Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Smartphone Financial Transactions: Security Risks and Control Options

CAPSTONE 1 Bibliography

Andrew Keys
Sr. Manager Software Engineering
Bank of America

University of Oregon
Applied Information
Management
Program

December 2013

Academic Extension
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

Dr. Linda F. Ettinger, Capstone Instructor

Dr. Kara McFall, Capstone Instructor

Smartphone Financial Transactions: Security Risks and Control Options

Andrew T. Keys

Bank of America (eCommerce)

Abstract

Table of Contents

Introduction

Statement of the Problem

August 29, 2007 is a date that will be marked in history as the official launch of the Apple iPhone. The iPhone is a brand of smartphone (cellular or cell phone), able to perform many computer functions, and includes an operating system capable of running general-purpose applications. As noted by Wilcox (2007), the iPhone isn't just a device, it's a community. Google also launches Android in November 2007 for support of smartphone hardware ("Our history in depth," 2013).

The increasing popularity of the smartphone raises many security concerns (Lawton, 2008). Companies providing smartphone native and web applications are increasingly exposing their customers to security risk and need to help prevent attacks and educate customers on security concerns (Wang, Streff, & Raman, 2012). Their ability to host operating systems like iOS and Android provides a platform for viruses (Banuri, Alam, Khan, Manzoor, Ali, et al., 2012). In the last seven months of 2011, malicious software (called *malware*) attacks on the Android platform increased 3,325 percent (Wang et al., 2012). The rapid growth of the use of smartphones requires companies to assure their subscribers that the services they offer are reliable, secure, and trustworthy (Kim, Kang, & Cha, 2013).

As noted by Wang et al. (2012), with increased usage of smartphones in general comes the expectation of increased usage for financial transactions; this follows the trend of moving financial transactions from the personal computer (PC) or banking center to the cell phone. The consumer expects the base framework of the mobile device to be secure enough or at least aware enough to inform them about any potential harm of an application developed by third-party application developers (Banuri et al., 2012).

Research concerning smartphone use and security conducted by Mylonas et al. (2013) examines how smartphone users adopt or understand security options, for example *password protection*. Analysis from Mylonas et al. (2013) shows that smartphone users do not adopt existing security features such as encryption, device password, remote data wipe and remote device locator. Users also tend to ignore repetitive warnings, especially when a warning appears while the user attempts to fulfill a task (Tsai, Egelman, Cranor, & Acquisti, 2011).

Users who are not technically savvy are not able to make the appropriate security decisions; this circumstance contributes to the inability of companies to protect consumers (Mylonas et al., 2013). Banuri et al. (2012) believe that even with advancement in mobile security frameworks, the customer continues to be at risk if they use a smartphone for applications. However, Larkin (2009) notes that although a person might think the boost in convenience comes at the expense of security, banking on a smartphone can be safer than using a PC if customers understand that malware and viruses can impact their security.

Purpose

In March 2007, Bank of America launched mobile applications to allow customers to conduct financial transactions including view balances, pay bills, transfer money and deposit checks (Rosencrance, 2007). As noted by Mylonas et al. (2013), customers may not be aware of the latest security prevention measures. Currently, smartphone subscribers are solely responsible for installing applications and ensuring that they are secure (Wang et al., 2012). However, as noted by Larkin (2009), security breaches can occur on smartphones without the customers' knowledge while making financial transactions, including banking transfers, bill pay, and person-to-person payments. Ensuring security requires collaboration among mobile users, service providers, and industry partners (Wang et al., 2012).

The purpose of this annotated bibliography is to identify and describe (a) the latest security risks faced by consumers when using smartphones to conduct financial transactions and (b) the existing options to mitigate or avoid these risks. Several core questions could be asked in this context, including (a) what can mobile phone users do to improve their chances of preventing fraud on their mobile device should security be compromised; (b) why are customers not using the existing security controls; and (c) are the customers educated on the availability of security options for a smartphone device? The intent is to provide information that can be used to educate customers about the security risks and control options available to best secure smartphones, when conducting financial transactions.

Main question. As the usage of smartphones increases (Lawton, 2008), what are the key security risks faced by smartphone users when conducting financial transactions (Mylonas et al., 2013), and what security controls are available to address each of these risks (Konidala, Dwijaksara, Kim, Lee, Lee, et al., 2012).

Audience

The primary audience of this annotated bibliography is managers who lead information development departments, and who should be aware of potential security risks that could be faced by customers when using a mobile phone (Tsai et al., 2011). A recent survey (2013) revealed that 76% of the mobile users believed that applications downloaded from the application repository are secure (Mylonas et al., 2013). Mobile devices are, by their very nature, more vulnerable to threat such as theft and accidental loss than larger systems in fixed locations (Botha et al., 2009). Typically, managers within the mobile software engineering industry have a background in information security with a focus on operating systems and application security. Information development departments should be aware of potential security risks that could be faced by customers when moving from desktop browsing to smartphone downloadable applications (Mylonas et al., 2013). These managers need this study to ensure they educate their customers, developers, testers and business partners to the risks smartphone applications pose to security; they should be aware of potential security risks that could be faced by customers when moving from desktop browsing to smartphone downloadable applications (Dourish , Grinter, de la Flor, & Joseph, 2004). Managers equally need this study to understand how to add security frameworks to their software development lifecycle (Banuri et al., 2012).

