An Examination of Information Security in Mobile Banking Architectures

Dr. Kevin Streff
Kevin.streff@dsu.edu
Dakota State University

Justin Haar
jjhaar@pluto.dsu.edu
Dakota State University

ABSTRACT

This paper is an examination of mobile banking architectures and the security issues that relate to those architectures and mobile banking systems. The paper reviews and defines mobile banking and looks at reasons why banks are going mobile. We then explore the three architectures deployed in mobile banking applications. Lastly we examine the security threats that exist, and what can be done to mitigate these security threats.

Keywords: Mobile Banking, Information Assurance, m-Commerce, Mobile Commerce, Confidentiality, Networks and Security

1. INTRODUCTION

Mobile banking has been emerging since the late 1990's. However, phones contained limited memory, processing power, and display capabilities. Network speeds were low and data costs were high. These issues have resulted in consumer concerns and low mobile banking adoption rates. Technology has evolved so mobile banking services are possible through more robust hardware and faster networks. The phones have improved with larger, color screens and improved processing and memory abilities. Device cost is dropping as a mobile device that has the same processing power of computers from the late 90's is only a couple hundred dollars. (Riivari, 2005) Eighty percent of the consumers in the US own a mobile device.

In 2007, US banks began offering mobile banking (Holland, 2008) Bank of America reported 500,000 users in the first six months of offering their service. ("Bank of America Touts Mobile Banking Service's Growth", 2007) According to the Aite group, predicted mobile banking usage in the first year was 1.6 million users, indicating that the potential for mobile banking is great.

However, the security community must closely examine mobile banking because as these systems become more popular it will fall to us to defend the sensitive customer and financial information stored, processed and/or transacted in these systems. This paper has three goals. First, gain a greater understanding of what mobile banking really is and the potential that it promises. Second, define the different system architectures that can be used by banks to deploy mobile banking systems. Finally, identify and clarify some of the security threats related to these systems and how those threats apply to the different system architectures.

2. MOBILE BANKING AND MOBILE FINANCIAL SERVICES

Recent advances in mobile technology have expanded the service offerings of a mobile device. A mobile application is a program is downloaded onto a mobile device or accessed by a device through the internet. These applications take many forms such as mobile shopping systems that allow users to browse and buy products, mobile entertainment systems like mobile games that provide users with access to games from their phones, and of course mobile banking.

Mobile banking systems are applications that allow users to complete banking transactions on a mobile device. Mobile banking can be broken into three divisions: mobile accounting, mobile brokerage, and mobile financial information. Mobile accounting services are the services that are required to administer and operate the account and can be divided into two areas: account operations and account administration. Account operations are features like funds transfers and bill payments. Account administration has features like blocking lost cards, changing active accounts, and ordering checks. Mobile brokerage services are the services that are required to best utilize an investment account, including the ability to buy and sell securities and obtain accurate and up to date information about securities. Mobile financial services can be subdivided into two areas: account information and market information. Account information includes balance inquires, statement requests, alerts, branch and ATM locators, and credit card information. Marketing information provides information like exchange rates, interest rates, products and services, and stock quotes. (Rajnish & Stephan, 2007)

3. WHY ARE BANKS GOING MOBILE?

The banking industry is intensely regulated and highly competitive, as there are only so many products that banks can offer. A differentiator can be how bank products are accessed, which is where mobile banking is gaining momentum to recruit and retain customers.

Riivari outlines five reasons banks elect mobile banking his 2005 article:

- Improve customer Service
- Reduce costs
- Increase the reactivity of the company
- Increase market share
- Improve branding

The Gen Y market is most likely to use these systems because this market has already integrated mobile technology into their lives. Dexia Bank in Belgium has rolled out a marketing campaign using mobile banking to target the youth market in that country. (Riivari, 2005) In the US, Fuse, a research and marketing company, focuses on marketing to Gen Y. They point out that in the US, Gen Y represents 1/3rd of the US population and is a 170 billion dollar market. Gen Y selectively consumes products and services. They only download the songs they want to hear instead of buying the whole album. (Bielski, 2007)

Mobile banking allows banks to sell products in situations where they were unable to before. A customer making a large purchase requiring financing can leave banks out of the picture, especially on weekends and evenings when branches are closed. Mobile banking can fill this void with applications that are available on cell phones. It is possible that in coming years, credit card companies could adopt these systems to replace plastic cards. Mobile devices could be used to replace a cash-based financial system with a cashless one. (Hu, Li, & Hu, 2008)

4. MOBILE BANKING IN THE U.S.

Several banks outside of the US have offered mobile banking for years and provide great examples for US companies. US mobile banking has been slow to catch on. Bob Egan, an analyst for Tower Group, reports that even last spring the concept of mobile banking was really a novelty here in the US. Consumers have been slow to sign up. Consumers demand systems that protect their money and non-public information. (Hamblen, 2007)

Bank of America launched their system in March of 2007 with over 500,000 active users after the first six months. ("Bank of America Touts Mobile Banking Service's Growth", 2007) This system can transfer

funds, send bill payments, locate branches and ATM's, view account balances, and is supported by four of the six major wireless carriers in the US. Wachovia has developed their own mobile banking product with AT&T, launching in September 2006 and re-launching in March 2007. (Hamblen, 2007)

