The State of Mobile Security in Banking and Financial Transactions

Conducted by
Javelin Strategy & Research
September 2009

Overview

Many financial institutions are now incorporating mobile banking and financial services as a key component of their growth strategy, and use of the mobile phone to conduct banking and financial services tasks continues to rise among early adopters. However, among the majority of consumers, security threats are most commonly listed as the primary reason for not trying mobile banking. This whitepaper will attempt to technically address these largely unfounded consumer security fears while helping to lay a roadmap for financial institutions' successful implementation of mobile banking technology.

Key Questions Explored in This Paper

- Where is the weakest link in the mobile security chain?
- Are mobile security threats the same as online threats?
- How do different operating systems on mobile devices impact security?
- What are best practices to mitigate threats?
- Is mobile viable as a banking and financial services channel, or is the risk too great?

Key Findings

While consumers continue to express concern over using their mobile phone to conduct banking and financial services transactions, it is a fear born more of perception than reality. There are threats, but the security controls available to mitigate risk at this level are substantial and effective. However, security practices will need to continue to evolve as more and more smartphones enter the market running more and more applications, creating an ever growing opportunity for security threats.

I. Executive Summary

The purpose of this paper is to educate the reader on the security threats and vulnerabilities for mobile, especially in the context of the financial services industry. This report highlights the most popular strategies for deploying mobile services, including SMS, client-based applications and the mobile Web, and the benefits and risks to each type of service.

In 2009, mobile phones are commonplace: An estimated 86% of U.S. adults own one. Currently in the U.S., there are 36 million adults accessing mobile banking. Javelin Strategy & Research forecasts that within five years almost half of all mobile phone owners (45%) will be reaching for their mobile phones to conduct banking chores.

Many financial organizations have chosen to deploy mobile banking via SMS, client-based applications, or the mobile Web, either individually or in combination. According to the "2009 Mobile Banking and Smartphone Forecast" by Javelin in September 2009, the following table summarizes the modalities available over the mobile channel.

SMS/Text	Mobile Web	Downloadable application	Embedded application
100% of phones sold today	95% of phones sold today are Web-enabled; but many require difficult activation 18% have smartphones -- best for viewing	95% of phones sold today	Not widely available yet
FI-carrier-independent	FI-carrier-independent	May require FI partnerships with wireless carriers	May require FI partnerships with wireless carriers, mobile handset vendors
Relatively less expensive (depending on plan) or approximately $0.20 per message	Requires unlimited data plan	Requires unlimited data plan	Requires unlimited data plan and new phone
Easy to set up and use for most consumers	Fairly easy to set up and use for most consumers	More difficult; downloading application is challenging for many	Easiest to set up and use for most consumers, but availability limited

For American consumers, two of the biggest factors inhibiting the growth of mobile banking is the fear of data interception by a third party and lost devices. At present fear of data interception are largely unfounded, in part because the equipment necessary to break into a mobile network is expensive and generally not available

I. Executive Summary

to criminals who make quick money elsewhere. Mobile malware, including viruses, worms, and Trojan horses, are OS-specific. Additionally, the mobile channel is still too fragmented with too many handsets and operating systems for a single virus to claim widespread damage. Although large-scale mobile malware is not yet common, there have been several specific viruses written for most of the major operating systems. For example, the Symbian OS has seen its fair share of mobile malware.

Unlike "traditional" online devices, mobile devices feature a number of ways to communicate with other devices and with the Internet. Bluetooth has become standard, although in most instances it is disabled by default. USBs and mobile memory cards are vectors that pose more of a risk on the mobile device than an online PC, because people are more likely to trade MP3, ringtones, and media files this way. There are also possible but unlikely risks from over-the-air (OTA) programming, which could rewrite the firmware on a mobile device. Like online, the mobile channel, particularly the mobile Web, must contend with phishing and man-in-the-middle attacks. In addition, there's smishing (phishing conducted over SMS) and vishing (phishing conducted over the voice channel).

Mobile financial services are still in their early days, so this immature market is less attractive to criminals who can realize more profit from the online channel. One factor fueling the growth in mobile banking is the recent increase in customer service plans that offer unlimited text and/or data, which allows for downloaded banking and financial services applications. While this is good for the customer who chooses to receive account information in this way, it is also bad for the customer because attackers can also send more spam, which can lead to phishing and introduction of malware onto the mobile device.

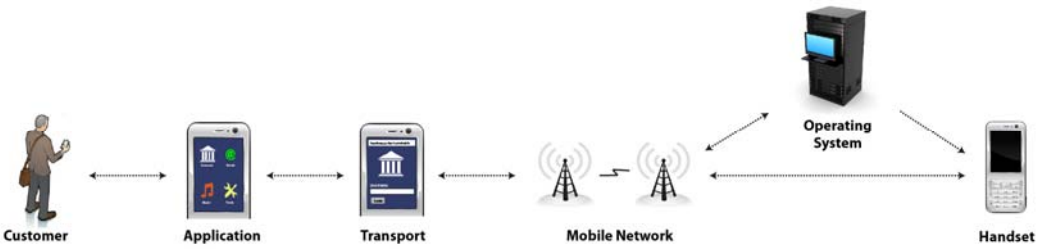
At the mobile gateway, attackers could potentially view or intercept SMS messages while they are in the clear as they travel across the network, although this risk is minimal. Insiders could place sniffers on the network, however, this requires expensive equipment on behalf of the attacker.

Mobile threats aren't, however, limited to the various mobile communications channels. If a handset is ever lost, the experience is much like losing your credit card or wallet: Valuable information could be compromised. For an enterprise, this could include intellectual property. For an individual, it could include information to access bank accounts as well as e-commerce and healthcare sites. This is one area where secure software development practices could help, limiting the amount of data collected by the handset, and/or securely removing any data once the application is closed.

Finally, this report includes a best practices section and a glossary covering many of the terms used.

II. The Mobile Ecosystem

When talking about the mobile ecosystem, the first line of defense (and often the weakest link in the security chain as well) is the mobile user. Users are largely responsible for physical security (protection against loss), authentication, and maintaining the security of the operating system and applications (downloading only from responsible parties). Customers aren't responsible for implementing the security features; that's the job of the bank or the service provider. Because threats and vulnerabilities can exist in all service layers and with every player, appropriate safeguards must be considered in all of these places as well. The mobile network operators (MNOs) that manage the network are responsible for network security and signaling security (which is the channel used by SMS and USSD). Aggregators also play a role in network security because they act as intermediaries between content providers and the mobile network operators.