A secondary audience includes smartphone users who should be better educated about current security risks when using smartphones to conduct financial transactions, and existing security control options (Mylonas et al., 2013).

Search Report

Searches for reference material are conducted using the Oregon University Libraries website portal. All searches are done using the "Quick Search" with all fields' option. UO Library database and index search includes the JSTOR, Academic Search Premier, and Web of Science.

There is not a large amount of research material, because mobile security is a relatively new area of study. Most relevant references returned are current (meaning published since 2007), due to the newness of smartphone technology. Results include irrelevant articles, i.e., those that address mobile security without details relevant to this study or articles that discuss network security.

Search terms. The main search terms are *mobile, software, smartphone, framework, security, malware,* and *protection*. This list covers the software attributes related to the main question. *Mobile* and *smartphone* refer to the device that is the focus of the research. *Software* and *framework* describe the technology that a software engineer uses to develop native applications. *Security, malware* and *protection* provide a broad search range on smartphone security threats and mitigations for those risks. Articles are considered relevant only if they contain current information (2007 or later) relevant to mobile security challenges and control options; 2007 was chosen as this is the year the iPhone launched. The list below covers the combination of search terms that are used to search for relevant articles.

- mobile software security framework – 117 results… 2 relevant resources
- Smartphone security challenges – 55 results… 3 relevant resources
- smartphone security framework - 48 results… 2 relevant resources
- smartphone security – 120 results… 8 relevant resources
- smartphone malware – 106 results… 3 relevant resources
- smartphone security protection – 39 results… 1 relevant resource

Evaluation criteria. Articles are evaluated based on authority of the author/publisher, objectivity of the author and quality, currency, and relevancy of the work (Bell & Frantz, 2013). In this study, only articles that are published in a peer-reviewed journals are selected to insure that all material is *objective* and of high *quality*. A *quality* paper consist of a logical structure, presents main points clearly, paper flows well, author's argument does not repeat, and paper is clear of grammatical errors (Bell & Frantz, 2013). *Currency* is established by reviewing articles written after 2007 in order to include information about the iOS (iPhone) and Android operating system after becoming public. There is one exception for an article that is published in 2004 which discusses user attitudes towards security. Articles are chosen based on *relevancy* to iPhone or Android security risks when conducting financial transactions, and how smartphone users can use existing security controls to mitigate these risks.

Documentation approach. Data analysis takes place using a spreadsheet of each category of information provided by the article. These categories are used to help organize the research paper on the broader subject of mobile phone security. This process identifies the articles that cover the main research question for this study. These categories include *smartphone security risks*, *smartphone malware*, *smartphone security framework* and *smartphone security controls*. *Smartphone security risk* includes any event on a phone that could compromise a user's information, location or transaction. *Security framework* provides software engineers development patterns to prevent security events. *Smartphone malware* is a malicious software application that intercepts the customer's actions and sends the data to a fraudulent site. *Smartphone security controls* are steps provided to help software engineers prevent security risk and actions that a smartphone owner can do to ensure a secure phone.

Reading and coding. While reviewing a selected reference, focus is on identification of two larger coding categories: (a) potential security risks to the smartphone when conducting financial transactions including malware, and (b) the existing security controls that provide protection for these risks including security frameworks. This approach is based on a form of qualitative data analysis described by Creswell (2008, pp. 184-188). Once identified, articles are labeled in a spreadsheet with the categories of *security framework, security, protection, malware and customer control.* *Security frameworks* and *protection* are addressed to give the software engineering manager guidance on how to prevent security breaches in published smartphone applications. *Security* and *malware* categories address the types of attacks that can occur on smartphones that host financial transactions. *Customer control* covers the attitudes of smartphone users and steps they can use to prevent security breaches.

The results of the reading and coding process are noted in the Summary section of each reference annotation. Conclusions are based on these results and framed in response to the research question, for the needs of the audience.

Annotated Bibliography

The Annotated Bibliography presents 15 references that address the main research question posed in this study: What are the key security risks faced by smartphone users when conducting financial transactions, and what security controls are available to address each of these risks? References are organized into three categories that address: (a) *smartphone security risks*, including references that examine any event on a phone that could compromise a user's information, location or transaction, and *smartphone malware*, including references that examine malicious software applications that intercept user actions and send the data to a fraudulent site, and (b) *existing smartphone security controls*, including references that examine steps provided to help software engineers prevent security risk and actions that a smartphone user can take to ensure a secure phone, and *security frameworks*, including references that examine frameworks designed to prevent security breaches.