Banks and carriers are partnering to build US mobile banking systems. North America boasts over 18,000 banks and only six mobile carriers, while Europe has only 7,000 banks and 147 carriers. (Hamblen, 2007) Banks in the US have the advantage of working with a number of different application development companies. Wells Fargo, Bank of America, and Citicards work with CellTrust. Citibank offers "mobile wallets" to customers. ("CellTrust 2-Way SMS Gateway") CellTrust isn't alone ClairMail (ClairMail.com), Firethorn (Hamblen, 2007), mFoundry ("The Mobile Platform for Financial Services. Additionally, 240 million cellular subscribers in the US represents a huge market potential for banks to tap into. (Hamblen, 2007) In 2007 an estimated 2.7 billion mobile banking transactions were completed. That number is expected to reach as many as 37 billion by 2011.

5. MOBILE DEVICES AND TECHNOLOGY

Mobile device are revolutionizing communication and the smartphone is leading the way. A smartphone is a phone, contact list, calendar, tasks list, organizer, PDA, email, spreadsheet, word processor, and instant messenger. The BlackBerry is a prominent smartphone. (Lin, 2007) To understand how these devices enable mobile commerce, we examine the technology they use, including mobile communications technology, devices and operating systems.

6. MOBILE NETWORK TECHNOLOGY

Global System for Mobile Communications (GSM) and Code Division Multiplex Access (CDMA) are two prominent technologies. GSM had some nicer features at first with improved roaming and fraud detection. CDMA has caught up and now both GSM and CDMA offer video, multimedia services, and high-speed internet access at comparable rates. GSM is a currently deployed in over 200 countries and is the standard in Europe and Asia. In 2006 GSM phones represented 73% of the total world market. GSM is second in market share in the United States to CDMA representing only 38% of the market. Cingular (AT&T) and T-Mobile both offer GSM service in the US. CDMA is the market leader in the US; however it is not widely utilized elsewhere. CDMA is the standard used by Verizon and Sprint. CDMA represented about 50% of the US market in 2006 but only 14% of the world market at that time. (Lin, 2007)

3G mobile technology has intensified the competition between CDMA and GSM in the US. All US providers upgraded their networks to support the 3G technologies. CDMA providers are now using the Evolution Data Only technology (EV-DO). GSM providers like Cingular and T-Mobile have gone in different direction with their 3G networks. Cingular first invested in EDGE or Enhanced Data Rates for Global Evolution technology. The finally decided instead to invest in the wideband CDMA technology. T-Mobile went with Universal Mobile Telephone Service technology. (Lin, 2007)

7. DEVICE OPERATING SYSTEMS

Mobile devices are computers like the desktops or laptops. Similarly, mobile devices have an operating system (OS) that instructs the device what to do. There are five operating systems used by mobile devices in today's market. (Malykhina, 2007) Each is overviewed next.

Symbain dominates the smartphone market as 73% of devices use this OS in 3rd quarter 2006 and is used in Nokia and Sony Ericsson phones. Symbain is less popular in the US where Cingular is the only carrier that supports it, representing 10% of devices in the US. Symbain is designed using C++ to allow developers to design applications of their own. Symbain licenses can be bought by any manufacturer and an application programming interface (API) is available. (Application programming interface) While Symbain dominates the world market the US market is ruled by RIM**,** the creator of Blackberry OS. Blackberry is Java based and currently supports over 1,500 business applications and a myriad of personal applications. A unique feature of this OS is its ability to distinguish trusted and un-trusted applications and, using that

distinction, limit access to resources. The Blackberry OS is also relatively secure, allowing for end-to-end encryption from device to a Blackberry Server. The biggest issue with RIM's Blackberry is licensing and only a limited number of non-Blackberry devices can support Blackberry features. Microsoft offers Windows Mobile for smartphones, which allow for better use of email, calendar, and voice notes. Microsoft offers support for Windows mobile with their other software like Windows Vista. Some users have noted that Windows Mobile devices have memory problems and are prone to lockups and require frequent resets. Linux is involved in mobile products as well. The Japanese company Access, who now owns PalmSource, offers a version of mobile Linux called Access Linux platform. Access Linux is able to run applications designed to work on Palm OS, which, given that there are 29,000 palm applications, is a useful feature and will aid in the adoption of mobile Linux. There are a large number of developers who already write software specifically for Linux but there are also a large number of different Linux versions and software written for one often doesn't work well on another. Apple's Mac OS X has come to the mobile world in the form of the iPhone. The iPhone is limited to Cingular's network and Apple and Cingular will strictly control what software can be used on the iPhone. The touch-screen differentiates the iPhone. (Malykhina, 2007)

8. MODELS OF MOBILE BANKING ARCHITECTURE

Mobile phones have three architecture alternatives when interactive with banks' mobile banking systems. Each is further described.