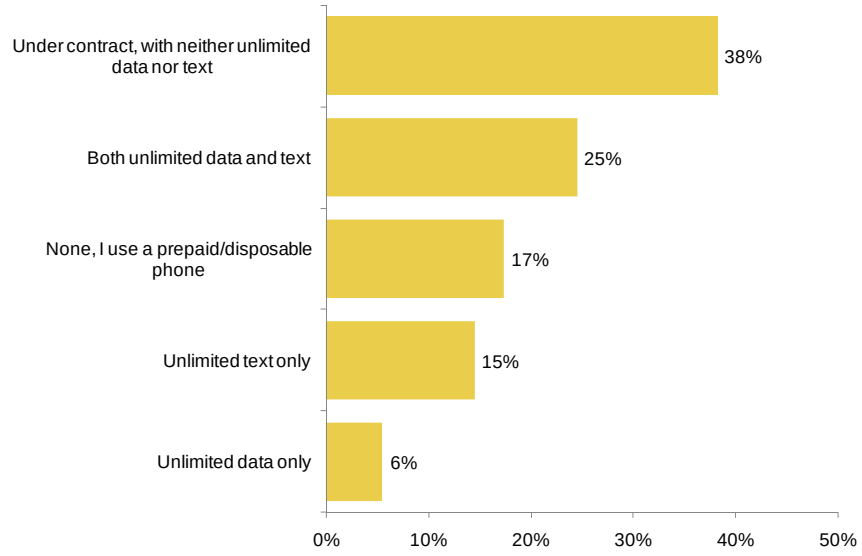
Each layer of the stack has to be secure. This may seem obvious, but it is complicated by the fact that different players "own" security for differently layers in the stack. For example, the handset manufacturer owns security for the handset and the operating system (OS), but the platform vendor owns the security for the application. Since the layers interact, the vendors have to interact as well in order to fully secure the mobile ecosystem and financial transactions conducted in that ecosystem.

II. The Mobile Ecosystem

2.1.0. The Stakeholders for Mobile

At the top of the stack is the customer. The customer is the end user (or consumer) who purchases the mobile handset and the service plan and ultimately downloads any applications added to the device. The applications vendor includes financial solutions vendors and the FIs.

Fueling the growth of mobile banking is the recent increase in customer service plans that offer unlimited text and/or data.



Q22: What type of wireless plan (data and text) do you currently use? (Select one only)

July 2009, n = 3,000
Base: All consumers with mobile phones.

The next level of the stack is the service provider. The service provider is the wireless carrier or mobile network operator (MNO), which, in the United States, includes Verizon, AT&T, T-Mobile, and Sprint, as well as a number of smaller players. The MNO is the party that has a license within a country to allocate a certain bandwidth of the radio spectrum to cellular communications.

Just below the service provider is the platform vendor. The platform vendor (for example, Tyfone, M-Com, ClairMail) is the party that develops the server (and sometimes client) software used by the bank to provide mobile banking services to the customer. This includes companies like Syniverse Technologies, which acts as an SMS aggregator, working with both the mobile networks and the financial institutions.

II. The Mobile Ecosystem

Finally, there's the handset manufacturer, which is responsible for the hardware used as well as -- in cooperation with the MNO -- the underlying operating system. In the United States, this includes Microsoft, Symbian, Apple, Google, and Linux. The same hardware and OS used by different carriers can be configured differently, often to accommodate the specific needs of the carrier.

2.2.0. The Mobile Services Stack

Since the customer is at the top of the stack, education isn't enough; there is also the issue of control. Often the customer is not given enough control over his or her security on the mobile device even when greater control is available. Customization can be found at various levels beneath the customer. These include:

The application layer can be either embedded on the handset or downloaded from the carrier's site, or make use of the mobile browser.

Mobile device transport layer includes HTTP and TCP/IP from the online world, along with Wireless Application Protocol *(*commonly referred to as *WAP), Short Message Service (SMS),* USSD, Bluetooth, and, although technically not a message transport, OTA (Over-The-Air). These are designed to interact with the Internet or service provider without being connected physically to a network.

The wireless network can be either Global System for Mobile communications (GSM) or code division multiple access (CDMA).

There's also the operating system platform, which is tightly proscribed by the handset's resources.

And finally, there's the handset, of which there are many variations on the market today.

III. Mobile Security

While mobile security is similar to online security, it is not identical. Like online security, the mobile channel must contend with phishing, malware, and man-in-the-middle attacks. In addition, there's smishing (phishing conducted over SMS) and vishing (phishing conducted over voice channel). Despite these threats, if secured properly, the mobile channel is one of the safest. What does securing it properly mean? It means implementing security controls that take advantage of the innate security strengths within mobile. If this isn't done, mobile is no more secure, and probably less secure, than other channels.

For the moment, the threat landscape is favorable to mobile devices. There are many reasons for this. One, mobile financial services are still in their early days. Consumer adoption at 18% isn't fully realized and mobile banking services aren't yet fully functional, e.g., they often don't include the capability to move money. This immature market is less attractive to criminals who can realize more profit from the online channel. Another mitigating factor is the diversity of operating systems, with no one dominant OS. For now the diversity of mobile handsets and platforms makes it harder for criminals to write malware. By contrast, writing a Windows-based 32-bit malware application allows the criminal to hit roughly 90% of the online PC market. This will change in the coming years, with increasing market share by the Apple iPhone and as financial institutions offer fuller banking functionality via the mobile channel.

3.1.1. Mobile's Dissimilarity to Online

One area where mobile is dissimilar to online is applications. On the mobile there is greater likelihood that applications are digitally signed, meaning the vendor has submitted them to the platform vendor for approval. However, this isn't the case for Android, because it is open source, which poses a security concern because there is no approving authority for developers to post applications to the platform. So, for example, a criminal might post a bogus mobile banking app, which was really a piece of malware.

Applications on certain mobile devices also run within "sandboxes", which isolate the code within the environment, with limited rights. The mobile platform allows for remote device management, with the ability to terminate an application or even the entire device if it is reported lost or stolen — something that is not common with online applications.

3.2.1. Mobile's Strengths and Weaknesses

As with any communications channel, there are relative strengths and weaknesses to mobile devices.

Among the strengths, mobile device is top of mind with mobile device customers. If a customer leaves home for work in the morning without a mobile device, or without a wallet, which one is he or she most likely to

III. Mobile Security

discover missing first? If the handset is ever lost or compromised, it can be remotely deactivated by the carrier. Additionally, particular applications can be deactivated from the server or the entire device can be remote-wiped. Currently, for example, enterprise-based BlackBerrys and some mobile banking platform vendors offer this feature. This helps mitigate the fact that handsets are easily lost or stolen: Javelin research shows 19% of mobile phone owners have had a handset lost or stolen.

The mobile channel also has the fastest reaction speed to emerging fraud. Because people are more likely to have their mobile devices with them 24/7, they are more likely to be responsive to a fraud alert from their financial institution. Rather than wait until the end of the month to review their paper statement for signs of unusual activity, customers can be notified by their financial institution within hours either via SMS or push e-mail. Furthermore, this method "deputizes the customer," involving them directly in securing their financial accounts. Javelin research shows 80% of all consumers believe this responsibility should be shared between consumers and their financial institutions. This translates to time saved between when the fraud is first instigated and when it is detected. Criminals use time to their advantage, and mobile has the potential to take the time advantage away. (Consumer self-detection results in a period of misuse that averages 56 days less than notification by an outside institution.)

Like personal computers, mobile devices can be used as an authentication factor. Authentication can be based on “something you have, something you know, or something you are.” The mobile handset becomes "something you have." But currently the typical mobile device is less personalized than the typical personal computer, making native device recognition less reliable. One method to increase security is to download a token onto the mobile device that will become its unique identifier. Another method is to contract with the wireless carrier network to identify the device.