Each reference annotation consists of (a) a bibliographic citation in APA format, (b) short abstract, and (c) summary. The summaries include an overview of the content in each reference relevant to the research categories of (a) smartphone security risks and smartphone malware, and (b) existing smartphone security controls and security frameworks.

Smartphone Security Risks and Smartphone Malware

Botha, R. , Furnell, S. , & Clarke, N. (2009). From desktop to mobile: Examining the security experience. *Computers & Security, 28*(3-4), 130-137. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404808001089

Abstract. The use of mobile devices is becoming more commonplace, with data regularly able to make the transition from desktop systems to pocket and handheld devices such as smartphones and PDAs. However, although these devices may consequently contain or manipulate the same data, their security capabilities are not as mature as those offered in fully-fledged desktop operating systems. This paper explores the availability of security mechanisms from the perspective of a user who is security-aware in the desktop environment and wishes to consider utilizing similar protection in a mobile context. Key issues of concern are whether analogous functionality can be found, and if so, whether it is offered in a manner that parallels the desktop experience (i.e. to ensure understanding and usability). The discussion is supported by an examination of the Windows XP and Windows Mobile environments, with specific consideration given to the facilities available for user authentication, secure connectivity, and content protection on the devices. It is concluded that although security aspects receive some attention, the provided means generally suffer from usability issues or limitations that would prevent a user from achieving the same level of protection that they might enjoy in the desktop environment.

Summary. The article details research of impacts on mobile security as users move from a desktop environment to a smartphone device. The authors cover the considerations that users of cell phones need to consider when using a smartphone for the first time. This article examines security risks by addressing (a) user authentication including ID/passcode to prevent unauthorized access, (b) network connectivity issues with unsecure connections, and (c) malicious content security to prevent spoofing.

Chandramohan, M. , Tan, H.(2012). Detection of mobile malware in the wild. *Computer*, *45*(9), 65-71. Retrieved from http://www.computer.org/csdl/mags/co/2012/09/mco2012090065-abs.html

Abstract. New techniques for detecting the presence of mobile malware can help protect smartphones from potential security risks.

Summary. The authors examine attacks on smartphones due to users downloading unsafe applications. This article addresses the main research question of smartphone main security risks. They cover three versions of unsafe applications that can impact the security on smartphones to include (a) malware, (b) spyware, and (c) greyware. They review how these malicious applications can (a) offer novelty and amusement, (b) sell user information, (c) steal user credentials, (d) manipulate content delivery, (e) send SMS (simple message service) spam, and (f) manipulate search engine results. The article explains controls that can detect malware including (a) static analysis, meaning that software can review for common malware patterns to provide warnings (b) dynamic analysis, meaning that software automatically updates controls for uncommon malware patterns (c) application permission analysis, meaning that applications detect when access is not authorized on a native application (d) and cloud based detection, meaning that a cloud based application provides malware protection for users that do not wish to install a malware application.

Damopoulos, D. , Kambourakis, G. , Anagnostopoulos, M. , Gritzalis, S. , & Park, J. (2013). User privacy and modern mobile services: Are they on the same path?. *Personal & Ubiquitous Computing, 17*(7), 1437-1448. http://link.springer.com/article/10.1007%2Fs00779-012-0579-1

Abstract. Perhaps, the most important parameter for any mobile application or service is the way it is delivered and experienced by the end-users, who usually, in due course, decide to keep it on their software portfolio or not. Most would agree that security and privacy have both a crucial role to play toward this goal. In this context, the current paper revolves around a key question: Do modern mobile applications respect the privacy of the end-user? The focus is on the iPhone platform security and especially on user's data privacy. By the implementation of a DNS poisoning malware and two real attack scenarios on the popular Siri and Tethering services, we demonstrate that the privacy of the end-user is at stake.

Summary. The research described in this article provides methods for software engineers to prevent privacy breaches and answers the main question of smartphone controls to prevent security risks. The article also covers top security risks with the smartphone to include (a) mDNS (multicast domain name service), which provides zero configuration host name resolution (b) tethering, which means connecting your device to a separate computer to provide network services (c) Siri services, which provide voice activated search commands, which can be attacked by overriding the voice commands and (d) DNS poisoning malware, which corrupts the DNS local cache. The article examines security control options that exist to address each of these risks by providing developers with controls to prevent (a) DNS hijacking, (b) privacy leaks over Siri, (c) exposing user's geographic location, and (d) acquiring a user's controls.

Kim, J. , Kang, S. , & Cha, H. (2013). Smartphone banking: The factors influencing the intention to use. *Transactions on Internet and Information Systems, 7*(5), 1213-1235. Retrieved from http://go.galegroup.com/ps/i.do?action=interpret&ty=as&v=2.1&lm=&u=s8492775&it=search&s=RELEVANCE&p=AONE&qt=SN~1976-

7277~~TI~Smartphone+Banking++The~~VO~7~~SP~1213~~IU~5&sw=w&authCount=1

Abstract. In this paper, we investigated the factors affecting the intention to use smartphone banking with a research model based on the Technology Acceptance Model (TAM) extended to include security risk, trust, and self-efficacy. With analysis after controlling factors such as age, gender, and previous experience of smartphone banking that may have effects, we conclude that perceived usefulness, perceived ease of use, security risk, and trust have direct effect on the intention to use smartphone banking, and self-efficacy has indirect effect on the intention to use through mediation of perceived ease of use. We performed a study to check the validity of TAM in the context of smartphone banking, and confirmed that perceived ease of use has both direct and indirect effect on the intention to use.

Summary. This paper researches the increased usage of the smartphone in South Korea by conducting surveys of mobile banking users and their awareness of security issues related to smartphone banking. The research examines smartphone (a) security risks and (b) network trust with cell provider and WIFI. This research utilized the Davis TAM model by analyzing implications of prior research on mobile banking. The authors hypothesize that trust and security risk would further impact mobile banking use. In order to test the model and validate the hypothesis they employed an empirical study using data from online survey responses. The conclusion in the paper confirms that *trust* and *security* impact the use of smartphone to conduct banking transactions. Identified security threats include: (a) hacking, (b) malicious code, (c) stolen ID/passcode and (d) fraudulent SSL digital certificate. The paper provides support for prevention measures for each of the security threats to include (a) malware protection for malicious code and hacking, (b) coding prevention of stolen ID and passcode, and (c) proper alerting of fraudulent certificates.

Konidala, D. , Dwijaksara, M. , Kim, K. , Lee, D. , Lee, B. , et al. (2012). Resuscitating privacy-preserving mobile payment with customer in complete control. *Personal and Ubiquitous Computing, 16*(6), 643-654. Retrieved from http://download.springer.com/static/pdf/886/art%253A10.1007%252Fs00779-011-0436-7.pdf?auth66=1385100268_6c8f6c9d48e55cf60791aca472255767&ext=.pdf

Abstract. Credit/debit card payment transactions do not protect the privacy of the customer. Once the card is handed over to the merchant for payment processing, customers are "no longer in control" on how their card details and money are handled. This leads to card fraud, identity theft, and customer profiling. Therefore, for those customers who value their privacy and security of their payment transactions, this paper proposes a choice-an alternate mobile payment model called "Pre-Paid Mobile HTTPS-based Payment model". In our proposed payment model, the customer obtains the merchant's bank account information and then instructs his/her bank to transfer the money to the merchant's bank account. We utilize near field communication (NFC) protocol to obtain the merchant's bank account information into the customer's NFC-enabled smartphone. We also use partially blind signature scheme to hide the customers' identity from the bank. As a result, our payment model provides the customer with complete control on his/her payments and privacy protection from both the bank and the merchant. We emulated our proposed mobile payment model using Android SDK 2.1 platform and analyzed its execution time.

Summary. The authors' research focuses on using the smartphone as a payment device and what security risks can occur because of the payment transactions. This paper focuses on the main question answering how security risks can impact smartphone transactions. The research addresses attacks that can impact a transaction to include, (a) man in the middle where another device intercepts the user's transactions and (b) replay attack, which is a breach of security where information is stored without authorization and then retransmitted to trick the receiver into unauthorized operations. The solution utilizes (a) partially blind signature as a protocol for obtaining a digital signature from a signer that allows the signer to explicitly include necessary information (expiration date, collateral conditions, or whatever) in the resulting signatures under some agreement with the receiver; (b) anonymous pre-paid digital cash certificate similar to bit coin that provides transfer of digital cash; and (c) hypertext transfer protocol secure (HTTPS) to help secure financial transactions via an encrypted pipeline.

Lawton, G.. (2008). Is it finally time to worry about mobile malware?. *Computer, 41*(5), 12-14. Retrieved from http://www.computer.org/csdl/mags/co/2008/05/mco2008050012.pdf

Abstract. With smart-phone use growing rapidly and devices gaining more capabilities that create possible vulnerabilities, experts think mobile malware finally might be about to become an important issue.

Summary. This article is based on research on the threat of malware as it existed in 2008. The study addresses the main research question of the key security risks faced by smartphone users when conducting financial transactions. Lawton addresses the subject of malware and how it impacts smartphone devices by attacking via (a) Bluetooth, (b) flashcard memory readers, (c) instant messaging, and (d) email. The study shows attacks that occurred close to the time of publication in 2008 and methods in which users can prevent malware from being installed on their cell phones. He describes existing security controls to include (a) antivirus software, (b) firewalls, (c) improved application signing, and (d) user education.