MESSAGE BASED SERVICES MODEL

Message based systems work through text messaging. There are two situations in which a message is sent. A customer may send a message to the bank containing a request and the bank will respond back with information, such as the balance of accounts. Second, customers can set up situational criterion on an account that will send them a message when a certain situation occurs such as falling below a certain balance. (Rajnish & Stephan, 2007)

There are two types of message systems: SMS and MMS. SMS or short message services includes sending text messages to a bank which receive and interpret the commands sent in the message. The bank returns a text message with the information requested. The issue with SMS messages is that they have limited size, able to include only a handful of characters in a message. MMS is a new type of message service that works in the same basic way as SMS, but can carry larger payloads. Currently, only one bank is utilizing MMS services: Banca Intesa of Italy. (Rajnish & Stephan, 2007) Wells Fargo uses a message based system. To establish this service a customer enrolls a phone in mobile banking services, and Wells Fargo will send a text message with a one-time password. The customer confirms the password online and is ready to go. For added security, the account nicknames are identified, and communication refers to these nicknames and not their account numbers, alleviating the fear of account compromise due to intercepting the message. To use the service, customers text message Wells Fargo at 93557 containing a request. Each bank has their own number. Commands like bal, bal all, or bal <account nickname> return the balance of either the primary account, all the accounts, or a particular account based on its nickname. ("Wells Fargo Mobile Banking")

Message based systems have a number of advantages. First, these systems are widely available and supported by most carriers and phones. No confidential information is transmitted to the user or stored on the user's device. Either the customer or bank can initiate communications. ("ClairMail Security") However, the simplicity of this system also limits it, as SMS messages can't carry large payloads so the information that is provided on an account needs to be limited for risk of overwhelming the user's device. Typically these messages are limited to 140 characters. ("CellTrust 2-Way SMS Gateway") There is also the concern that most SMS systems do not guarantee delivery of the message. Though CellTrust has developed a system to overcome this issue by using special micro-clients that provide encryption and that can show if a user has received a message. ("CellTrust 2-Way SMS Gateway")

MOBILE BROWSERS MODEL

Mobile browsers model is the ability to access the bank's internet banking website from a cell phone. If a user has an IP enabled phones, they can connect to the internet via their carrier's internet services or a wireless hotspot. The major advantage of this approach is it all the processing is done on a remote server and minimal information is stored on the device. Another advantage is that there is no need to install special software since phones capable of using this technology come with the software installed. (Rajnish & Stephan, 2007)

Given the limited power, memory, screen size and processing ability of phones, application designers use a special web based programming language like Wireless Access Protocol (WAP) to write pages for mobile devices. WAP was first created in 1998 and was created as an industry standard for wireless applications. Many US banks prefer this method because they are familiar with it. Customers find it easy to interact with these systems because of that same familiarity. (Hamblen, 2007) Further, limited set-up is required to access these systems as customers visit the banks mobile website and enter user name and password to access mobile services. ("Wachovia Mobile") ("Wells Fargo Mobile Banking") ("Bank of America Mobile Banking Frequently Asked Questions"). These mobile banking sites are just like the banks online banking systems, so customers are familiar with the layout and design.

Some advantages of the mobile browsers model include ease of use and user familiarity. Users also don't have to download any special software. Additionally since everything is stored on the banks servers it's easy to update. One significant disadvantage is that these services are not offered everywhere and do not work on all handsets. Data costs are also high for the end user with these systems. This is also a risk of confidential information being at risk as these systems are more susceptible to attack. Mobile devices aren't capable of running firewalls or other forms of protection and so these sessions are susceptible to attack. ("ClairMail Security")

CLIENT APPLICATION MODEL

The client side application architecture requires the user to download the mobile banking software onto their phone. These Java-based systems can be very nice from a customer interaction standpoint, as a bank can offer simple, easy to use applications to provide a variety of services. (Riivari, 2005) The real advantage to these applications is that they can be run remotely and only need to connect to the banks systems long enough to get information and execute a transaction thereby lowering the normally high data costs that may be associated with web based applications. (Rajnish & Stephan, 2007)

To setup a client based application a customer enrolls in a mobile banking service with their bank and downloads a mobile banking application to their phone. Mobile phones have limited disk size, memory, and processing ability so this approach is problematic for older phones. To use a client application, the customer selects visual commands or clicks certain links and the application sends a message to the bank and displays the results for the user. These systems can offer a range of services like funds transfer and bill pay payments as well as account details and activity. (Rajnish & Stephan, 2007)

9. SECURITY THREATS AND CONCERNS

In *A Mobile Security Battle. Security* Jain (2006) makes a salient point: "The vulnerability of mobile computing and communications is a big but sometimes hidden enterprise security threat. Mobile handhelds are compact, portable and easily lost or stolen, and hence, put sensitive information at risk. The proliferation of insecure WLAN networks pose a further threat to corporate security." In order to keep a mobile banking system secure, Tang, Terziyan, and Veijalainen outline five security requirements:

- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Authorization

Confidentiality ensures that non-public information remains private. Confidentiality

through mobile devices is challenging because these systems depend on wireless communications and generally use the Internet. Authentication is the process of identifying a user to be who they claim to be. This usually takes the form of a credential (e.g., username and password). Integrity ensures that data is not tampered with on its path to its destination. This is concerned with preventing man-in-the-middle attacks or other active session hijacking attacks. Non-repudiation ensures transactions are legally binding. This is critical for electronic banking systems because it prevents complication from regulation violation. Authorization ensures transactions are endorsed and authorized by all parties involved. This comes into play with inter and intra bank funds transfers. (Tang, Terziyan, & Veijalainen, 2008)