Because consumers carry their mobile phones with them 24/7, they can be used to replace one-time password-generating hardware tokens. Software-based one-time password (OTP) tokens make more sense, not only because they are more convenient to carry for the consumer, and greatly increase security, but also because the software can be redeployed less expensively over the air. Latest developments to watch for include software that inputs the OTP automatically into the password field, thwarting key logging malware and increasing ease of use. However, not all handsets have the processor and memory required to generate OTPs.

At the moment there is no dominant mobile operating system or handset vendor. It is harder to write mobile malware than online malware. Similarly, it will be more difficult to educate end users because security vendors will have to produce different anti-malware solutions for each variation of OS and hardware.

III. Mobile Security

Mobile platforms and handsets do include the use of PINs for power-on and idle timeouts (screensaver) recovery. However, these are not enabled by default. Use of a power-on PIN or password is a user choice that cannot be enforced from the server. This will require education to inform end users to the value of setting these protections.

Finally, the controlled nature of the mobile networks makes them somewhat safer than the Internet because there are steep hardware costs for attackers to gain access to mobile networks.

Among mobile's weaknesses is data stored on the handset. If the mobile banking application is well-written, it should not store sensitive data in the first place, so this risk can be mitigated by using secure software development practices. Additionally, stored usernames and passwords, which may conveniently allow for quick access, need to be adequately protected against unauthorized third-party access, especially to such accounts as financial and medical services.

	Strengths	Weakness
Mobile Handset	Always present with customer	May store username, password, and personal data
	Can be used as an authentication factor	
	A PIN can be used to lock the mobile device	Most PIN locks are not enabled by default
	One-time passwords (OTP) can be generated on the mobile device	Not all mobile devices have the processor and memory required for OTP generation
Mobile Operating System (OS)	No dominant OS means the likelihood of malware is less.	No dominant OS means it is harder to obtain anti-malware software
Mobile Network	Steep hardware costs required for attacks	

III. Mobile Security

3.3.1. Customer Perceptions

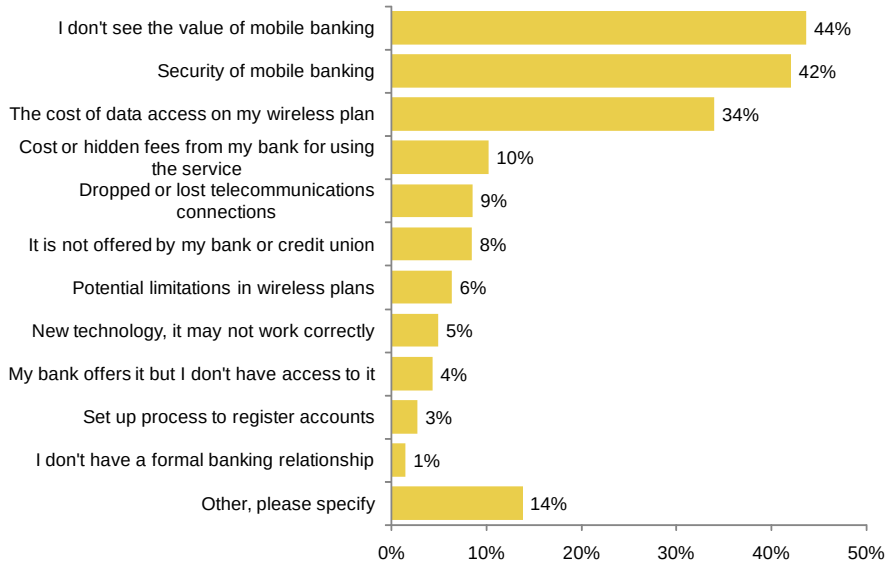
What are the biggest factors inhibiting the growth of mobile banking today? For consumers, security consistently remains one of the biggest stumbling blocks to mobile adoption, although usage of the channel seems to allay some of these fears. Nonetheless, almost half of mobile bankers cite security as their main concern (47%).

Mobile banking requires security to support wireless transactions on multiple levels:

- The mobile device itself
- The security of the particular banking application that may be run from the device
- Securing of the data stored on the mobile phone
- Securing or encrypting the data transmitted over the air

Authentication of the customer is needed to guarantee that a legitimate and authorized customer is performing the transaction; authentication of the device guarantees that the transaction is occurring over an authorized mobile device. Finally, authentication of the financial institution to the customer helps avoid phishing scams and other attacks.

Security Is the Sticking Point for Consumer Adoption



Q6: You indicated you do not use mobile banking. For what reasons do you not use mobile banking? (select up to three)

July 2009, n=2,396
Base: All consumers with mobile who do not use mobile banking.

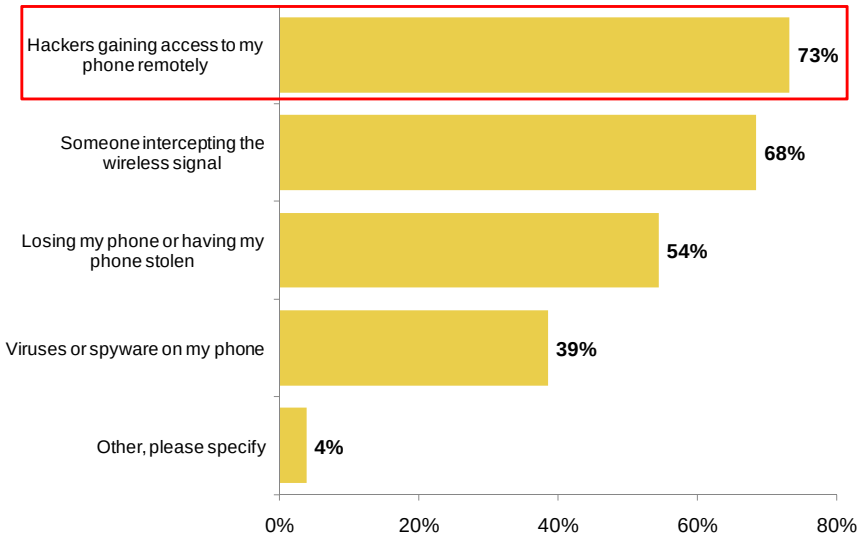
III. Mobile Security

With security as a key driver of consumer acceptance and growth of the channel, it must be given top priority in product and marketing budgets for mobile financial services. Fortunately, for both financial institutions and consumers, the mobile channel can increase banking security if it is deployed correctly: Users are able to track their financial information in real-time from practically anywhere in the world. Frequent self-monitoring of accounts is an effective way for consumers to detect fraudulent transactions and activities. Text-message alerts allow users to receive regular updates on account activity, adding another level of security. Half of U.S. consumers believe that text message alerts sent to their mobile handsets is an effective way to fight fraud.

Unfortunately, many myths abound about mobile security.

