensuring the security and compliance of these new suppliers and vendors. Mobile banking and payment applications developed by 3rd parties should be fully pen-tested prior to implementation and should be re- tested with each new release. There should be full understanding of how customer data is transmitted and stored by the application as well as locally by the vendor.

5.5. Fraud Management

In order to manage fraud, mobile banking companies should implement strong fraud prevention and detection services. This fraud service should include customer education, strong authentication, secure mobile applications, strict account set up and management processes, real time detective services, and 24x7 customer support.

Customers should be educated on their options to prevent fraud and what to do if they suspect fraud. Customers should be able to opt into strict process rules include limiting transaction value, requiring dual approvers on high risk transactions, and not

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

allowing changes to customer sensitive data such as address or authorized transfer to individuals without strong restrictions. Dual approver is a process that requires one person to initiate the transaction and a second approver on a different device to authorize the transaction. Customers should be encouraged to enroll in predefined alerts that will help in the area of fraud prevention. Other key data points used in fraud prevention include IP reputation, endpoint identity, geo-location, user history and behavior. Additionally, the service should provide controls based on the transactional risk score such as step up authentication where the customer is prompted for additional information as the transaction initiated is more risky.

Strong authentication is critical in the mobile space since devices are easily lost and stolen. The most mature and widely deployed method is knowledge based authentication which includes passwords, question and answer (Q&A), and image recognition. Another form of authentication can come from establishing a device identity. There are many methods by which this can be accomplished but the essential element is to authenticate to an ID from that specific device that is derived from attributes (HW and SW) of that device. While authentication through biometrics is not new, it is still challenged with issues related to false positives. With advanced mobile device hardware such as cameras and voice recognition, there will be increased use of biometric authentication in the use of mobile banking.

The mobile device offers another benefit in online banking. The customer's mobile device can be used as an out of band (OOB) authenticator or a one-time password (OTP) generator. In the case of OTP, the mobile device produces a software token that can then be utilized to authenticate in the online banking app. The OTP application on the device effectively turns the mobile device into a token without having to deploy and manage traditional hardware based tokens. OOB is defined as an alternative technical channel to the prime device being utilized. For example, an IVR (Interactive Voice Response) or mobile device is considered OOB of the HTTPS session on your computer. Use of OOB to prevent fraud is called transaction verification and can be implemented to authenticate and/or verify transactions. In the case of mobile, SMS can be utilized to authenticate attempted transactions relative to the online banking account. The SMS

© 2012 The SANS Institute Author retains full rights.

messages can be triggered based on the risk of the specific transaction and can prompt the account owner to validate and approve in process transactions.

With users migrating away from traditional branches and even the online space, the mobile device will at some point be the prime channel for banking and payments. This presents a challenge as now there is only one device and the benefits of OOB become more difficult. Some fraud companies are approaching the OOB issue in a slightly different manner, the virtual OOB approach. With the virtual OOB approach, another totally separate application on the device acts as an OOB channel. One could argue that this is not a true OOB approach, however, may be a key direction as users move to one device for all key interactions.

6. Conclusion

The mobile banking and payments ecosystem is complex and dynamic. It is not clear who will emerge as the winner(s) in the growing space from a financial services, application provider or technology perspective. Security and the perception of security will clearly play a role in who ends up dominating.

Traditional financial service companies (banks, processors, and card associations) clearly have an advantage from controlling the existing banking and payments infrastructure. The extent to which they can strategically extend their products and services in a way that maintains the customer's trust in their services be key to their success. A foundational element of that trust is the security of the products and services.

The wireless carriers are challenged by entering a segment with little financial service experience. Wireless carriers are challenged by being perceived as simply a wireless bandwidth pipe and have struggled with this since the advent of wireless data.

Application providers (Google, Apple) within this space clearly hold an edge relative to innovation and speed to market, however, lack of focus on security and privacy will inhibit progress. Additionally, both wireless carriers and application

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

providers are at a clear disadvantage in terms of understanding the regulatory environment faced by current financial service providers.

7.0 References

Allan, Ant. "Q&A: Phone-Based Authentication Methods", Gartner, June 24, 2010

Basso, Monica and Gammage, Brian. "Smartpone Virtualization: Making Mobile Applications More Trustable", Gartner, April 21, 2011

Chen, Brian X and Bilton, Nick. "Et Tu, Google? Android Apps Can Also Secretly Copy Photos", March 1, 2012, http://bits.blogs.nytimes.com/2012/03/01/android-photos/

Danchev, Dancho. "Fake Gmail Android application steals personal data", June 6, 2012, http://www.zdnet.com/blog/security/fake-gmail-android-application-steals-personal-data/12308

Eigdon, Emmett. "US Mobile Banking Forecast", Forrester, January 31, 2011

Essers, Loek. "Untethered jailbreak for iOS 5.1.1 available for download", May 25th, 2012, http://www.computerworld.com/s/article/9227495/Untethered_jailbreak_for_iOS_5.1.1_available_for_download

Fonte, Erin F. "Mobile Banking/Mobile Payments 2011: Hot Topics for Financial Institutions, Vendors and Third-Party Payment Providers", Cox Smith Matthews Incorporated, December 15, 2011

Golvin, Charles S. and Husson, Thomas. "Google Wallet Is Not About Mobile Payments", Forrester, May 27, 2011

Hesse, Alexander. "The Time is Right to Start Experimenting with Mobile Banking for Marketing and Sales", Forrester, April 5, 2011

Hung, Mark and Litan, Avivah. "Google Wallet Kicks Off First Phase of Smartphone NFC Adoption", Gartner, June 1, 2011

Vanessa Pegueros, vpegueros@gmail.com

© 2012 SANS Institute, Author retains full rights.