In the next section we will look at a number of security topics as they relate to these requirements and to the mobile banking platforms we discussed in the last section. This overview will allow us to identify areas of risk and some possible solutions

AUTHENTICATION

FFIEC requires banks to use multiple forms of authentication for electronic banking. All mobile banking systems need to use at least two separate forms of authentication to identify the customer. ("Authentication in an Internet Banking Environment") There are three forms of identification: what you have, what you know, and what you are. What you know includes items like usernames, passwords or pin numbers. What you have examples include a debit card, a smart card, or your mobile device. Who you are requires biometrics (Clarke, 2005)

Current authentication methods available include a PIN number for the phones and a PIN number, one-time password or pin number, or a username or password for the banking systems. PIN numbers, usernames and passwords depend on what the user knows, and the literature includes well-documented flaws of this model, such as users using weak, guessable, passwords, users writing them down, leaving them where they are found, or sharing them. A survey conducted by Clarke and Furnell (2005) found that 66% of those surveyed used a PIN on device startup, but 30% thought PINs were inconvenient. Additionally 38% had their mobile devices unlocked by their service provider because they had locked themselves out. One solution has been proposed to help protect mobile devices by increasing the security of the PIN itself. When PIN protection is enabled on a mobile device that device only stores a portion of the PIN. The other portion of the PIN is stored on a server. This distributes the PIN in such a way that even if an attacker has direct access to the phone they can only get half the PIN from the phones' memory. Mobile banking systems currently utilize this concept in part. The bank provides the PIN and authenticates it through the phone. 3G network technology will help bring about changes and the increased functionality of mobile devices make it possible to use additional and more advanced authentication methods. (Clarke, 2005)

The system currently used by Wells Fargo for SMS messages currently relies on the phone number are the primary means of authentication. ("Wells Fargo Mobile Banking") The phone itself is perhaps not the greatest authentication tool we could use. It has some advantages like the fact that the user must have the phone to utilize these services and only this one phone can use these services. The problem becomes the bank can't tell if it's a real customer not.

Another form of authentication is "What the user is". Essentially this is the use of biometrics. In a 2005 survey, Clarke and Furnell found that 83% were in favor of using some type of biometric system to protect their phones, including one of the five listed below:

- Facial Recognition
- Keystroke Analysis
- Handwriting Recognition
- Speaker/Voice Recognition
- Service Utilization

A biometric authentication method that deserves note is service utilization, where

users are granted or denied access based on their previous behavior and utilization of certain systems. Behavioral analysis looks for patterns of how users do certain things. For example, if a user has to transfer funds, there are several different ways a user can access the transfer portion of the application. Different users may use different ways to access that portion of the system. The way this can be utilized for authentication is if they suddenly do things a different way, it raises a red flag. (Mazhelis, 2007) The technology to fully utilize service utilization is only partially in place; however, service utilization holds promise in the near future.

Another authentication technique is out-of-band communication, which allows the bank to identify the customer through a communication channel other than the one being used. (Feig, 2007) Bank of America utilizes this method with their mobile banking system. Customer gain access to the system by visiting www.ba.mobi and entering their username/password. Bank of America then sends the customer a pin number as a text message, which is then entered to gain access to the system. ("Bank of America Mobile Banking Frequently Asked Questions")

A robust authentication system utilizes multiple forms of identity at application startup and during application use. While using an application, the system may test behavior or compare keystrokes to patterns which are on file. If an anomaly is detected, the system could prompt for a more intrusive but more accurate form of identification. If the user fails again, an IVR system could call and use voiceprint analysis along with a PIN. Eventually, if the user fails enough they are locked out. This approach promotes increased security as it is difficult for an attacker to keep getting the right answers. (Clarke, 2005)

There are a number of possibilities for authentication across mobile banking architectures. SMS systems utilize tokens and could also utilize tokens in the form of smart card in order to take authentication off one device and provide different options for the user to move around. SMS systems can also utilize PINs by having the user send a PIN or by utilizing an IVR system to call the user to verify the PIN. These systems can also benefit from the use of 1 time PINs at system startup and when questionable activity is detected. Mobile web systems mainly utilize user names and passwords; however, some mobile web services also use out-of-band authentication because they utilize 1 time passwords sent in the form of an SMS message which must be entered into the webpage to log in. This feature promotes good security because an attacker can't just try to log into the site as they also need access to the phone to get the password. Client side applications benefit from their ability to be highly customizable, often utilize usernames and passwords, PIN numbers, or out-of-band authentication.

Denial of Service

Denial-of-service (DOS) is the process of preventing access to a device or system by overwhelming it with phony communication, therefore rendering it unable to accept legitimate transactions. DOS attacks are prominent in wired networks and are making their way into wireless/mobile solutions. It is possible to use several mobile devices to send a stream of SMS messages to another mobile device. This type of attack is called a SMS flood and sends thousands of messages anonymously in seconds. (Jain, 2006) ClairMail (2007) states that a limiting factor in launching a DOS against a mobile banking platform is the cost of attack. Carriers charge to both send and receive information. It's possible that the next slammer will utilize SMS messages and could cripple a company if it is not detected. The mobile web and client application architectures are vulnerable to a traditional DOS attack. For example an attacker could use a DOS to knock a user's phone offline with an SMS storm then try to connect to their banks mobile website while the victim's phone is disabled and incapable of receiving any alerts or messages from the bank.