Lin, C., & Varadharajan, V. (2010). Mobiletrust: A trust enhanced security architecture for mobile agent systems. *International Journal of Information Security, 9*(3), 153-178. Retrieved from http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=d3cc5b5a-e496-4d73-bd56-08d7a3946a09%40sessionmgr12&vid=2&hid=28

Abstract. While offering many practical benefits for distributed applications, mobile agent systems pose some fundamental security challenges. In this paper, we present a new approach to mobile agent security which helps to address some of these challenges. We present a new technique, which we refer to as trust enhanced security, and apply it to mobile agent-based systems; this new technique advocates a shift in security solutions from security-centric to trust-centric. This extends the traditional security mechanisms by enabling trust decisions through explicit specification and management of security-related trust relationships. The integration of the trust decisions into security decision-making process leads to our trust enhanced security performance. A formal trust model is proposed and is incorporated into the development of a novel trust management architecture-MobileTrust for mobile agent-based applications. We have conducted detailed practical investigations to evaluate and validate the emergent properties of the trust enhanced security technique. We present and discuss the key results in this paper.

Summary. The authors research smartphone application security when deploying native applications on mobile devices. The research shows how controls can be put in place to provide trust by authorizing use of an application. To provide application security, the authors define requirements (a) to abstract trust from the smartphone to the application, (b) to allow the application to recognize user authentication for trust establishment, and (c) for integration of trust and security in the smartphones network connectivity. Through this framework, the research shows how enhanced trust architecture can protect smartphone applications from security risks.

Waehlisch, M. , Trapp, S. , Schiller, J. , Jochheim, B. , Nolte, T. , et al. (2012). Vitamin c for your smartphone: The SKIMs approach for cooperative and lightweight security at mobiles. *Computer Communication Review, 42*(4), 271-274. Retrieved from http://delivery.acm.org/10.1145/2380000/2377726/p271-wahlisch.pdf?ip=128.223.174.110&id=2377726&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF15542EBFCB1385A8FF2B5F7F13CB63901&CFID=257393117&CFTOKEN=44624622&__acm__=1383105685_b38b112764016b7471f597ca7febbbf5

Abstract. Smartphones are popular attack targets, but usually too weak in applying common protection concepts. SKIMS designs and implements a cooperative, cross-layer security system for mobile devices. Detection mechanisms as well as a proactive and reactive defense of attacks are core components of this project. In this demo, we show a comprehensive proof-of-concept of our approaches, which include entropy-based malware detection, a mobile honey pot, and spontaneous, socio-inspired trust establishment.

Summary. This paper provides research into security control options that exist to address four security risks faced by smartphone users when conducting financial transactions. In contrast to wired end systems, mobile devices exhibit three characteristic differences: (a) they normally are equipped with several different network interfaces; (b) their capabilities are significantly limited so that they are not able to permanently maintain strong protection mechanisms; and (c) physical vicinity with the help of appropriate access technologies allow for the establishment of separate, cooperative delivery structures. The authors provide controls for (a) detection of malware to include malicious software to steal customer information; (b) ad-hoc trust establishment, which includes the establishment of a secure trust between two devices; (c) secure data transmission, which includes the ability to send data over a secure channel; and (d) reporting threat levels to the SKIMs security application. Each component for detection reports its current threat level to the SKIMS app, which calculates an overall state. The application decides based on the threat level what level of control to deploy.

Wang, Y. , Streff, K. , & Raman, S. (2012). Smartphone security challenges. *Computer, 45*(12), 52-58. Retrieved from http://www.computer.org/csdl/mags/co/2012/12/mco2012120052.pdf

Abstract. Because of their unique characteristics, smartphones present challenges requiring new business models that offer countermeasures to help ensure their security.

Summary. This research article addresses the main question of what risks exist for smartphones that conduct financial transactions. The article provides evidence of security risks at the application, communication, and resource layers. Four security threats discussed in the article are (a) malware attacks, (b) sensor impacts, (c) network sniffing of data passed between device and source, and (d) sensitive data storage on a smartphone. Of the security threats described, the authors provide control options for both the publisher of applications and the end user of the smartphone. Control options include (a) keeping sensitive data separate from non sensitive data, which allows for user permissions to prevent unauthorized access; (b) providing anti malware protection software which will prevent the user from infecting their smartphone device; and (c) increased security awareness allows the user to protect their device if lost.

Zonouz, S. , Houmansadr, A. , Berthier, R. , Borisov, N. , Sanders, W. , et al. (2013). Secloud: A cloud-based comprehensive and lightweight security solution for smartphones. *Computers & Security, 37*, 215-227. Retrieve from http://ac.els-cdn.com/S016740481300031X/1-s2.0-S016740481300031X-main.pdf?_tid=7a254cce-4115-11e3-8c08-00000aab0f6c&acdnat=1383104805_ecbcf38c56841405a8b7f62d07259476

Abstract. As smartphones are becoming more complex and powerful to provide better functionalities, concerns are increasing regarding security threats against their users. Since smartphones use software architecture similar to PCs, they are vulnerable to the same classes of security risks. Unfortunately, smartphones are constrained by their limited resources that prevent the integration of advanced security monitoring solutions that work with traditional PCs. We propose Secloud, a cloud-based security solution for smartphone devices. Secloud emulates a registered smartphone device inside a designated cloud and keeps it synchronized by continuously passing the device inputs and network connections to the cloud. This allows Secloud to perform a resource-intensive security analysis on the emulated replica that would otherwise be infeasible to run on the device itself. We demonstrate the practical feasibility of Secloud through a prototype for Android devices and illustrate its resource effectiveness by comparing it with on-device solutions. As more companies move their application to mobile and their supporting technology to the cloud it is important to understand the inherent risks created by cloud computing.