Many customer fears about mobile security turn out to be unfounded. For example, customers frequently cite the interception of data by a third party (73%) as one of their top security concerns with mobile banking. While mobile malware does exist, the risk of having a mobile phone call remotely accessed is almost nonexistent. Nonetheless, once sufficient numbers of consumers are banking on the mobile channel, it will become a larger target for hackers. Mobile Web and dedicated mobile applications are subject to man-in-the-middle attacks, in which the attacker intercepts data between the customer and the financial institution. The Web browser is subject to man-in-the-browser attacks, in which the session interception is done by a Trojan horse as opposed to a human being. While even SMS can be spoofed or compromised, customer education can be effective, as in other channels, to mitigate the risk.

Hackers Gaining Access to Mobile Phone Is Top Security Fear



Q35: You mentioned that security was one of your top concerns with mobile banking, what security aspects are you most concerned with? (Select up to three)

March 2008, n = 702
Base: Respondents with mobile banking security concerns.

III. Mobile Security

3.4.1. Threats, Vulnerabilities and Countermeasures

Mobile phishing takes many different forms. The most common form used today makes use of SMS (smishing), the use of SMS to spread phony URLs, and VoIP (vishing), the use of telephone numbers to lead victims to bogus voice services (such as IVR) that fool victims into believing they're talking with their financial institution. Attackers often send fraudulent SMS messages to large volumes of users, attempting to gain private information. Mobile phishing can affect SMS or Web-based banking when messages include a URL or a phone number. Upon calling a phone number, a user may interact with an actual person or a voicemail system, both of which risk exposing that user's personal information.

3.4.2. Broad Threats

Broad threats in the mobile channel include unauthorized access to services or sensitive data. Malicious hacking and damage to the device, denial-of-service attacks, and Web-based attacks have more or less the same threat profile on the mobile as PCs. Mobile's malware is currently platform-specific, with only a very few examples of cross-platform malware to date. Because of various controls on the mobile device, mobile malware today still requires user interaction. That may not be true with more robust mobile operating systems in the future.

Mobile viruses are one area where user education is an effective mitigation. The fragmentation of the handset, browser, OS and carrier markets makes it hard to design an effective "one message fits all devices" education campaign, although at the end of this report we do offer some best practices.

Javelin believes that current threat to mobile banking is low. There are many unique devices, browsers and operating systems, which makes it difficult for attackers to target large swaths of customers. It is also one of the reasons most of the mobile viruses today are written for the Symbian OS, which is the most prevalent mobile OS in the world. Javelin believes that the lack of credible threats to financial data may be due to the newness of the financial offerings on mobile.

3.4.3.0 Handset

Unfortunately, the customer may become frustrated with "too much security" when using either the handset or the application security features. The customer may then chose to disable them or at least try to disable them. The best security features marry convenience with safety: For example, an encrypted handset may allow a consumer to answer certain phone calls without logging in.

III. Mobile Security

In other parts of the world, specifically Japan and South Korea, mobile banking on GSM networks has been in use for several years. Despite its widespread use, the known fraud in mobile banking in Pacific Asia has been low. One feature that contributes to the low fraud rates is the linking of devices through hardware chips and bank accounts. The hardware links the user's bank account to a specific mobile device so that only that specific device can conduct transactions. This can be done by OTA provisioning of the SIM or by use of a smart card. It is slightly more expensive to deploy on CDMA networks.

3.4.3.1 Memory Cards

The use of memory cards with the handset could be problematic. In 2004, a mobile virus known as Skulls used infected memory cards to infect Symbian Series 60 devices. Skulls is a Trojan horse that arrives as an installer for a normal application. Skulls then overwrites existing applications (except those required to communicate), rendering them useless. It replaces mobile desktop icons with images of skulls. Some of the 30-plus variants also install other mobile malware onto the phone.

3.4.3.2 Downloads

The client-side environment includes the applications downloaded and installed on the device. These can be signed by either the carrier or the financial institution. Often the applications are sandboxed on the device. The most secure choice for financial institutions is not to send sensitive data to the handset at all. The next best is to delete it at the end of each session, or if sensitive data is stored on the handset, to encrypt the data.

3.4.3.3 Applications

Enterprises and commercial software developers should employ secure software development best practices. Despite the rigorous testing of mobile applications by various carriers and platforms, some malicious software has leaked into the online application stores. Authentication of the application code could be used to help customers know they are downloading the real banking application. This is a problem with open source software, such as that designed for Android or Linux platforms. Here, no one vets the application, unlike Symbian and Apple.

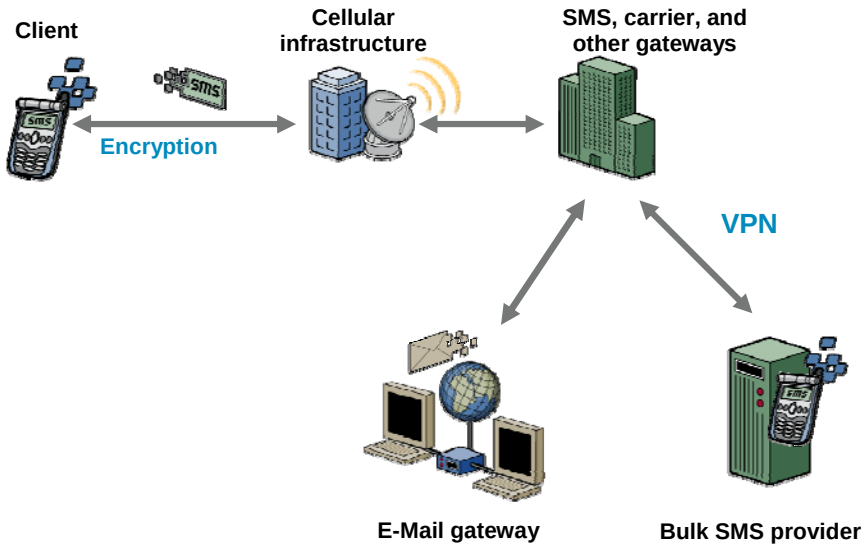
3.4.3.4 Mobile Browsers

Some of the mobile browsers are subject to the same flaws as PC browsers such as malicious scripts, man-in-the-browser attacks, cross-site site scripting (XSS), and cross-site request forgery (xSRF). Although they have smaller feature sets, mobile browsers have been subject to attacks in which unauthorized commands are transmitted from a user to a Web site. It is difficult to determine the legitimacy of a URL with a mobile browser: The small-form factor makes it incapable of displaying full URLs or it can take many menus to access the security information of a given site. Most mobile browsers lack support for protections normally available on desktop systems such as URL filtering, phishing toolbars, and secure sockets layer (SSL) or extended validation secure sockets layer (EV SSL) certificates. Based upon these concerns, it seems likely that users of mobile devices have an increased risk of falling victim to a phishing attack when they surf with mobile browsers.

III. Mobile Security

3.4.3.5 Mobile E-mail

Mobile e-mail clients are often the source of spam, phishing and malware introduction. For example, criminals use the e-mail-to-SMS gateways that allow the user to send e-mails instead of spending money sending SMS messages. In this way, criminals can send e-mail to all possible SMS recipients.



As a result, SMS gateway providers have responded to abuse by rejecting excessive numbers of messages or fraudulent messages. Filtering is dependent on the cooperation of Internet service providers (ISPs) rather than defensive tools on mobile devices. Uncooperative ISPs could cause this network filtering to fail. SMS and e-mail protocols allow attackers to send spoofed messages from falsified source addresses. Spoofed e-mail messages are generally more common because anyone can operate a mail server and send e-mail spam. E-mail-to-SMS gateways are one option that attackers have abused in the past to send SMS phishing messages.

3.4.3.6 Mobile IM (MIM)

Mobile IM (MIM) is subject to similar threats that are found on the PC desktop. Phishing and malicious URLs are the problem.

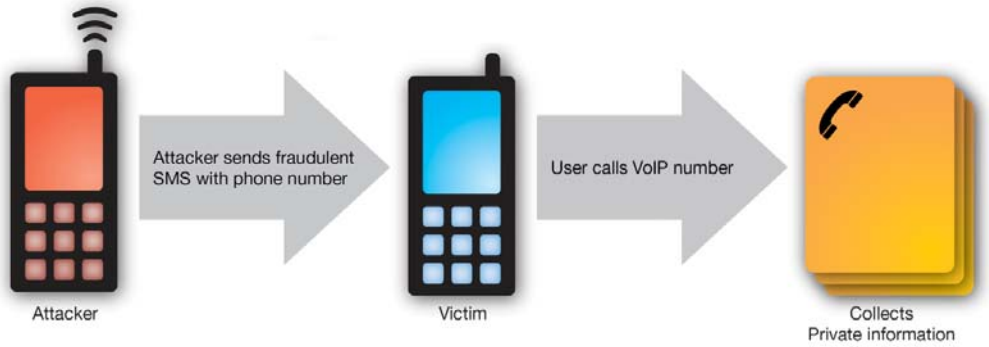
Some legitimate financial services may suffer from user doubt and uncertainty related to sending legitimate SMS messages because of the potential for attackers to send spoofed messages. Financial organizations should avoid repeating the mistakes they made with e-mail, which have caused some to abandon contacting their clients through e-mail altogether. To gain the user's trust, financial service providers may choose to avoid sending phone numbers, SMS numbers or URL links. Combining these restrictive measures with user education campaigns can limit the effectiveness of phishing attacks.

III. Mobile Security

3.4.3.7 Voice

Phishers also often spoof the source e-mail address and use a large number of different phone numbers to perform vishing. Vishing is the criminal practice using social engineering over the telephone—both land-based and mobile. Fraudulent vishing messages on the mobile are similar to vishing attacks online and contain a phone number that a victim calls upon receiving the message.

How Vishing Works



There are many examples of vishing attacks that use voicemail systems to steal user information, including bank account information. In January 2008, the Facebook application "secret crush" began phishing users by requesting their mobile phone numbers through the social networking Web site. Subsequently, it would send users messages from a premium SMS service that cost $6.60 per message, according to one user afflicted by the scam. Users who reply to the premium-rate number (1-994-4989) receive charges on their mobile phone bills.

3.4.4 Operating Systems

Educating users about operating system features and encouraging them not to install software from unofficial sources can help to mitigate mobile threats.

3.4.4.1 Symbian

The Symbian OS, an open industry standard with the greatest global market share, has been the most targeted by malware so far. The best known of these is the Cabir worm, discovered in June 2004. The Cabir worm was developed as a “proof of concept” virus by Group 29A (an international group of programmers) and has spawned at least fifteen variants. A proof-of-concept virus is developed by programmers to demonstrate existing vulnerabilities in software, and is often sent to the manufacturer or an antivirus firm, rather than being used maliciously. The original worm spread over Bluetooth connections on Symbian Series 60 mobile phones, arriving in the inbox as a caribe.sis file. The user has to accept the file, and it spreads slowly because it is capable of infecting only one other phone per activation or reboot. In August 2004, Mquito, the first Trojan to target Symbian, appeared

III. Mobile Security

in an illegal version of a game by Ojun called Mosquito. Each time the game was played, the Trojan would send a premium SMS message. In an ironic twist, it was discovered that the Trojan had been placed by the developer Ojun itself, with the premium SMS call going to Ojun to notify the firm whenever an illegal version was played or the game was run on an unregistered mobile phone. While it worked as planned, a significant number of legitimate users were also affected with premium SMS charges, so Ojun ended up cancelling the premium number and re-releasing the game without the Trojan.

To combat malware, Symbian adopted a digital signature program; all mobile applications would have to be approved by Symbian before they could be installed on a Symbian phone. On or before Feb. 4, 2009, Chinese mobile phone users began reporting a new virus that affects Symbian S60. All code on S60, third edition, must be signed, and this virus is no exception; it uses a certificate from Symbian licensed to "ShenZhen ChenGuangWuXian." After a user installs the program, it spreads to other users by sending SMS messages that contain URLs for users to download and install the code. The "Sexy View" virus attempts to persuade recipients to download and install a Symbian Installer file (SISX) at the URL, but it does not use any exploits to install such files automatically. Such mistakes show the limitations of platform download stores or signature programs.

3.4.4.2 Windows

In the lucrative U.S. market, Windows mobile has held a slim lead in user numbers, making it a target as well. WinCE.Duts, discovered in July 2004, is another proof-of-concept virus developed by Group 29a for mobile devices running under Windows CE for pocket PCs. While it requires user confirmation to download, Duts can infect mobile devices via e-mail, mobile Web, and through the synchronization or Bluetooth protocols.

Arriving in September 2005, Cardtrap is the first known cross-platform virus, in which the main goal is to infect the user's PC. Cardtrap is disguised as an installer for a normal program, but once it's accepted, it installs other malicious codes and corrupts existing applications. When the phone's infected memory card (multimedia card or "E drive") is inserted into the PC in an attempt to remove the virus on the phone, malicious code (e.g., worms, Trojans, backdoors) is transferred to the PC, among them a virus that disables security on the PC.

In early 2008, a new WinCE Trojan called InfoJack insidiously appeared inside legitimate installer packages like Google Maps as an option. This Trojan disables Windows' mobile security so that other unaccredited applications can be installed without permission. It then sends the serial number, operating system information, and other data to a Web site in China. In early 2009, HTC devices running Windows Mobile 6 and Windows Mobile 6.1 were prone to a directory transversal vulnerability in Bluetooth OBEX FTP service. "Directory traversal" allows an attacker to exploit inadequate security to input file names, allowing software to access files that are not supposed to be

III. Mobile Security

accessible. Successful exploitation allows an attacker to list directories and write or read files for execution.

3.4.4.3 Palm

Palm, although having a smaller footprint worldwide, is not immune to vulnerabilities. In 2009, Palm issued updates for its new Palm Pre model. Among the issues addressed was a denial of service when a user clicked over long URLs (greater than 4,063 characters). Attackers could have distributed an exploit for this through e-mail, MIM, or SMS.

3.4.4.4 iPhone

At Black Hat USA 2009, researchers showed how one could use a malicious SMS message to shut down the ComCenter in the Apple iPhone. The attack would not only disable SMS, but also Wi-Fi and 3G service on the device. Apple has since fixed this particular vulnerability. The researchers were also able to perform similar attacks on Google Android, and Windows Mobile. The researchers had not yet had the time to study the Palm Pre.

3.4.4.5 BlackBerry

In early 2009, a vulnerability was announced that could allow criminals to take control of the servers running BlackBerry systems. It worked by sending e-mails with tainted attachments within Adobe Systems' PDF format. If the customer opened one of these compromised PDFs, it attempted to install malicious software on the server so that criminals could then use that server to send spam or steal corporate or personal data.

3.4.4.5 Android

In some ways the open-source Android platform is more secure than other operating systems. By design, its OS uses the sandbox approach, which isolates code injected into the browser from other parts of the mobile system. That hasn't stopped research into vulnerabilities. In early 2009, security researcher Charlie Miller discovered a way that allows criminals to take control of the phone's Web browser. If compromised, the browser's credentials and history could be visible to a remote hacker. No word on whether this vulnerability has been patched.

3.4.4.6 Linux

Linux has a very small footprint on the market, and thus less incentive for attack. A few years ago, Motorola, NEC, NTT, DoCoMo, Panasonic Mobile Communications, Samsung Electronics and Vodafone banded together to form the LiMo foundation, an industry group dedicated to providing the first open, hardware-independent, Linux-based OS. One of its purposes is to seek participation from application and middleware vendors for the nascent operating system.

3.4.4.7 J2ME mobile phones

Not really an operating system, Sun's Java 2 Micro Edition (J2ME) allows devices with limited hardware resources (with as little as 128K or RAM and processors less powerful than desktop

III. Mobile Security

machines) to run applications. J2ME uses profiles defined for a particular type of device. Each mobile device has its own minimum set of class libraries required for that specific device and a special version of the Java virtual machine required to run that library. In early 2006, RedbrowserA was the first Trojan to target J2ME mobile phones. It attempts to convince customers that it will allow them to send free SMS messages using a WAP site. Instead, it sent premium SMS messages to a Russian number. Premium rate SMS are used legitimately for third-party content or service providers to make money over the mobile network by charging the customer's bill for the premium service.

3.4.5 Transport

In addition to keeping the operating system updated and protected, how the data is sent to and from the financial institution is also important.

3.4.5.1 HTTP

Smartphone browsers are able to access the Internet and take advantage of some of the communication protocols leveraged in online security. These include SSL, a method of mutual authentication that includes encryption.

3.4.5.2 WAP

Wireless Application protocol (WAP) is an open data transport standard for mobile environments. Its main use is to access the Internet from a mobile device. A WAP browser includes all the basic services of a PC-based browser, but reduced to function within the restrictions of the mobile ecosystem -- for example, a reduced screen size. WAP sites are Web sites that are dynamically converted to WML (wireless markup language) and optimized to be viewed via the WAP browser.

3.4.5.3 TCP/IP

TCP/IP is the Internet protocol used on all computers and is available for use on smartphones with full or robust operating systems and greater memory. TCP/IP handles low-level networking protocols such as IP, TCP and UDP. Vulnerabilities within TCP/IP could lead to denial-of-service attacks (crashes or loss of service), or IP spoofing (in which attackers forge an address to look like a trusted source), or Routing Information Protocol attacks (which changes where data goes).

3.4.5.4 SMS

SMS, when used by itself for financial services, is vulnerable to a number of attacks. SMS logs on the handset pose a potential threat, depending on the sensitive nature of the data sent or received in the SMS messages. Client-based SMS applications may represent risks for stored sensitive information if they store information in clear-text or if attackers are able to decrypt files. Data saved by a client-based SMS application is a lower risk because applications can have stronger restrictions on destroying and encrypting important and confidential data. Tools exist to extract SMS and e-mail logs from memory; therefore, once an attacker gains access to the logged information from a financial

III. Mobile Security

institution, he or she might be able to masquerade as the user and conduct important transactions. Organizations should avoid requesting or sending full account numbers or other information necessary for an attacker to conduct transactions through e-mail or SMS messages.

3.4.5.5 Bluetooth

Bluetooth is a short-range wireless protocol that includes a promiscuous feature. OBEX is designed to allow Bluetooth devices to discover other Bluetooth devices in the area, then connect to them. While it works well when connecting a wireless headset to a mobile device, Bluetooth protocols can also be used to connect to a mobile device with unfortunate results when malware is involved. Bluejacking and bluesnarfing are two methods in which an attacker can approach a victim, connect via Bluetooth, and dial premium phone numbers or create a denial-of-service attack without the victim realizing it. As a result, many phones today disable Bluetooth by default. The risk of this activity is low because it requires a combination of Bluetooth being enabled, physical proximity, and malicious intent. The Cabir worm, discussed earlier, was discovered in June 2004 and has spawned at least fifteen variants. The original worm spread over Bluetooth connections on Symbian Series 60 mobile phones, arriving in the inbox as a caribe.sis file. The user had to accept the file, which spreads slowly because it is capable of infecting only one other phone per activation or reboot. The Mabir.A is a later variant that spreads through either Bluetooth or MMS messaging. It spreads by intercepting all SMS and MMS messaging, then immediately sending an MMS message containing the virus to the initial sender. The recipient, who assumes the new infected message is a reply to the original message, must accept the download before becoming infected. Mabir.A, like the original Cabir, can also spread through Bluetooth, searching for a nearby phone to send the virus. The MMS variant is more troubling because MMS allows for the virus to be sent over greater distances and the costs for MMS messaging is higher, but the malware is still limited to one phone per activation or reboot. This will be a bigger threat for mobile payments than for mobile banking.

3.4.5.6 OTA

Over-the-air programming (OTA) allows for over-the-air provisioning or administration of new software updates or feature settings. Some phones with this ability are labeled as OTA-capable. OTA via SMS optimizes the SIM settings on a mobile device to access WAP or MMS. OTA provides a remote control for service and subscription activation, personalization or programming of new features. Various standards exist, including the Open Mobile Alliance (OMA).

3.4.5.7 USSD

Unstructured Supplementary Service Data (USSD) is a real-time or instant messaging service available on all GSM phones. If SMS is similar to e-mail, then USSD is similar to telnet. For financial institutions, it is used to query the available account balance and other similar information. USSD is not used in the United States.

III. Mobile Security

3.4.6.0 Network

Examples of a network attack would include insider (employee) of the service provider or an attacker who is able to gain access to the network. While the likelihood of an occurrence of an attacker gaining direct access to a network seems low, there are a few examples in which insider threats affected mobile phones. In 2007, Vodafone Greece was hacked. Software extensions installed on the Ericsson AXE switching equipment permitted eavesdropping on government phone calls.

3.4.6.1 GSM

More serious is the recent cracking of the encryption used on GSM in other parts of the world, but not yet in North America. Several researchers and organizations have published research showing how to break A5/1 and A5/2 encryption algorithms to intercept and decrypt traffic through such encryption. Both active and passive techniques exist; the passive technique is much harder to detect because it avoids sending any additional traffic and only listens. Third parties sell devices such as the "Passive GSM Interception System (SCL-5020)," to spy on communications when they use weak or no encryption (A5/0 and A5/2), however, the cost to hack GSM is still substantial.

3.4.6.2 CDMA

CDMA transmissions remain slightly harder to crack than GSM transmissions. That is in part because of the underlying CDMA schema that assigns each transmitter a code, then multiplexes the codes over the same channel. This allows the system to handle more users with fewer cellular towers.

3.5.0. MNO network

With the right tools, a criminal could gain access to the MNO network.

3.5.1. Transport (including gateways)

The WAP gateway converts messages from the WAP device using WTLS sent over the wireless network to SSL/TLS to be sent over the wired Internet to the server. At the WAP gateway, fraudsters could potentially view or intercept enterprise traffic or data, but the risks of such an event(s) are relatively minimal. WAP 2.0, adopted in 2002, is expected to help because the signals are sent via TLS, hence no reason to translate, no gap to mitigate.

3.5.2. Network

Like online, mobile IP networks are also subject to denial-of-service attacks. In one attack, a cable modem with 500 Kbps could be used to send data packets that would block access to more than one million mobile device users.[2] The packets themselves would:

- Re-establish connections after they have been released. This would create congestion at radio network controllers, thereby causing problems for legitimate subscribers.

[2] http://www.theregister.co.uk/2009/06/08/mobile_dos_threat/

III. Mobile Security

- Prevent a mobile device from going into sleep mode. This could overload the network with extra traffic.
- Place rogue devices on a network. This would also create spurious traffic that might be hard to locate.
- Excessive port scanning. This could be both an intended and unintended result of connected devices that are infected with computer malware.

3.5.3. Physical

Enterprises should consider mobile device management software. This allows enterprises to manage the mobile device remotely, as well as wipe the contents should the handset be lost or stolen. Such software also allows for secure VPN access to the corporate network or mail server. The software should work both ways: protecting the data on the handset should the device be lost or stolen, and protecting the network from mobile intrusions via handset activity.

IV. Security Best Practices

4.1.1. Best practices: General

Similar to URLs, most phones also convert phone numbers from SMS messages into links to easily place calls. Financial institutions may consider using phone calls as an additional verification technique. Caller ID remains an unreliable source, and better methods, such as device recognition, are preferred. It is harder to transfer transaction information over the phone; therefore, this method is not preferred for secondary verification.

Analysts should evaluate critical SMS services for SMS spoofing vulnerability and persistent log storage. Applications may choose to avoid sending full account numbers, which could reveal more information than necessary. While there are attacks that allow the attacker to intercept messages, spoofing is another more likely problem that could impact applications when they act upon fraudulent information. Applications can perform handshakes or two-factor authentication with other protocols such as OTP, e-mail and telephone. While SMS has some threats, none of them are significantly more risky than e-mail, which many financial institutions use for validating transactions. In addition to the user advice to avoid trusting fraudulent messages, service providers can filter messages. The following sections discuss controls available to SMS gateway providers to prevent spam and spoofing.

4.1.2 Best Practices: Handset

Client applications can be one of the most secure mechanisms for conducting critical transactions but could still contain vulnerabilities or be subject to mobile threats. Authors have more control of network protocols and options to use encryption. They can destroy temporary data and encrypt locally stored sensitive data. Critical applications may allow organizations to support special functionality such as profiling and registering a device and verifying the system integrity. Certain features may be available through the operating system rather than through a custom-designed application. While such control is potentially beneficial, it requires investment in multiple operating systems and platforms. Maintenance and development costs may be higher than other solutions and require more support.

4.1.3. Best Practices: Network

Many ISPs automatically attempt to limit phishing and fraud to mobile devices because they bill users per message. Providers may decide to block a known SMS gateway provider because attackers commonly use them to send spam or spoofed messages. Similarly, SMS service providers may monitor message contents and work with financial institutions to prevent such messages from reaching end devices. The current state of SMS filtering can help organizations that reach out to service providers to prevent threats at the network level

IV. Security Best Practices

rather than at the devices themselves. However, SMS filtering may add latency and involve regulatory requirements around data storage.

Several options are available at SMS and e-mail gateways to limit spam, spoofed messages or otherwise unwanted messages. Network options include:

- End-user block lists
- Whitelisting
- Content-based detection
  - Regular expressions
  - URL reputation
  - Source SMS/phone number
- Legal action
- Limit outgoing spoofed messages

Many of the controls to prevent unwanted SMS messages are reactive and filter incoming or outgoing messages. Some providers allow users to block specific organizations or numbers manually through an SMS or HTTP interface. These approaches are less reliable than SMS gateway controls because they depend on the user to block each message after it arrives and do not prevent spoofed messages.

Gateways also monitor the volume of SMS messages they send and receive. In this way, they limit fraudulent messages and identify when actors attempt to contact large numbers of inactive recipients. Contacting inactive recipients can indicate a user who is sending messages to every possible recipient. Messages originating from premium numbers are another type of message that some SMS gateway providers may filter. This prevents actors from sending messages from premium numbers because users incur bills when they reply.

E-mail-to-SMS gateways also have many controls to prevent abuse. They accept messages from e-mail accounts and forward them to SMS recipients. Traditional filtering techniques for e-mail such as Sender Policy Framework, block lists, open relays and message attributes are all ways that e-mail-to-SMS gateways limit unwanted SMS messages.

SMS gateways also have the ability to allow known good services to send messages. Financial institutions that use SMS services can make information public, which allows gateways to confidently whitelist their services.

IV. Security Best Practices

4.1.3. Best Practices: Customer Security Awareness

The techniques to spread viruses and worms on mobile platforms to date are limited. Attackers generally do not use exploits to install mobile malicious code on phones but depend more on social engineering or physical access to install malicious programs. In those cases, educating users about potential threats, operating system features, code signing, and encouraging users not to install software from unofficial sources can help mitigate the threats. Additionally, users must update mobile phone operating systems and software to take advantage of the most recent security features that reduce their risk of being a victim to malicious mobile code.

Spoofed messages could entice users to take an unwanted action or reveal personal information. Users should review official documents showing how the providers plan to communicate with them to prevent themselves from becoming victims and to help them identify fraudulent messages.

V. Conclusions

Despite the move by many carriers to provide unlimited text and data plans, many customers project their banking experiences with phishing and malware in the online channel onto the mobile channel. That is incorrect. There are some significant differences, and some additional safeguards, present in the mobile channel. If implemented, the mobile channel can be safer than the online channel for commerce and financial transactions.

By working together, the handset manufacturers, operating system vendors and browser vendors can enable security features and disable additional controls by default. In turn, the network provider can work with the browser and financial services software vendors to ensure that secure communications can be provided between clients and servers. Finally, user education is the best way to mitigate the threat of mobile viruses. As malware moves away from requiring user interaction, however, additional anti-malware protection for the mobile on the handset may be necessary.

Although the mobile threat landscape remains relatively quiet compared to its online cousin, the potential for fraud to enterprises still exists in the form of phishing, smishing, and vishing. Here, network providers may decide to block a known SMS provider because attackers commonly use them to send spam or spoofed messages.

Additionally, the growing adoption of full-featured smartphones will increase the risks of cross-site scripting and cross-site request forgeries, the current bane of the online world, as attackers find new ways to push out malicious commands to mobile browsers. Here, use of URL filtering, phishing toolbars, and SSL or EV SSL certificates in future mobile browsers should mitigate this threat.

VI. Glossary

3G: 3rd generation of mobile technology standards, which allows wireless carriers the ability to offer a wider range of services by achieving greater bandwidth; cellular networks advance to support high-speed Internet access and video conferencing through HSPA (High Speed Packet Access) data transmission.

API (Application Programming Interface): Set of procedures allowing compatibility between applications and operating systems (mobile).

Application: See **Downloadable application.**

ASP (Application Service Provider): An organization that hosts software applications using the software-as-a-service (SaaS) model.

Authentication Factor: A piece of information used to verify a person's identity for security purposes, commonly known as "something you know, something you are or do, and something you have."

Browser-based: Mobile Web sites similar to Internet sites that allow for viewing through a mobile browser (Also referred to as Browser-based /Thin Client/WAP site).

Cache: A block of memory for temporary storage of data, originating from somewhere else.

CDMA: Code Division Multiple Access, a wireless protocol used in 2G (second generation) and 3G (third generation) wireless communications that allows many signals to occupy a single transmission channel (used in ultra-high frequency channels such as 800 MHz and 1.9 GHz).

Code Signing: Applications (code) can be digitally authenticated (signed). For example, Windows Mobile offers code signing.

DNS Cache Poisoning: To access the Internet, usually a computer uses a DNS (domain name server) server that is provided by the user's own Internet Service Provider (ISP). The DNS contains a small amount of information cached by previous users. By exploiting a flaw in the DNS, attackers replace this data with incorrect data, and the DNS serves up the incorrect information to users requesting the same information (a type of MITM attack). For example, the attacker can send users to a false Web site to download malware.

Downloadable application: Special programs that can be downloaded to the customer's mobile device that allow for mobile banking. (Also referred to as Downloadable application/Application/Rich Client/Thick Client.)

FFIEC: Federal Financial Institutions Examination Council

GSM (Global System for Mobile Communication): Standard for mobile phones allowing for international.

HTTP: Hyper Text Transfer Protocol, an Internet communications transfer protocol; the request-response standard between a client and a server.

VI. Glossary

IM: Instant messaging, a form of real-time communication over the Internet based on typed text.

IVR: Interactive voice response, a type of phone technology that allows a computer to detect voice and touch tones to relay information automatically.

Key-logger: A stealth application that monitors and records each keystroke a user makes.

Man-in-the-middle attack: Attack that intercepts legitimate communication between two entities, such as a bank and a client. While the attacker has the intercepted communication, it can change the communication or even redirect it to a new site that the attacker controls. Typically, the two entities have no idea the man-in-the-middle exists.

Man-in-the-browser attack: A Trojan designed to intercept and manipulate data flowing between a browser and a site's security. Most commonly these Trojans are used to commit financial fraud.

MFA: Refer to **Multifactor Authentication**.

MMAP: Mobile Messaging Access Protocol, a protocol for sending SMS messages

MMS: Multimedia Messaging Service, standard for sending multimedia objects (rich text, video, audio and images) over wireless telephones similar to SMS.

MNO: Mobile Network Operator, also known as carrier service provider or wireless service provider.

Multifactor Authentication: Using at least two factors for authorization for security; e.g., for financial institutions; MFA is mandated by the FFIEC for Internet banking.

OATH: According to the organization, "an industry-wide collaboration to develop an open reference architecture by leveraging existing open standards for the universal adoption of strong authentication."

OTA: Over the air, that is, transmitted wirelessly.

OTP: One-time password; by constantly altering the password, the risk of unauthorized intrusion is lessened.

PKI: Public Key Infrastructure, a cryptographic secure key exchange to authenticate and download an account.

PKI Public Key Cryptography: Type of asymmetric cryptography in which the key used for encrypting a message differs from the decryption key.

Platform: Hardware architecture or software framework that allows software to run, e.g., an operating system is a platform.

Phishing: The practice of sending false e-mails that typically look like they came from a legitimate business, requesting private information, often via a click-through to another Web site that the crook has set up to look legitimate, but which is actually harvesting information.

VI. Glossary

Pharming: A hacking attack that redirects a Web site's traffic to another, false Web site.

Pretexting: The action of obtaining private personal information under false pretenses, often done over the phone, using prior information to gain new information, such as using an account number to gain a Social Security number.

PSKC: The standardization of the seed token by the Internet Engineering Task Force (IETF), known as Portable Symmetric Key Container. This will allow any vendor to seed its token with any other vendor's seed.

Redirects: Sending users to a Web site that impersonates another site. For example, making main pages available under many different URLs has opened up redirect vulnerability. URL redirects are often used in phishing attacks.

SHTTP: Secure HTTP, an extension to HTTP protocols to send secure communications over the Web.

SaaS (Software as a Service): A software application hosted by an ASP and accessed by users over a network, often employing a subscription or pay-per-use business model.

SDK (Software Development Kit): Programming tools to allow software engineers to build applications for a certain device or operating system (i.e. mobile devices, mobile device operating system).

SMS (Short Messaging Service): Communications channel allowing the exchange of short text messages.

SMS Text Banking: Mobile banking performed over the SMS text network, which is available on 100% of mobile phones, but is limited to 160 characters. (Also referred to as Text Banking/SMS Text/SMS Banking.)

SMTP (Simple Mail Transfer Protocol): Standard for e-mail transmissions over the Internet, text-based protocol.

SSL (Secure Sockets Layer): An encryption standard used to provide secure communications over the Internet for applications such as Web browsing, e-mail, instant messaging, and other data transfers.

SMPP: Short Message Peer-to-Peer Protocol, a standard for SMS messaging, which allows for priority routing, notification of failed and successful deliveries, and for return receipt.

SMS: Short Messaging Service, a communications protocol allowing for short text messages between mobile devices.

Sniffing: Computer software or hardware that intercepts and logs traffic passing over a digital network or part of a network.

SSL: Secure Sockets Layer, encrypts the data communications layer for mobile, the predecessor to TLS.

VI. Glossary

TLS: Transport Layer Security, cryptographic protocols for sending messages and data over the mobile Internet.

Trojan: A Trojan is a program that performs illicit activity when it is run. It may be used to obtain personal information and allow a fraudster to take control of the computer from a remote site.

UDLAPs: User-Defined Limits and Prohibitions, customer-driven alerts and prohibitions.

Vishing: The practice of using social engineering and VOIP or landline telephoning to obtain access to private personal data for financial gain.

VoIP: Voice over Internet Protocol, transmission technology that allows for delivery of voice over the Internet.

VPN: Virtual Private Networks are where some of the links between nodes are carried by wireless connections or virtual systems, such as the Internet, instead of by wires.

WAP (Wireless Application Protocol): An open standard for applications on mobile devices to communicate with servers over the Internet. WAP sites are Web sites written in WML (Wireless Markup Language) and accessed via a mobile browser.

WAP Site: See **Browser-based.**

WAP Gap: At the WAP gateway, WTLS transmissions are decrypted and then re-encrypted as SSL/TLS, exposing the data during the process.

WML (Wireless Markup Language): Based on XML (programming language for converting documents to be viewed over the internet), used for writing WAP browser sites.

WTLS (Wireless Transport Layer Security): The security layer of WAP, WTLS enables encrypted communications between mobile browsers and servers over the Internet.