Mobile banking systems are vulnerable to both existing types of DOS attacks and those that can be launched though new delivery channels like a SMS messages. If an attacker were to launch a sustained DOS against a banks mobile website for example it would be very costly to the bank both financially and could have a negative effect on their customer relationship. An attack

such on the banks SMS system could limit customer accessibility by both SMS users and java based applications and could have a more damaging financial affect because the bank may be charged for receiving the messages.

LOST AND STOLEN PHONE

Cell phones are small and portable; however, the disadvantage is that they are easily lost or stolen. When considering the threats of lost or stolen devices there are three different areas of note: authentication, authorization, and confidentiality. The threat of this is real with 1.3 million devices being lost or stolen in the UK in 2001. (Clarke, 2007b) This threat increases as the number of phones increases and, in 2006, over 1 billion phones were sold worldwide, with 80 million of them being smartphones. (Lin 2007) The use of smartphones is growing by an estimated 70 percent in that same timeframe. (MacLeod, 2006) Smartphones are at greater risk not only due to their growing numbers but the fact that they can store an entire identity. A 2007 survey found that 44% of users didn't use a PIN. (Clarke, 2007b) Since users can't be counted on to secure their devices and the software on them other approaches must be found.

Two actions are available if a mobile device is lost or stolen. The bank can disable a user's mobile banking services just like they can with a lost or stolen debit card. Second, AT&T ("AT&T Mobile Banking") and ClairMail (ClairMail Security White Paper, 2007) incorporate features that prevent their system from responding back to a compromised phone. CellTrust also provides the ability to use a phone and remove information from a compromised device as long as it is connected to a network. The CellTrust system has the ability connect to the phone to remove the banking application if a phone is compromised ("CellTrust 2-Way SMS Gateway").

PHISHING, VISHING OR SMISHING

Social engineering attacks are dangerous because they exploit human error. Phishing, vishing, and SMiShing are all attacks used to get users to give up their authentication information so an attacker can gain access to their accounts by appearing to be a legitimate user. Phishing is the practice of luring unsuspecting users to a fake website by using authentic-looking email with the real organization's logo, in an attempt to steal passwords, financial or personal information, or introduce a virus attack. (Phishing) Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private personal and financial information from the public. (Vishing) SMiShing uses SMS messages instead of voice communication to get the information from the victim. (SMiShing) Most of these attacks are launched from an email pretending to be someone the user knows telling them to verify information, and then redirects them to a fake website to have them fill out a form the attacker can then use to steal their credentials or worse their identity. Mobile devices are at risk from this threat, especially SMiShing. Instead of an email, an attacker could send a text message and make it look as if it's coming from the bank, saying "We need you to call 1 800 123 4567 and talk to the representative and verify your account information." IP-enabled phones are just as vulnerable to an attack as a traditional computer. Just send an email with a link to a mobile website and have then fill out the form and the attacker wins. Since mobile banking commonly uses traditional authentication methods such as a user name and password if an attacker can fool the user into releasing their credentials that users information and identity are compromised and this could lead to serious financial loss to banks as well.

PHONE CRACKING AND CLONING

Cracking is defined as to break or snap apart. (Cracking) Attackers find ways to "break" software to gain control of a device. Cloning is defined as making multiple identical copies of something. (Cloning) Cloning mobile devices is duplicating same identifying information as the original device on a phony device. Cracking and cloning threaten authentication and integrity. If a phone is cracked an attacker gains access to data stored on the device. An example of a phone crack on the I-Phone was done by ISE, which deployed an attack called fuzzing to inject invalid data into a program looking for a buffer overflow. They found an exploit in the I-Phones web browser to gain administrative privileges of the phone.

Subsequently, an attacker could view SMS message logs, call history, and have data sent back to their machine. (Miller, 2007)

Another known phone crack exploits vulnerabilities in Bluetooth. If a phone is Bluetooth enabled, any Bluetooth device within 30 feet can connect to it. (Lin 2007) Using a technique known as Bluesnarfing, an attacker remotely downloads, uploads, or edits files on a device within range without the owner's permission. One test of this in London with 943 phones found 379 had their default settings on and 138 were vulnerable to the attack. (Goodwin, 2005) Cloning new cell phones is difficult, while older analog phones were relatively easy to clone with some basic radio reception equipment. To defeat digital phones however takes a lot more effort and an attack requires sophisticated electronics to clone a GSM phone. To clone CDMA phones an attacker simply needs to get the phones electronic serial number (ESN) and mobile identification number (MIN). (Lin 2007) One Alltel customer from Wisconsin had her phone cloned and over 100 calls made after she visited a small town near the US Mexico border. Another Alltel customer from Ohio experienced the same problem after a trip to Florida. The problem affects all carriers and every phone is subject to cloning if it is left on. An attacker can use a device to scan for the signals sent out by the phone and can obtain the codes used to identify the phone. An attacker can get all the components required to build a cloning device from any electronics store for less than $2000 and can build a device sophisticated enough to capture phone signals from up to a mile away. (Vandini, 2008)

In terms of mobile banking we must consider both cracking and cloning as active threats. Cracking is a threat because an attacker could pull sensitive data off the phone. They could also use cracks to install malware. Cloning is a great threat because an attacker could fake the phones information and possibly have half of what is needed to identify a customer. An attacker could also use cloning in conjunction with a DOS to access the users data without their knowledge.