Summary. This article provides research on security threats with smartphones that could be addressed by moving to cloud computing. Cloud computing allows the security support to be centrally located in a trusted location, thus preventing smartphone users from downloading malware client applications. This paper provides examples that address the main research question of common threats against smartphone transactions and what methods can be used to prevent these security threats. This paper also discusses conducting financial transactions on a smartphone and provides one example of a control that can be used to prevent security breaches. The authors discuss threats related to (a) malware, (b) network compromise, and (c) user privacy. The authors propose solutions to these threats to include (a) virus scanning, (b) network monitoring, and (c) user education. Solutions provided in the cloud provide application programmers a trusted source for security that can be centrally located on a trusted network.

Existing Smartphone Security Controls and Frameworks

Banuri, H. , Alam, M. , Khan, S. , Manzoor, J. , Ali, B. , et al. (2012). An android runtime security policy enforcement framework. *Personal and Ubiquitous Computing, 16*(6), 631-641. Retrieved from http://link.springer.com/article/10.1007%2Fs00779-011-0437-6

Abstract. Today, smart phone's malwares are deceptive enough to spoof itself as a legal mobile application. The front-end service of Trojans is attractive enough to deceive mobile users. Mobile users download similar malwares without knowing their illegitimate background threat. Unlike other vendors, Android is an open-source mobile operating system, and hence, it lacks a dedicated team to analyze the application code and decide its trustworthiness. We propose an augmented framework for Android that monitors the dynamic behavior of application during its execution. Our proposed architecture called Security Enhanced Android Framework (seaf) validates the behavior of an application through its permissions exercising patterns. Based on the exercised permissions' combination, the mobile user is intimated about the dangerous behavior of an application. We have implemented the proposed framework within Android software stack and ported it to device. Our initial investigation shows that our solution is practical enough to be used in the consumer market.

Summary. The authors present research on the android security framework that provides methods for software engineers to prevent malware attacks on native applications. This research addresses controls to prevent security risks on smartphone devices. The authors address attacks on (a) SMS (simple message service), (b) telephony, (c) camera, and (d) GPS. To prevent malware from accessing these sensory features on android devices the authors demonstrate how to use the (a) policy repository, (b) permission manager, and (c) policy evaluator. Using the policy repository, the application developer can create permission for an application that alerts the user when malware attempts to inject into an application. The implementation of the proposed framework has been implemented on the Android platform as an enhancement to the existing security framework. The authors of the paper show that these enhancements provide malware protection with minimum overhead.

Botha, R. , Furnell, S. , & Clarke, N. (2009). From desktop to mobile: Examining the security experience. *Computers & Security, 28*(3-4), 130-137. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404808001089

Abstract. The use of mobile devices is becoming more commonplace, with data regularly able to make the transition from desktop systems to pocket and handheld devices such as smartphones and PDAs. However, although these devices may consequently contain or manipulate the same data, their security capabilities are not as mature as those offered in fully-fledged desktop operating systems. This paper explores the availability of security mechanisms from the perspective of a user who is security-aware in the desktop environment and wishes to consider utilizing similar protection in a mobile context. Key issues of concern are whether analogous functionality can be found, and if so, whether it is offered in a manner that parallels the desktop experience (i.e. to ensure understanding and usability). The discussion is supported by an examination of the Windows XP and Windows Mobile environments, with specific consideration given to the facilities available for user authentication, secure connectivity, and content protection on the devices. It is concluded that although security aspects receive some attention, the provided means generally suffer from usability issues or limitations that would prevent a user from achieving the same level of protection that they might enjoy in the desktop environment.

Summary. The article details research of impacts on mobile security as users move from a desktop environment to a smartphone device. The authors cover the considerations that users of cell phones need to consider when using a smartphone for the first time. To prevent attacks via malware and man in the middle the authors examine smartphone control by discussing (a) password protecting the smartphone, (b) using smartphones on secure networks, and (c) understanding the limitations of the smartphone's ability to protect content.

