FEDERAL RESERVE
BANK OF BOSTON™

The Future of Mobile Security: Understanding the Risk Environment for Mobile Payments

Summary Report of January 29-30, 2013 Mobile Payments Industry Workgroup Meeting

Susan Pandy, Federal Reserve Bank of Boston

October 18, 2013

The views expressed in this paper are solely those of the author and do not reflect official positions of the Federal Reserve Banks of Atlanta or Boston or the Federal Reserve System. The authors would like to thank members of the MPIW and panelists for their thoughtful comments and review of the report.

I. Introduction

The introduction of mobile technology is redefining the payment system, with new stakeholders such as wireless carriers, mobile application developers, mobile operating system providers, and new ways to conduct payments and related services electronically. The payments industry needs to understand the benefits and risks, particularly as they relate to the security and safety of the payments system and the impact on consumers. If implemented effectively, mobile payments can be more secure than payments made in the traditional e-commerce environment. This can be done by leveraging some of the unique functions of the device for enhanced authentication, such as the camera, GPS, voice, etc. The data that can be gleaned from a mobile device should also lead to enhanced risk management. As smartphone adoption continues to rise and consumers conduct more financial transactions using mobile devices, security becomes paramount.

In January 2013, the Federal Reserve Banks of Boston and Atlanta convened a meeting with the Mobile Payments Industry Workgroup (MPIW) and several experts in payments security and risk management to discuss issues, challenges, and opportunities for building a mobile channel that can support the emergent mobile payments landscape. The meeting was comprised of two panels. The first panel, led by a software security services company and a risk management think tank, focused on potential risks in the retail point-of-sale (POS) environment. The second panel included an authentication technology vendor, a mobile security and forensics vendor, and an information technology, risk and compliance auditor, who discussed their perspectives on mobile security threats and mitigations.

The objective of this white paper is to highlight some of the potential vulnerabilities of mobile payments at the retail POS and how to mitigate these threats to create a safer and more secure mobile payments environment. The topics in this paper are based on the respective panels. They include a review of (i) hacking and other potential vulnerabilities to the POS system, (ii) security measures for POS terminals, (iii) the risk model for mobile payments, and (iv) the need to reinvent strong authentication.

II. Hacking and Potential Vulnerabilities to the POS System

Karsten Nohl, [1] a well-known cryptographer and security expert, discussed his views on retail POS payments. He described his research that showed vulnerabilities which led him to predict that terminals

[1] Karsten Nohl is a German cryptographer well-known for his research of potential payment fraud stemming from encryption and software in SIM cards and POS terminals in Germany. His hacks have been discussed at events such as the Black Hat annual hackers conference. For more information about some of his recent hacks see: http://www.nytimes.com/2013/07/22/technology/encryption-flaw-makes-phones-possible-accomplices-in-theft.html?_r=0 and http://www.forbes.com/sites/parmyolson/2013/07/21/sim-cards-have-finally-been-hacked-and-the-flaw-could-affect-millions-of-phones/.

in merchant locations will be the focus of attacks in the future. He also explained findings from recent research conducted by the University of Cambridge, which showed that POS terminals in Europe might be remotely infected to perform EMV "pre-play" [2] attacks. However, he admitted that such vulnerabilities to POS terminals in Europe are likely enhanced by the absence of incentives for both merchants and POS terminal providers[3] to prevent fraud (because the liability is with the consumer) and the lack of enhanced trust relationships in the ecosystem.[4] While vendor rules in the U.S. and Europe are similar, terminals in the U.S. that are subject to compromise tend to be those that belong to smaller merchants and are noncompliant with industry security requirements that can prevent such attacks. Furthermore, the probability of such attacks is very low and upon learning of these vulnerabilities, the industry moves quickly to address them.