Questionable Activity

Questionable activity is concerned with authorization, authentication, and non-repudiation. For example, if a customer only occasionally checks the balance of one or two accounts using their mobile device and on occasion transfers small amounts between his own accounts, then this is their typical behavior. If one day this user requests a large funds transfer to a third party account or a bill pay payment to someone they have never sent funds to before, this is questionable activity, disallowed and flagged for follow-up. If a transaction is questionable but we have determined that the user is the legitimate user we must ensure that the transaction is legally binding so an user can't come back later and claim that it wasn't them. Credit and debit card companies today use a variety of techniques to monitor the normal activity cards and similar behavioral based detection systems can be used with mobile banking platforms (Mazhelis, 2007). Several currently deployed banking systems, like those of ClairMail, have questionable activity monitoring capabilities. ("ClairMail Security") An example can be found in the online banking systems, like the one used by Bank of America, an unusual transaction will trigger the bank to send a text message containing a 6-digit pin to a customer's phone. The bank sends a message to the customer telling them that they will be getting a call from the banks outbound IVR asking for PIN verification. The bank then calls the phone number on file for the customer and asks to verify the PIN before completing the transaction. For added security a bank could also use a voice authentication system to not only verify the PIN but the customers voice as well. (Feig, 2007)

Questionable access to some resources may also want to be examined. For example, if the user was just using their services in Chicago and an hour later is trying to connect from Hong Kong that should through up a red flag. Systems need to be able to detect and respond to these threats in a user friendly mannor.

Sensitive Data, Signatures, and Encryption

Another aspect of a mobile banking system is how it deals with customer data that must

be kept private. A system must ensure that regardless of where the data is stored an attacker can't read or manipulate the data. Solutions like signatures provide non-repudiation. When it comes to existing mobile banking systems, the two most commonly used systems, being Mobile Web and SMS, store most of the sensitive information on a bank's server. Mobile web applications require the mobile device to connect to the bank's web server, where all the information is stored and processed. Again, the use of account nicknames and limited access to account information affords more protection when attacker tries to compromise an account.

Client applications are what present the real threat to data integrity. These applications can utilize account nicknames to help protect account numbers; however, most of the processing is done on the mobile device. There are solutions to protect the data on the phone: 1) encrypt the information stored on mobile devices, 2) encrypt the communication so that if an attacker is able to intercept the message it's still useless without the key. The currently accepted standard of encryption is the highly secure Advanced Encryption Standard (AES). CellTrust utilizes AES in conjunction with special micro clients to protect SMS messages and gives the ability to send SMS messages containing encrypted messages. ("CellTrust 2-Way SMS Gateway") The phone can then decrypt the messages for the end user. ClairMail also points to the use of SSL and HTTPS during message-data communication. They also store information such as mobile profiles in Blowfish Encryption Algorithm. ("ClairMail Security"). However, there is no encryption technique specifically designed for mobile devices. Mobile devices generally lack processing power to encrypt/decrypt efficiently. Yuh-Min Tseng (2007) proposes a group key protocol for mobile devices. Many current security techniques for wired networks don't function as well on low-power mobile devices and their wireless networks.

Also another tool that can help with end-to-end encryption and protection of mobile devices are TPM's designed specifically to work on mobile devices or security smartcards. These devices are chips that are added into the motherboard and add the ability to store keys, signatures, passwords, and digital certificates. These devices will aid in the storage and processing of various security procedures and can help improve overall device security. The real advantage to these is they allow for seamless, cost-effective, and transparent to the users, which gives greater chance of being used. (Berger, 2007)

The OS and digital signatures can also play a role in the encryption process as well. For example, Windows mobile offers the ability to create and store keys, manage certificates and run cryptographic operations. Symbain also has modules that can aid in key and certificate management as well. The features of an OS can be further enhanced by the use of smart cards designed to aid in key management and signatures and certificate storage. Digital signatures offer the customer the ability to sign documents without needing to visit a branch. In e-commerce security systems, non-repudiation is used to provide evidence that a party participated in a transaction. This concept can be used in m-banking as well. For example, signatures can be used to ensure that the customer did authorize a bill pay payment before it's sent. (Ruiz-Martínez, Sánchez-Martínez, Martínez-Montesinos, & Gómez-Skarmeta, 2007)

VIRUSES AND MALWARE

While PC viruses outnumber mobile device viruses, it is easier for mobile device viruses to propagate. As adoption of mobile banking systems increases, so will the attacks on mobile banking systems. The world of mobile devices has already caught the eyes of several attackers and a number of proof-of-concept viruses have already emerged. (virus wars) Those devices running Microsoft's Windows Mobile are of particular concern given anything Microsoft tends to be a favorite target of the hacker community. (Malykhina, 2006)

A number of mobile viruses are currently a threat to mobile devices. Commwarrior uses MMS and Bluetooth to spread malware from device to device. (Lin, 2007) Trojan.Wesber and Redbrowser are similar viruses that infect windows devices and send SMS messages. (Malykhina, 2006) These viruses mainly test spreading mechanisms but

others are capable of delivering a dangerous payload. The Skulls Trojan infects Symbain devices and overwrites and corrupts applications. Bluetooth is the most common spreading mechanism used by viruses. This is because many newer smartphones are coming Bluetooth-enabled and any Bluetooth enabled device within range can be infected. This was demonstrated in Finland when a minor outbreak of mobile-malware spread from Bluetooth device to Bluetooth device at a soccer game. (Conry-Murry, 2005) Another example of the threat Bluetooth can represent is business men and women beaming electronic business cards to each other. It is possible for an attacker to put a virus into his or her card that could be uploaded into a competitor's network for some sort of personal or financial gain. (Jain, 2006) Bluetooth isn't the only spreading mechanism though. Attackers have written malware that uses both the internet and cellular networks to spread. Additionally SMS and MMS can be used to spread messages containing Symbian Installation System (SIS). (Conry-Murry, 2005)

This threat can be a major concern to both banks and end users. They can be used to launch a number of attacks against mobile banking systems from message flooding of the banks systems to the installation of malware to obtain user credentials or account information.

Antivirus companies like Symantec have produced mobile anti-virus tools to help protect mobile devices. Symantec now offers a mobile antivirus designed to protect Windows mobile devices. (Malykhina, 2006) Symantec has been working for several years with Nokia and now, Nokia has Symantec software on their Series 60 smartphones. This software is capable of passively scanning for malware in SMS, EMS, MMS, HTTP and e-mail files and can also be ran manually. (Saran, 2005)

TRAFFIC INTERCEPTS

Active wiretapping or traffic intercepts attacks are concerned with intercepting and/or altering the data while it is in transit. (Schneider, 2007) This is also known as a man-in-the-middle attack (MITM). (Man-in-the-middle attack) Essentially, an attacker intercepts information sent through communication channels and alters that information, which is a threat to the integrity and confidentiality. Another data integrity threat is a replay attack, where the attacker watches a transaction while the user completes it but doesn't actively get involved at the time. Instead the attacker merely gathers information and at a later time duplicates user activity to get the desired result. (Replay Attack) Mobile banking systems must consider the security threats that are raised by traffic intercept attacks. This threat is increased if the user connects via a wireless hotspot and instead going through the more tightly controlled network. Since we are dealing with IP enabled devices without firewalls they could become easy victims. The best way to protect data in transit is with the use of encryption. A system deployed by CellTrust includes encryption in SMS messages that utilize micro clients to enable encryption of messages and send several messages that the clients can decrypt.

10. CONCLUSION

There are three architectures used to operationalize mobile banking systems. Message based systems work on almost every device and with almost every carrier. Web based systems are the most popular in the US because of their similarity to existing online banking systems. There are also client side applications for robust mobile banking solutions. However, there are several security issues that need examination to ensure the safety and reliability of these systems. Any mobile banking system needs to have confidentiality, authentication, integrity, non-repudiation, and authorization. Customers must know these systems will provide good authentication, solutions to lost or stolen devices, phishing, cracking and cloning, denial-of-service attacks, questionable activity, sensitive data, and traffic intercepts.

The issue of how the different systems protect sensitive data is important. The most important of the security issues is that of authentication and encryption. When designing these systems we need to understand how important authentication is and the various means that are available to authenticate users and protect their devices

and our mobile banking systems. The best defense is encryption but there are some problems with encryption on mobile devices.

The potential of mobile banking systems to be the newest means for banks to interact with their customers in a meaningful way is very important. The security issues are very relevant and the threats are real. As banks move forward with mobile banking projects it is important they consider threats. With that understanding they can then develop the systems from the ground up to address these security issues and build safe and secure systems.

11. REFERENCES

Application_programming_interface. (n.d.). Wikipedia. Retrieved April 2008, Available: http://www.reference.com/browse/wiki/Application_programming_interface

AT&T Mobile Banking. (n.d.). Retrieved March 2008. Available: http://www.wireless.att.com/learn/ringtones-downloads/mobile-banking/index.jsp

Authentication in an Internet Banking Environment. (n.d.). Retrieved April 2008. Available: www.ffiec.gov/pdf/authentication_guidance.pdf

Bank of America Mobile Banking Frequently Asked Questions. (n.d.). Retrieved March 2008. Available: http://www.bankofamerica.com/onlinebanking/index.cfm?template=faq_mobilebanking

Bank of America Touts Mobile Banking Service's Growth. (2007, December). *Wireless News*, 1.

Berger, B. (2007, March). "Protecting Enterprise Data on Mobile Systems with Trusted Computing." *Security, 44(3),* 70,72,74.

CellTrust 2-Way SMS Gateway. (n.d.). Retrieved March 2008. Available: http://www.celltrust.com/

ClairMail Security White Paper. (2007, July). Retrieved February 2008. Available: http://www.pdfdownload.org/pdf2html/pdf2html.php?url=http%3A%2F%2Fwww.ClairMail.com%2Fproducts%2F..%2Fdownloads%2FClairMail_Security_White_Paper.pdf&images=yes

Clarke, N. L., & Furnell, S. M. (2005). "Authentication of users on mobile telephones -- A survey of attitudes and practices." Computers & Security*, 24(7),* 519-527.