Chang, D. , Hines, S. , West, P. , Tyson, G. , & Whalley, D. (2012). Program differentiation. *Journal of Circuits, Systems & Computers*, *21*(2), 1240007-1240001. Retrieved from http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=73694fa9-07c4-4f2c-869f-db8bc49b5530%40sessionmgr4003&vid=2&hid=4104

Abstract. Mobile electronics are undergoing a convergence of what were formerly multiple single application devices into a single programmable device generally a smart phone. The programmability of these devices increases their vulnerability to malicious attack. In this paper, we propose a new malware management system that seeks to use program differentiation to reduce the propagation of malware when software vulnerability exists. By modifying aspects of the control flow of the application, we allow various portions of an application executable to be permuted into unique versions for each distributed instance. Differentiation is achieved using hardware and systems software modifications which are amenable to and scalable in embedded systems. Our initial areas for modification include function call/return and system call semantics, as well as a hardware-supported Instruction Register File. Differentiation of executables hinders analysis for vulnerabilities as well as prevents the exploitation of a vulnerability in a single distributed version from propagating to other instances of that application. Computational demands on any instance of the application are minimized, while the resources required to attack multiple systems grows with the number of systems attacked. By focusing on prevention of malware propagation in addition to traditional absolute defenses, we target the economics of malware in order to make attacks prohibitively expensive and infeasible.

Summary. The authors research the defense of malware threats against smartphone applications. This article supports the main question of software controls that software engineers can use to prevent malware from infecting a native application. The authors propose to enhance traditional malware attack prevention to stop malware propagation. They propose the use of *software differentiation* at runtime when a vulnerability exists in a software application. This is accomplished through mirroring the application flow, enabling function call/return and system call semantics to be altered into unique versions for each application instance. The authors propose three methods of differentiation: (a) return address differentiation (RAT), which is replacing the return address of an index to a table to prevent injection, (b) system call differentiation, which is implemented by jumping into a function in the operating system via an index in a jump table, and (c) instruction set architecture (ISA), which is implemented by hiding instructions using a level of indirection in the decoding of instructions. All three methods of differentiation offer software engineers coding options to prevent malware intrusion into native applications.

Dourish, P. , Grinter, R. , de la Flor, J. , & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, *8*(6), 391-401. Retrieved from http://download.springer.com/static/pdf/968/art%253A10.1007%252Fs00779-004-0308-5.pdf?auth66=1384662169_2cb669516377807991919d75a956ae5e&ext=.pdf

Abstract. Ubiquitous and mobile technologies create new challenges for system security. Effective security solutions depend not only on the mathematical and technical properties of those solutions, but also on people's ability to understand them and use them as part of their work. As a step towards solving this problem, we have been examining how people experience security as a facet of their daily life, and how they routinely answer the question, "is this system secure enough for what I want to do?" We present a number of findings concerning the scope of security, attitudes towards security, and the social and organizational contexts within which security concerns arise, and point towards emerging technical solutions.

Summary. The authors use two qualitative approaches to analyze methodologies for managing security, including (a) a semi structured interview to gather the data and (b) grounded theory to analyze it. Grounded theory provides a set of procedures for developing analytic accounts of qualitative data based on the iterative generation, validation, and refinement of coding schemes. Their study answers the question of what security control options exist to address risks by analyzing the customer adoption of specific security controls. Their study focuses on (a) the experience of security, (b) attitudes towards security, (c) expectations of security as a barrier and (d) security as a whole (offline and online). The relevant content includes security controls that focus on (a) delegating security, (b) secure actions, (c) holistic security management, and (d) managing identity.

Larkin, E. (2009). Banking by phone: Convenient and safe?. *PC World*, 27(11), 39. Retrieved from http://www.jstor.org/stable/23015560

Abstract. The article offers tips on enhancing security measures when involved in mobile banking. Among the three options for mobile banking are downloading a program for one's cell phone, utilizing the browser of a phone to access a mobile version of one's bank's web site, and sending an SMS message. The author recommends an iPhone application from USAA, which can be used by USAA customers to make deposits by taking a picture of a paper check. The use of a personal identification number (PIN) or a password to lock a phone is also recommended.

Summary. The author provides research on the banking capabilities of the smartphone to include (a) SMS messaging, (b) photo check deposits and (c) transfers between accounts. The author offers information that deals with controls that customers can use to protect their devices. The controls include (a) password protection, which includes enabling password feature on a smartphone to access the phones features (b) installing remote wipe application on a smartphone, includes installing an application that can remotely remove all personal information on a smartphone and (c) SMS alerts to large transactions, which includes working with the financial institution to send an alert when transactions are over a certain amount.

Lin, C., & Varadharajan, V. (2010). Mobiletrust: A trust enhanced security architecture for mobile agent systems. *International Journal of Information Security, 9*(3), 153-178. Retrieved from http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=d3cc5b5a-e496-4d73-bd56-08d7a3946a09%40sessionmgr12&vid=2&hid=28

Abstract. While offering many practical benefits for distributed applications, mobile agent systems pose some fundamental security challenges. In this paper, we present a new approach to mobile agent security which helps to address some of these challenges. We present a new technique, which we refer to as trust enhanced security, and apply it to mobile agent-based systems; this new technique advocates a shift in security solutions from security-centric to trust-centric. This extends the traditional security mechanisms by enabling trust decisions through explicit specification and management of security-related trust relationships. The integration of the trust decisions into security decision-making process leads to our trust enhanced security performance. A formal trust model is proposed and is incorporated into the development of a novel trust management architecture-MobileTrust for mobile agent-based applications. We have conducted detailed practical investigations to evaluate and validate the emergent properties of the trust enhanced security technique. We present and discuss the key results in this paper.