Nohl added that certified payment terminals in Germany lack many of the protections available for smartphones. He explained that smartphones contain multiple protections for hardware (e.g., secure boot, hardware key store, debug modes disabled),[5] the operating system (e.g., sandboxing, memory randomization, signature validation),[6] and in the software (e.g., source code analysis, modern

[2] In a pre-play attack, if the attacker is able to physically collect and analyze transactions, or collect them by infecting a terminal (ATM or POS) with malware, or by a man-in-the-middle attack between the terminal and the acquirer, that sends the data remotely, he can save the authentication data from a particular time and re-use it at a later time pre-determined by the counter. In effect, pre-play attacks allow criminals to send fraudulent transaction requests from rogue chip-enabled credit cards. See Bond et al. (2012) [Working Paper] *Chip and skim: cloning EMV cards with the pre-play attack.* University of Cambridge, UK, accessed from http://www.cl.cam.ac.uk/~rja14/Papers/unattack.pdf.

[3] Terminal manufacturers in Germany are not incentivized to provide security protections, such as security patches for POS terminals.

[4] Trust in smaller merchants is lacking because they tend to avoid or delay the necessary upgrades to their POS terminals, or to ensure that the proper security controls are in place. On the other hand, trust may be equally lacking in the financial institutions that may authorize transactions from suspect accounts.

[5] A *secure boot* is a mechanism that enforces that only authenticated programs and/or events are executed on a particular platform and can prevent such things as malware from loading during the system start-up process. A *hardware key store* keeps keys on specialized hardware tokens such as a USB token or smart card and reader. The key cannot be used without the user's password. *Disabling the debug modes* refers to switching off the mechanism by which the chip can be externally controlled and its memory, including secret keys, read out.

[6] *Sandboxing*, *memory randomization*, and *signature validation* are part of the multi-layer security protections for mobile operating systems. *Sandboxing* is an approach to software development and mobile application management that limits the environments in which certain code can execute. One goal is to improve security by isolating an application to prevent outside malware, intruders, system resources, or other applications from interacting with the protected app. Source: http://searchconsumerization.techtarget.com/definition/application-sandboxing. Another goal is to isolate apps before release in a self-contained environment mimicking the real implementation. After an app is vetted and proven not to alter the existing infrastructure/device it will operate on, it is removed from the sandbox. *Memory randomization*, a.k.a. space layout randomization (ASLR), ensures that the memory regions of mobile apps and system shared libraries are all randomized at device and application startup. This limits exposure to memory corruption bugs, and effectively reduces exploitation attempts by malware vendors. In effect, this tool makes it hard to predict where something will be in memory. Source: http://www.rdacorp.com/2012/08/mobile-application-development-security/. *Signature validation* is necessary to ensure that all digital signatures on software components and applications come from a trusted source and have not been modified. If the OS does not validate these digital signatures, then there is the potential for malware to infiltrate the device. Validating digital signatures ensures that the digital signature control properly mitigates the risk that malware will be installed or execute on the system. Source: http://www.stigviewer.com/check/V-33202.

programming language).[7] The payment terminals he studied only have two of these protections – a hardware key store and signature validation.

Nohl suggested two possible mitigations against vulnerabilities at the retail POS: (1) to encrypt card data and communicate it directly to the bank during the transaction, eliminating the POS terminal in the middle; and (2) to consider a zero–trust framework that could be achieved by applying end-to-end security, which includes adding cryptography to legacy systems or locking down the hardware.[8] MPIW members added that the industry needs to maintain a focus on infrastructure (security) around authorizations and update this focus from the traditional e-commerce approach.

III. Security Measures for POS Terminals

The next discussion focused on security measures that exist to protect POS terminals from vulnerabilities, such as viruses that can steal tokens from terminals and, in doing so, spread the virus to other terminals. MPIW members and panel experts discussed whether or not current industry standards adequately address POS terminal threats and protect terminals.

MPIW members noted that past breaches, which involved compromised PIN pad devices, occurred because these devices did not have point-to-point encryption. The PCI Council[9] has since issued requirements for point-to-point encryption so newer terminals will prevent these attacks. However, the biggest vulnerability once again rests with smaller merchants that have chosen not to update their outdated terminals with adequate security controls.

MPIW members maintained that the PCI Payment Application Data Security Standard (PA-DSS)[10] provides a robust infrastructure that secures terminals and noted that the certification standards for terminals and vendor certification requirements have become more stringent. The PCI Council has written guidelines for mobile POS devices that act as card readers to accept card payments (mPOS), but has not yet published any requirements to address POS terminals that accept consumer-initiated mobile payments or taken any action towards certifying mobile devices or mobile payment applications. The PCI

[7] *Source code analysis* tools are designed to analyze source code and/or compiled version of code in order to help find security flaws. Source: https://www.owasp.org/index.php/Source_Code_Analysis_Tools. *Programming languages* are used for controlling the behavior of a machine. An example of a modern programming language is JavaScript.

[8] The zero trust framework is a new security approach which calls for the inspection of all network traffic both inside and outside in real-time. For more information, See *No more chewy centers: Introducing the zero trust model of information security*, accessed from http://www.forrester.com.

[9] The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements. For more information, see https://www.pcisecuritystandards.org.

[10] See https://www.pcisecuritystandards.org/security_standards/documents.php?association=PA-DSS.

Council is currently reviewing the impact of mobile on POS terminals (and on the application side) and how the industry can create a more streamlined, trusted environment, while it maintains support for and continues to discuss point-to-point encryption.

Compliance with PCI standards will help to manage card data breaches, but the significant investment required by the retail community must be factored into implementation.

According to some panelists, the industry needs to modify its approach to addressing mobile payment data breaches by focusing more on preventing hacking events and less on audit-based checklists before broad mobile standards can be developed. By gaining an understanding of the risks across different use cases and how the mobile payment transactions flow, industry security specialists could develop better mitigation controls and reduce reliance on audit-based checklists.[11] This analysis would build a foundation on which mobile payment standards could then be developed.

IV. Assessing the Risk Model for Mobile Payments

Several security technology providers, including a security audit company, discussed the risk model for mobile payments. They noted that security vendors do not focus on the payment method, but rather look for ways to mitigate the threats that apply to the end-to-end transaction.

The participants pointed out the top three mobile risks: 1) the vulnerability of mis-developed mobile apps; 2) mobile device services; and 3) insecure storage. Each of these risks is described in more detail below.

Mobile Apps: Legitimate mobile apps can be undermined by rooting (Android OS) or jail-breaking (Apple iOS) and malware. Rogue mobile apps can exploit vulnerabilities in the major mobile operating systems (OS) which have become a target for mobile malware. The level of vulnerability to each OS stems from the difference in how each platform controls its vendors and the respective marketplace for development and distribution of apps.[12]

Mobile apps may be vulnerable if, for example, a consumer uses the WiFi in a local coffee shop and inadvertently connects to a fraudulent WiFi. The fraudster becomes the man-in-the-middle and steals the consumer's bank log-in credentials when she logs into her bank's mobile app. As a potential solution, panelists suggested that the security vendor encrypt the bank app and the contents of the message before it

[11] The panelists were discussing the benefits of actively developing solutions to combat future fraudulent attacks versus the auditing approach. Auditing based on industry standards tends to only capture security practices in a moment in time versus a longer term solution to fraud prevention based on an enhanced understanding of the technology, risks, and threat scenarios.

[12] While iOS is not completely invulnerable, the number of threats to Google Android has continued to increase. SophosLabs. 2012. *Security Threat Report 2012*, accessed from http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf.

is handed off to the https channel. When the fraudster intercepts and unwraps the message being transmitted from the consumer to the bank, the message remains encrypted.

Mobile Device: The mobile device has a number of unique characteristics that warrant a different risk model than the online environment. The mobile device is portable (i.e., it can be lost), leverages converged communications (e.g., SMS, video, email, voice), and may be susceptible to rogue apps.[13]

Insecure Storage: Many mobile devices store a plethora of sensitive information that, if not properly secured, can be compromised and lead to fraudulent activity. Panelists suggested not storing sensitive information inside the device. If local storage is required, the data should be encrypted.

A key feature of the mobile device is the ability to protect sensitive data, such as payment credentials, either in a secure element chip (SE) in the phone or by housing this sensitive information in the cloud (on a remote server) and accessing the data using secure tokenization technology.

The panelists agreed that there is a big opportunity to leverage the mobile device and apps to mitigate fraud. For instance, they believe that the industry may see a rise in application level encryption, as well as a move towards a cloud-based environment in which only the user and her/his actions are authenticated.

Use of the cloud for digital/mobile payments is still relatively new. Cloud service providers and businesses should review how payments data is securely stored in the cloud.[14] They should develop strong risk management practices to prevent intentional and unintentional data leakage between cloud environments, and avoid data breaches that may cause financial fraud loss, reputational/brand damage, privacy exposure, etc.

Panelists also noted that some mitigation tools, such as biometrics and out-of-band authentication, have been around since 2002 and should be re-assessed. Biometrics, in particular, may be witnessing resurgence. For example, Apple's new iPhone 5S includes a fingerprint sensor to activate the mobile device.

[13] Various mobile operating systems have had fraudulent apps that appear in their stores and are downloaded by unsuspecting users who downloaded seemingly innocent services, such as horoscopes, wallpapers and games. These forecasts and other apps have been ploys for criminals to lure consumers into clicking on options that led to premium charges tied to SMS usage. Fraudulent apps can also introduce malware to mobile device operating systems.

[14] In July 2013, The Clearing House announced its Secure Cloud pilot with several participating banks. The pilot is scheduled to begin in fourth quarter 2013 and run through the summer of 2014. The pilot aims to create an open standard for the payments industry that will replace mobile-wallet users' cards and other account information with randomly generated, one-time tokens, or strings of digits. For more information, see http://www.americanbanker.com/issues/178_125/banks-to-heighten-mobile-wallet-security-by-walling-off-data-1060305-1.html.

V. Mobile Payments is Driving the Need to Reinvent Strong Authentication

Industry experts agreed that authentication is the key to addressing the payments security environment (whether it is online, POS, or mobile) and protecting mobile payment users and service providers. The payments industry has not effectively addressed e-commerce authentication and has the opportunity to improve mobile payment security with enhanced solutions for strong authentication.

Two industry groups are working to address the problems that users face creating and remembering multiple usernames and passwords: the Fast Identity Online (FIDO) Alliance[15] and the Initiative for Open Authentication (OATH).[16] FIDO's goal is to change the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. This proposed standard for security devices and browser plug-ins will allow any website or cloud application to interface with a broad variety of existing and future FIDO-enabled devices that the user has for online security.

OATH has developed a roadmap for designing an open architecture to authenticate every user and every device, on all networks, using any strong credential. OATH's objective is to make strong authentication ubiquitous through the collaborative development of an open authentication specification that can be adopted across the industry. The OATH roadmap contends that the trustworthiness of an identity depends on multiple factors: 1) the initial authentication process (identity verification); 2) the type of credential being issued (security token); and 3) the depth of the relationship between the authenticator and the authenticated entity.[17]

The new security environment for mobile includes the use of cloud-based services (remote servers) to securely store and/or access payment information. Cloud-based strong authentication services have emerged to provide a cost-efficient approach, particularly for smaller companies, because they do not require upfront software or hardware investments. Hardware tokens, while they provide high levels of security, are expensive to purchase, distribute to users, and manage. New types of authentication form factors are now available, such as software tokens, SMS tokens, and non-token-based authentication

[15] The FIDO alliance is comprised of several companies that include Lenovo, Infineon, Agnitio, PayPal, Validity, Google, and others representing enterprises, consumers, device Original Equipment Manufacturers (OEMS) and token vendors. For more information, see http://www.fidoalliance.org/.

[16] See http://www.openauthentication.org/.

[17] See www.openauthentication.org.

methods. These new options will allow strong authentication to be extended to a wider range of environments, including mobile devices and online portals.

VI. Conclusion

The adoption of mobile payments in the U.S., particularly at POS, is still early in its life cycle. There is sufficient time to analyze potential threats and vulnerabilities, and develop/implement effective mitigation tools, including the use of the mobile device itself. However, this effort requires industry collaboration to identify weak points and develop ubiquitous security solutions that address the biggest risks.

The MPIW will form a workgroup to identify potential gaps in standards, document best practices, and determine the need for industry guidelines and/or provide recommendations to formal standards bodies. The effort will include:

1) Analyzing several mobile payment use case scenarios to identify the attack vectors, threats, vulnerabilities, mitigations, and controls for each:
   - Compare cloud vs. mobile device storage and mitigation steps
   - Compare software versus hardware-based security solutions
   - Develop a risk management assessment framework to compare the risks and mitigations of the different use cases and list the hardware/software used in each scenario
2) Publishing a report based on the analysis that identifies key security areas that mobile payment stakeholders can address collaboratively or individually, and related guidelines

The objective will be to provide a framework within which stakeholders can work to build common solutions in a changing technology environment, and to provide education and awareness, not only to industry stakeholders, but also to policymakers and, ultimately, consumers to help drive consumer adoption regardless of the technology platform.

Appendix

Moderators

Steve Mott, BetterBuyDesign

BetterBuyDesign is a payments system consulting firm that leverages the expertise and experience of Steve Mott, an acknowledged pioneer in eCommerce, and a syndicated group of experts with extensive credential in transactional systems. In many instances, BBD provides “idea brokering” between advanced technology products and services between small, high-tech firms and large corporations seeking to deploy competitively advantageous services in online and mobile environments. A particular focus of this idea-brokering is on fostering the development and adoption of innovative transactional environments–especially creating new payment options. BBD also performs a wide gamut of traditional management consulting services–from strategy review and development to due diligence for merger and acquisition events and related business development activities.

For more information visit: http://www.betterbuydesign.com.

Seb Taveau, CTO, Validity

Headquartered in San Jose, California, Validity is the world leader in Natural ID authentication, providing fingerprint sensors with the highest levels of performance, security, cost-effectiveness, and design flexibility. Validity’s patented LiveFlex® fingerprint sensor technology enables authentication, mobile payments, and touch-based navigation for smartphones, tablets, and notebook computers. For the latest news on biometrics and authentication, read the Natural ID blog by Validity CTO, Sebastien Taveau.

For more information visit: http://www.validityinc.com/.

Panelists

Peter Tapling, CEO, Authentify

Authentify, Inc. is the leading innovator of global phone-based, out-of-band authentication services and was recently ranked as a visionary by Gartner. These services enable organizations that need strong security to quickly and cost-effectively add 2-factor or 3-factor authentication layers to user logon, transaction verification, or critical changes such as adding a payee to an e-pay or wire account. The company’s patented technology employs a service-oriented message architecture and XML API to seamlessly integrate into existing security processes. Authentify markets primarily to financial services firms that need to protect their clients’ online accounts, corporate security professionals managing corporate access control, and e-merchants who want to limit fraud on their sites.

For more information visit: http://www.authentify.com/.

Joel Scambray, Cigital

Cigital, Inc. is the world’s leading software security services and solutions company. Cigital helps public and private organizations launch and mature software security initiatives, as well as design, build, test, and maintain secure software through a combination of expert consultants, innovative technologies, and effective training built on over twenty years of cutting-edge research and successful client engagements. Cigital is headquartered outside Washington, D.C. with regional offices throughout North America, Europe, and Southeast Asia.

For more information visit: http://www.cigital.com.

Rick Dakin, Coalfire

Coalfire is a leading, independent information technology Governance, Risk, and Compliance (IT GRC) firm that provides IT audit, risk assessment and compliance management solutions. Founded in 2001, Coalfire has offices in Dallas, Denver, Los Angeles, New York, San Francisco, Seattle, and Washington D.C. and completes thousands of projects annually in retail, financial services, healthcare, government, and utilities. Coalfire's solutions are adapted to requirements under emerging data privacy legislation, the PCI DSS, GLBA, FFIEC, HIPAA/HITECH, HITRUST, NERC CIP, Sarbanes-Oxley, FISMA, and FedRAMP.

For more information visit: http://www.coalfire.com/.

Karsten Nohl, Security Research Labs

Security Research Labs is a risk management think tank in Berlin, Germany supporting IT security strategy at Fortune500 companies. SRLabs' research is concerned with hacking devices in payment, communication, and utility infrastructures.

For more information visit: https://srlabs.de/.

Ted Eull, viaForensics

viaForensics is an innovative mobile security and forensics firm known for cutting-edge mobile R&D. Areas of focus include mobile device and app security products and services, as well as mobile forensics software and training. As leading experts on Android and iPhone forensics, viaForensics has developed a suite of unique products and services to serve the mobile and enterprise security needs of corporations and government agencies.

For more information visit: https://viaforensics.com/.