Clarke, N. L., & Furnell, S. M. (2007a). "Advanced user authentication for mobile devices." Computers & Security*, 26(2),* 109.

Clarke, N. L., & Furnell, S. M. (2007b). "Authenticating mobile phone users using keystroke analysis." International Journal of Information Security, 6(1), 1.

Cloning. (n.d.). The American Heritage® Dictionary of the English Language, Fourth Edition. Retrieved April 2008, Available: http://dictionary.reference.com/browse/Cloning

Conry-Murray, A. (2005, December). "Mobile Anti-Virus: Now or Later?" IT Architect, 20(12), 92-95.

cracking. (n.d.). The American Heritage® Dictionary of the English Language, Fourth Edition. Retrieved April 01, 2008, from Dictionary.com website: http://dictionary.reference.com/browse/cracking

Denial-of-service_attack. (n.d.). Wikipedia. Retrieved April 2008. Available: http://www.reference.com/browse/wiki/Denial-of-service_attack

Feig, N. (2007, November). "Authentication Goes Mobile -- Banks look to out-of-band authentication as customers seek enhanced online banking security." Bank Systems & Technology, 44(11), 23.

Goodwin, B. (2005, September). "PDAs and mobiles left open to 'Bluesnarfing'." Computer Weekly, 8.

Hamblen, M. (2007, May 31). "Mobile banking still slow to catch on in US." (PC World) Retrieved April 2008. Available: http://pcworld.about.com/od/webservices/Mobile-banking-still-slow-to-c.htm

Holland, N. (2008, January). "The Predictable Success Of Mobile Banking." Bank Systems & Technology, 45(1), 27.

Jain, S. (2006, October). "A Mobile Security Battle." Security, 43(10), 66-67.

Lin, P. P., & Brown, K. F. (2007). "Smartphones Provide New Capabilities for Mobile Professionals." The CPA Journal, 77(5), 66-71.

MacLeod, M. (2006, December). "Success of mobile devices builds security opportunities." MicroScope, 16.

Malykhina, E. (2006, November). "Smartphones Under Fire." InformationWeek, (1114), 55-56.

Malykhina, E. (2007, January). "PHONE SMARTS." InformationWeek,(1122), 32-38.

Man-in-the-middle attack. (n.d.). Wikipedia Retrieved April 2008. Available: http://www.reference.com/browse/wiki/Man-in-the-middle_attack

Mazhelis, O., & Puuronen, S. (2007). "A framework for behavior-based detection of user substitution in a mobile context." Computers & Security, 26(2), 154.

Miller, C. (2007, August). "ISE Hacks to Protect iPhone." Design News, 62(11), 18.

Wells Fargo Mobile Banking. (n.d.). Retrieved March 2008. Available: https://www.wellsfargo.com/mobile/

phishing. (n.d.). Webster's New Millennium™ Dictionary of English, Preview Edition (v 0.9.7).

Rajnish, T., & Stephan, B. (2007). "The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector." Hamburg University Press.

Replay Attack. (n.d.). Wikipedia. Retrieved April 2008. Available: http://www.reference.com/browse/wiki/Replay_attack

Riivari J. (2005). "Mobile banking: A powerful new marketing and CRM tool for financial services companies all over Europe." Journal of Financial Services Marketing, 10(1), 11-20.

Ruiz-Martínez, A., Sánchez-Martínez, D., Martínez-Montesinos, M. Gómez-Skarmeta. A. F. (2007). "A Survey of Electronic Signature Solutions in Mobile Devices." Journal of Theoretical and Applied Electronic Commerce Research, 2(3), 94-109.

Saran, C. (2005, October). "Nokia counters malware threat to data on its smartphones." Computer Weekly, 26.

Schneider, G. (2007). Electronic Commerce Security. In Electronic Commerce (Seventh Annual Edition ed.). (PP. 438-483) Boston, Massachusetts, United States of America: Thompson Learning Inc.

SMiShing. (n.d.). Wikipedia. Retrieved March 2008. Available: http://www.reference.com/browse/wiki/SMiShing

Tang, J., Terziyan, V., Veijalainen, J. (2003). "Distributed PIN Verification Scheme for Improving Security of Mobile Devices." Mobile Networks and Applications, 8(2), 159.

The Mobile Platform for Financial Services. (n.d.). Retrieved March 2008, Available: http://www.mfoundry.com/display/corp/Home

Vandini, C. (2008, 10 March). "Cell phone cloning stuns owners: Unsuspecting victims surprised by high bills, extra calls." McClatchy - Tribune Business News.

Vishing. (n.d.). Wikipedia. Retrieved March 2008. Available: http://www.reference.com/browse/wiki/Vishing

Wachovia Mobile. (n.d.). Retrieved March 2008. Available: http://www.wachovia.com/misc2/0,1794,00.html?DCMP=KNL-CPS-Mobil-%200711&HBX_PK=Wachovia+mobile+banking&HBX_OU=50

Yuh-Min Tseng (2007). "A secure authenticated group key agreement protocol for resource-limited mobile devices." The Computer Journal, 50(1), 41-52.