Husson, Thomas. "Mobile Payments Enter a Disruptive Phase", Forrester, March 31, 2011

Jackson, William. "Mobile malware is on the march, and Android is target No. 1", February 16, 2012, http://gcn.com/Articles/2012/02/16/Mobile-malware-Android-top-target.aspx?Page=1

Kleynhans, Stephen and Silver, Michael A. "New World of Emerging Devices and Usage Paradigms Influences Features of Microsoft's Windows 8", Gartner, April 4, 2012

Kovacs, Eduard. "Amateur Programmer: SMS Spoofing for Malicious Purposes Is Easy", January 25th, 2012, http://news.softpedia.com/news/Amateur-Programmer-SMS-Spoofing-for-Malicious-Purposes-Is-Easy-248669.shtml

Litan, Avivah. "Best Practices in Mobile User Authentication and Layered Fraud Prevention", Gartner, August 11, 2011

Litan, Avivah. "Visa's Long-Overdue US EMV Move Will Improve Security, but Do little to Alleviate PCI Compliance Work", Gartner, September 13, 2011

Mills, Elinor. "Google now scanning Android apps for malware", February 2, 2012, http://news.cnet.com/8301-1009_3-57370650-83/google-now-scanning-android-apps-for-malware/

Morgan, Gareth. "Mobile malware rises by 155 per cent as Android platform risks grow", February 16, 2012, http://www.v3.co.uk/v3-uk/news/2153026/mobile-malware-rises-155-cent-android-platform-risks-grow

Niemi, Valtteri and Nyberg, Kaisa. "UMTS Security", John Wiley & Sons, England, 2003

Pitts, James D. "Surfing the Payment Channels, Mastering the Fraud Tsunami", JDP Enterprises, Carrollton, TX, 2010

Schwartz, Matthew J. "New Android Malware Has Costly Twist", February 6, 2012, http://www.informationweek.com/news/security/mobile/232600313

Shen, Sandy. "Visa's Fundamo Acquisition Marks the Financial Inclusion of Mobile Money Services" Gartner, July 5, 2011

Vanessa Pegueros, vpegueros@gmail.com

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Silver, Michael A., Kleynhans, Stephen, Smith, David Mitchell. "Windows 8 Announcement Should Not Delay Windows 7 Deployment Plans", Gartner, June 8, 2011

Strickland, Jonathan, "How the Google Phone Works", http://electronics.howstuffworks.com/google-phone.htm

Wannemacher, Peter. "Case Study: Discover Financial Services Partners with Paypal to Roll Out Mobile P2P Payments", Forrester, November 2, 2011

Wannemacher, Peter. "2012 US Mobile Banking Functionality Rankings", Forrester, April 26, 2012

Worth, Dan. "Top Android apps accused of passing personal data to advertisers", March 5, 2012, http://www.v3.co.uk/v3-uk/news/2157040/android-apps-accused-passing-personal-advertisers

"8th Annual Card Issuers' Safety Scorecard: Proliferation of Alerts Lead to Quicker Detection Time and Lower Fraud Costs" Javelin Strategy & Research, June 2012

"Consumer and Mobile Financial Services", Board of Governors of the Federal Reserve System, March 2012

"Credit Card 101", Shift 4 Secure Payment Processing, www.shift4.com

"EMV Essentials for the US Merchant", a Mercator Advisory Group Brief Sponsored by Heartland Payment Systems, January 2012

"iOS Security", Apple Inc., May 2012

"Malware disguised as new Instagram Android app", April 18, 2012, http://www.net-security.org/malware_news.php?id=2076&utm

"Mobile device security, Understanding vulnerabilities and managing risks" Ernest and Young, Insights on IT risk Technical briefing, January 2012

"Mobile malware increased six-fold in 2011", March 1, 2012, http://mybroadband.co.za/news/security/44689-mobile-device-malware-increased-six-fold-in-2011.html

"Mobile Payments, Delivering Compelling Customer and Shareholder Value through a Complete, Coherent Approach", A White paper by Microsoft and M-Com

"Recommendations for the Security of Internet Payments", European Central Bank, April 2012

Vanessa Pegueros, vpegueros@gmail.com

© 2012 SANS Institute, Author retains full rights.

"US Mobile Payments: The time has come", Aite Group, Nov. 2010

"Worldwide Smartphone Market Continues to Soar, Carrying Samsung Into the Top Position in Total Mobile Phone and Smartphone Shipments", IDC Press Release, May 1, 2012, http://www.idc.com/getdoc.jsp?containerId=prUS23455612

© 2012 SANS Institute, Author retains full rights.

Vanessa Pegueros, vpegueros@gmail.com

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced