

Mobile Security Whitepaper

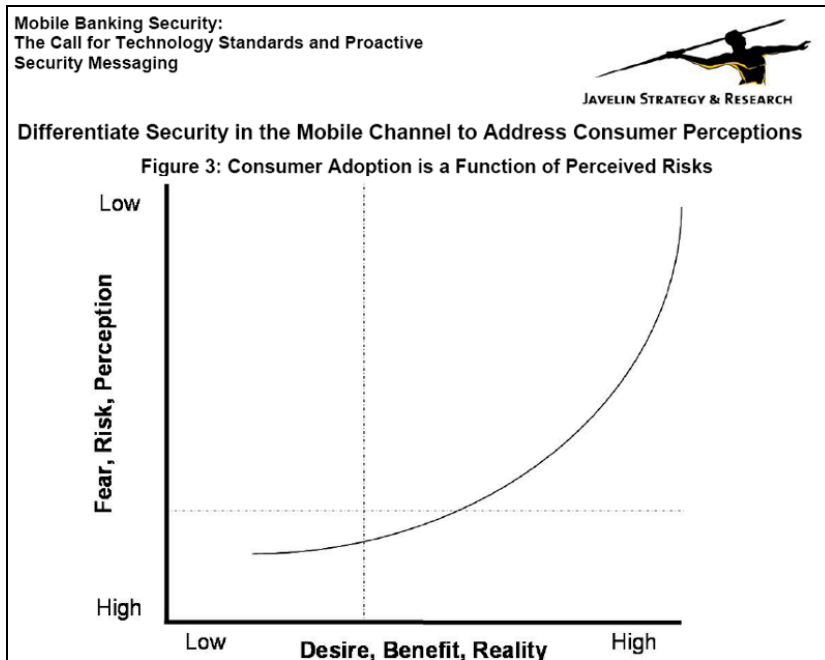
February 15, 2008



David Eads
mFoundry
deads@mfoundry.com

Overview

Analysts such as Javelin Strategy & Research indicate that adoption of mobile financial services applications will accelerate as the perceived security of solutions by consumers increases.



Obviously, mobile banking systems must first actually be secure to increase the perception of security. Institutions must choose carefully to ensure that their various mobile banking offerings provide the same level of security or better as other channels such as online banking, ATM and branch networks.

Types of Attacks

Inevitably, criminals will attack mobile channels as they have every other financial services channel in the past. However, mobile channels can be as secure or more secure than existing online banking and ATM networks if the same focus on security is applied to the mobile channel.

Mobile channels are subject to many of the same types of attacks as online channels. Mobile technology also introduces some new opportunities for criminals. Institutions should protect themselves from the following types of attacks:

Snooping

Criminals can obtain and use sensitive information by simply intercepting unencrypted data. Unfortunately, many mobile solutions don't provide basic data protection mechanisms that are taken for granted in other channels.

Phishing

Criminals can trick users into sending sensitive data directly to them by posing as the financial institution. Mobile device limitations encourage typographical errors. Institutions must insure the authenticity of their software and should limit the amount of user input.

Smishing

Similar to phishing, but unique to SMS messaging, in so-called “smishing”, criminals pose as the financial institution to trick users into sending sensitive information via a text message. For example, criminals can send phishing-like SMS messages to consumers posing as a legitimate financial institution hoping that recipients will respond to their requests for sensitive information. Additionally, criminals could setup a phony SMS service with a phone number very similar to the financial institution. Similarly, Criminals could drive traffic to their phony SMS service via phishing emails.

Pretexting

Criminals can pretend they are a particular customer and convince one of your representatives to perform an unauthorized transaction or release sensitive information that allows the criminal to gain access to the user’s assets. This type of attack was made famous by the spying upon the Hewlett-Packard board by officers of the company.

Man-in-the-Middle

If a system is designed with data flowing through a single component, criminals can access all the information flowing through it if they can find a way to compromise that component. For example, if a carrier had equipment that terminated the encrypted connection from the mobile device and initiated a new tunnel to the financial institution; a criminal could gain access to the sensitive information if they found a way to compromise this equipment in the middle.

Keystroke Loggers & Spyware

Criminals can write malicious software (also known as “malware”) that captures user input and secretly sends the information to the criminal. Often users are tricked into installing malware. Sometimes malware hides within useful software the user wants (also referred to as a “Trojan Horse” attack). Sometimes the malware is a counterfeit or altered version of the real software. Institutions and users should ensure any financial software is authentic and unaltered.

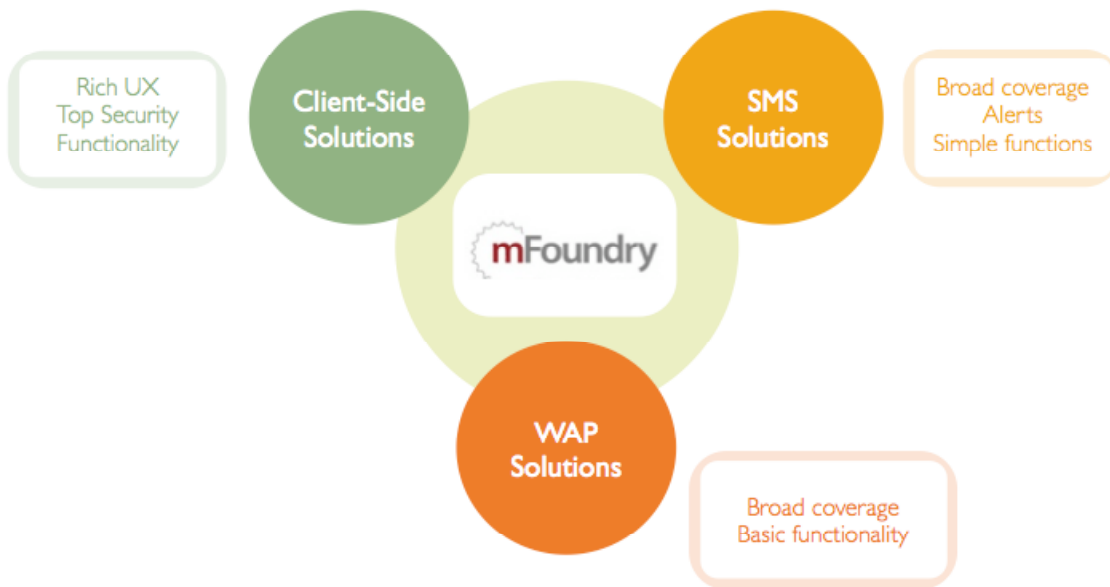
Minimum Protection

Specifically, any mobile solution must provide the following minimum safeguards:

- **Complete 128-bit data encryption.** Sensitive and personally identifiable information must never be transferred in the clear.
- **Strong authentication and authorization.** Password schemes should be as strong or stronger than online banking and ATM.
- **Sensitive data should never be stored on the mobile device.**
- **Usernames and passwords should never be stored by third-parties and/or combined across institutions.** Users should provide usernames and passwords when challenged to ensure they are authorized to access sensitive information and perform financial transactions. Furthermore if usernames and passwords are combined into a keychain, accounts at all institutions could be compromised if a breach occurs.
- **Safeguards must exist to immediately disable mobile access if a phone is reported lost or stolen.**
- **Software authenticity** – users must be absolutely certain of the source of any financial software. Therefore, software installation should occur at the users’ request preferably over a secure network connection. Preloaded software could be compromised and/or be outdated. According to Javelin, a majority of users consider software downloaded from the financial institution to be the most secure method. Software should also limit the entry of URLs and other data to reduce the likelihood of users accidentally navigating to a malicious site (e.g. “phishing”).

Types of Mobile Software Solutions

Mobile users have devices with screen, connectivity, processing speed and input mechanisms operating at a fraction of those found on a standard desktop computer. For example, the typical phone screen resolution is 1/10th the size of the average desktop monitor resolution. While mobile devices are becoming more powerful and networks faster, it is critical that the mobile experience be simple and usable even in a low performance situation. Ease of use becomes even more critical when considering the types of multitasking users do with their mobile devices, such as walking or driving.



Three types of solutions have arisen to address the challenges of mobile applications: WAP, SMS and Client-Side Solutions. Each technology has advantages and disadvantages. Accordingly, most financial institutions have chosen to seamlessly implement all three types of solutions to use each type of solution where it works best. It is important to use the right type of solution for sensitive data to avoid security risks.

mFoundry has pioneered cross-device, cross-carrier Client-Side software and is complementary to other WAP and SMS solutions. Furthermore, through a partnership with ClairMail, mFoundry and ClairMail exclusively can provide a complete out-of-the-box mobile package containing all three types of mobile technologies.

WAP Solutions

WAP (Wireless Access Protocol, also known as “Mobile Internet”) solutions provide the broadest device support and as such, often provide the quickest and easiest means to provide a very basic mobile presence. Unfortunately, although vastly improved from earlier versions, the WAP protocol remains somewhat limited in functionality and rendering control when compared to a traditional web browser. Furthermore, some security issues linger despite the improvements in WAP 2.0.

WAP also cannot take advantage of hardware capabilities of advance phones such as GPS and eventually Near Field Communication (NFC) chips for payment purposes. Therefore, WAP solutions are best suited to provide a basic mobile presence and provide a gateway to other parts of your mobile presence.

SMS Solutions

SMS (Short Message Service) solutions provide a unique asynchronous capability useful for sending balance or bill pay alerts. Like WAP, SMS messages have limited functionality due to the nature of their protocol and are not encrypted throughout the transmission. Furthermore, typing on mobile devices is notoriously difficult. User typographical errors could result in security breaches similar to “phishing” in online banking which has been dubbed “smishing”. SMS solutions are ideally used to send asynchronous alerts from the institution to the mobile devices that do not contain sensitive or personally identifiable information.

Client-Side Solutions

Client-Side solutions are applications running on the mobile device. Client-Side solutions could be a binary application downloaded to the phone or an Ajax (Asynchronous JavaScript and XML) application launched from a secure site. Client-Side solutions offer the most functionality, best user experience and the most security.

mFoundry specializes in Client-Side solutions and supports significantly more devices than any other provider. mFoundry supports almost every mobile device (140+ devices), all the major U.S. carriers, and many of the minor carriers. mFoundry also provides dynamic Over-the-Air (OTA) updates to facilitate seamless delivery and to ensure up-to-date software on the device.

Furthermore, Client-Side solutions must be carefully designed to not introduce security risks. For example, a 128-bit Secure Sockets Layer (SSL) tunnel should exist without interruption from the mobile device to the institution mobile gateway. Each transaction should also use multiple factors of authentication.

In summary, as with any system, mobile solutions must be carefully designed use the best of each technology and to ensure the security of sensitive information. Mobile systems are no less secure than other systems when implemented using the same best practices implemented in other channels such as online banking.

Common Security Issues

The following sections outline some of the more common security gaps in the various mobile solutions. These issues are all avoidable with the right product choice and proper implementation. mFoundry is the most equitable and secure mobile financial services platform and has resolved all these issues in its suite of products.

Unprotected Sensitive Data Transfer

As with any financial system, mobile banking solutions must provide strong encryption throughout the entire data path between the mobile device and the protected zone of the financial institution. Unfortunately some mobile solutions allow sensitive financial data to exist in the clear (unencrypted and unprotected) while on the carrier networks or in gateway servers.

mFoundry provides a secure, uninterrupted 128-bit SSL encrypted connection from the mobile device to the mobile gateway software hosted at secure, reputable financial institution (such as your institution, First Data, Fidelity Information Systems, NCR, PSCU, ACI and others).

SMS Security

SMS was not designed to carry sensitive information. SMS data is almost invariably unencrypted throughout much of the connection between the handset and the financial institution. Therefore, SMS solutions should be never transfer sensitive or personally identifiable information.

Smishing

Dubbed “smishing,” criminals can misrepresent themselves as someone the victim trusts, and then coax sensitive information from the victim. Mobile applications should limit the use of SMS for sensitive transactions. Furthermore, applications should find ways to verify the authenticity of the institution to the user in addition to the more traditional approach of verifying the identity and authenticity of the user to the institution.

Criminals also could set up WAP or SMS applications that take advantage of mistyped WAP URLs or phone numbers. Therefore, mobile applications should carefully limit the amount of user input and SMS messages should flow from the application to the mobile device as much as possible.

Unencrypted Sensitive Client-Side Data on Carrier Networks

Client-Side solutions such as mFoundry provide the most security between the user and the financial institution. The rich capabilities of client software running on the phone provide opportunities to enforce your existing institutional rules for challenge/response, password length and content, one-time passwords and so on.

Unfortunately, some client-side solutions insert gateways between devices and institutions. Gateways introduce a security risk because they require both endpoints (the mobile device and the financial institution) to authenticate with the gateway instead of each other, thus requiring the endpoints to simply trust that the gateway will protect the data and always send it to the appropriate location. This approach creates the opportunity for a Man-in-the-Middle attack in addition to exposing sensitive information.

mFoundry provides a secure tunnel directly from the phone to the financial institution to completely avoid this problem.

Furthermore mFoundry is the only solution to provide complete 128-bit SSL encryption throughout the communication channel from the mobile device to the financial institution. Other

solutions end SSL-tunnels at the carrier (similar to the WAP Gap), leaving sensitive information unprotected.

Password Keychains

Some mobile solutions keep their own database of user credentials for each institution the user has enabled. Surprisingly, some solutions actually outsource this critical control to the mobile carrier, which is obviously not a financial institution.

In addition to raising serious questions about responsibility and indemnification in the event of an attack, this approach introduces a number of security risks such as:

- Assets at all accounts are affected if the common keychain username and password is compromised
- The security of every institution in the keychain is reduced to the security of the weakest institution
- Keychains could allow non-financial institutions to control access to financial institutions
- Keychains prevent institutions from providing their own unique security model, in addition to ceding control to a third-party

Breach for One is a Breach for All

For example, let's say a user has mobile-enabled accounts at a bank, an unrelated brokerage house, and a third unrelated credit card company. If a criminal steals this user's phone and obtains the common keychain username and password, they would have complete ability to drain the bank account, sell all the brokerage securities and drain the assets, and free access to the line of credit on the credit card account.

mFoundry's approach is to allow the financial institution to dynamically issue its own unique combination of challenges and securely pass through the response without ever storing the credentials. Institutions select the password strength, when, and how often, and in what channels to challenge. In the event of a security breach, the only assets at risk are the ones whose credentials were lost.

Giving the Bank Vault Keys to the Phone Company

The keychain approach not only stores credentials in a second location, violating a basic security best practice, but the credentials are stored at a third-party (the mobile banking provider or even the mobile carrier in some cases). Mobile carriers have proven themselves susceptible to security breaches as witnessed in the HP pretexting case and in the cracking of Paris Hilton's phone. Telephone companies were not designed to protect financial assets. mFoundry recommends never storing user credentials to avoid this problem.

CSR Lock-out

Mobile devices are often lost. Mobile solutions must prevent lost phones from compromising security. mFoundry allows Customer Service Representatives (CSRs) to immediately lock-out a lost phone. Controlling access is easy without the keychain model because the financial institution has complete control and doesn't share access with any third parties.

CSR Lock-out can result in very complicated logistics for solutions that implement the keychain model. Since the account credentials are stored outside the financial institution, a mechanism is required to ensure the third-party cache is securely updated. Institutions and carriers must ensure this process is protected and hardened against an attack from criminals. Meanwhile, each institution may also require coordinating this process with their procedures for locking out their ONLINE BANKING channel. Institutions might also need the capability to quickly communicate these updates not only to the carrier, but to each other.

Individual Bank Security Models

Every institution has its own security policies and best practices. Often these policies and procedures reflect variations in business models, product mix and customer demographics. Many institutions view security as a competitive advantage. Each institution needs the flexibility to implement its own security approach and wants to leverage their expensive security infrastructure as much as possible. Fundamentally, institutions should protect each channel (ONLINE BANKING, ATM, Branch, IVR, and mobile) equally, because criminals will exploit the weakest link.

Unfortunately, many mobile solutions provide few or no options for institutions to implement their own security model in their mobile channel.

mFoundry provides institutions great flexibility in implementing their own unique security models and extending their business model to their mobile presence. mFoundry supports leveraging your investment in Strong Authentication and supports multichannel authentication. For example, an institution could choose to present additional, multichannel challenges when users attempt large or uncharacteristic transactions.

mFoundry is even taking Strong Authentication to the next level by providing capabilities for the mobile device and the server to challenge each other at the application layer to further ensure authentication and secure communication.

Risks of Preloaded Software

Some vendors preload software onto phones. Preloaded software introduces some risks. First, preloaded software is almost certainly out-of-date by the time it reaches the consumer. Out-of-date software may no longer communicate properly to newer versions of software at the institution. Furthermore, a distribution model that relies on preloading software, has no way to remove bugs from software in the carrier inventory or on consumer handsets.

Secondly, consumers cannot confirm the authenticity of preloaded software. Anyone with access to the device at the carrier or phone store could replace the correct software with criminal software (e.g. spyware) that gains access to the consumer's assets.

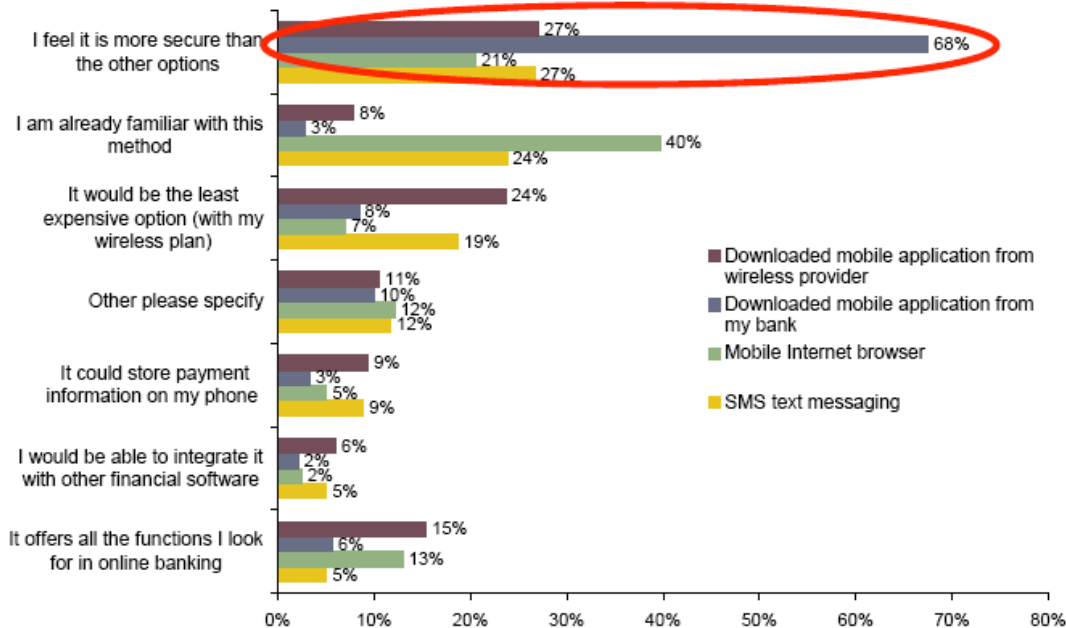
mFoundry lets you easily provide safe software to your customers. The default process is to send a text message to the customer's device from your online banking system when they request access to mobile banking. The text message contains a link to your software. The software is downloaded and installed automatically when the user selects the link. When the user opens the software they are challenged to provide a one-time authorization code displayed in their online banking account, in addition to their username and password. Of course, you can customize this default process to fit your security model.

**Mobile Banking Security:
The Call for Technology Standards and Proactive
Security Messaging**



Consumers Perceive Bank-Provided Downloadable Application as Most Secure

Figure 9: Majority of Security-Concerned Consumers Prefer Application from Bank



Q33: What was your primary reason for choosing the option you selected above? (Select one only) by Q32: Given the following choices how would you prefer to access your accounts on your mobile phone? (Select one only)

n = 2,230
Base: All consumers
© 2007 Javelin Strategy & Research

Summary

Mobile banking can be as secure as any other financial service channel. Unfortunately institutions must choose their solutions carefully. Some solutions introduce security risks that render them unsuitable for use with sensitive information.

Financial Institutions and regulatory bodies must pay close attention to how mobile systems are architected. Sensitive data must be protected throughout the transmission. Institutions should also leverage their investments in Strong Authentication and multichannel authentication technologies to harden the implementation.

Criminals will challenge even the best implementations. However, as an industry we should take advantage of all we have learned in other electronic and alternative delivery channels to protect consumers and our assets.