Summary. The authors research smartphone application security when deploying native applications on mobile devices. The research shows how controls can be put in place to provide trust by authorizing use of an application. To provide application security, the authors define requirements (a) to abstract trust from the smartphone to the application, (b) to allow the application to recognize user authentication for trust establishment, and (c) for integration of trust and security in the smartphones network connectivity. Through this framework, the research shows how enhanced trust architecture can protect smartphone applications from security risks.

Mylonas, A. , Kastania, A. , & Gritzalis, D. (2013). Delegate the smartphone user? security awareness in smartphone platforms. *Computers & Security, 34*, 47-66. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404812001733#

Abstract. Smartphone users increasingly download and install third-party applications from official application repositories. Attackers may use this centralized application delivery architecture as a security and privacy attack vector. This risk increases since application vetting mechanisms are often not in place and the user is delegated to authorize which functionality and protected resources are accessible by third-party applications. In this paper, we mount a survey to explore the security awareness of smartphone users who download applications from official application repositories (e.g. Google Play, Apple's App Store, etc.). The survey findings suggest a security complacency, as the majority of users trust the app repository, security controls are not enabled or not added, and users disregard security during application selection and installation. As a response to this security complacency we built a prediction model to identify users who trust the app repository. The model is assessed, evaluated and proved to be statistically significant and efficient. This article discusses steps needed to educate the consumer on how to protect themselves from security breaches.

Summary. This research paper discusses how centralized application repositories are breeding grounds for applications that contain hidden security holes that can impact a smartphone. The research deals with customer control options to help prevent security issues created by a lack of customer education. The survey was conducted in Athens, Greece to determine the awareness of smartphone users to malicious software. Their study confirms that users (a) trust application repositories, (b) have misconceptions on application testing, (c) do not read security and agreement messages, (d) use pirated applications and (e) do not adopt security controls. The authors note that according to the survey results customers are usually unaware of the risks when downloading applications from a repository.

Conclusion

The use of smartphones is currently on the rise as the primary computing device of choice for customers. Mobile devices, often referred to as smartphones, are equipped with enough processing power to replace the usage of laptops (Damopoulos, Kambourakis, Anagnostopoulos, Gritzalis, & Park, 2013). Currently, smartphone subscribers are solely responsible for installing applications and ensuring that they are secure (Wang et al., 2012). The popularity of smartphone applications has attracted attackers, who use the application download stores as a security and privacy attack platform (Mylonas et al., 2013). Wang et al. (2013) state that when users accidentally download malware to a smartphone, the malware tries to control the smartphone resources, collect data, or redirect the smartphone to a premium account or malicious website.

The purpose of this annotated bibliography is to identify and describe (a) the latest security risks faced by consumers when using smartphones to conduct financial transactions and (b) the existing options to mitigate or avoid these risks. The primary audience of this paper is software managers and engineers; managers need to set the standards and policies to ensure their teams are using security-conscious development practices, and engineers need to be aware of and implement these standards and policies.   Banuir et al. (2011) shows that software engineers can take steps to prevent security risks from occurring on customer devices that run applications they write. The secondary audience is the general smartphone user who does not have the knowledge to understand how devices, that are not protected, are susceptible to security risks (Mylonas, et al, 2013). Mylonas et al. (2013) believe that typical smartphone users are not able to make good security decisions, nor are they able to use security controls adequately. They suggest that the average person who downloads applications from sites like the Apple store or Google apps typically trusts the application that installs on their smartphone; users tend to (a) trust application repositories, (b) use pirated applications, and (c) not read the security agreements (Mylonas et al., 2013). This behavior leaves the smartphone susceptible to malicious software that can take over applications causing unimpeded access to (a) simple message service messages, (b) smartphone network transactions, (c) camera, and (d) global positioning system.

Smartphone Security Risks and Smartphone Malware

Smartphone malware is a malicious software application that intercepts the customer's actions and sends the data to a fraudulent site. Malware is an existing threat that exhibits malicious behavior and is broadly categorized to include viruses, botnets, worms, and Trojan horses. Chandramohan and Tan (2012) highlight how malware attacks software system security vulnerabilities, and how malware can be used to gain financial benefits. Lawton (2008) describes a malware InfoJack that sends the infected device's serial number and OS which allows hackers to change the phone's security settings so they can install new applications in the background. Malware attacks banking applications to capture ID/passcode and other financial information (Wang et al., 2012).

Lin and Varadharajan (2010) discuss how increased smartphone usage has elevated security risks as users inadvertently install applications that (a) include abuse by mobility agents that can steal information, (b) install without security policies which can lead to data theft, and (c) employ network connectivity that can expose data transmission to interception from malicious sites. Smartphone security is also at risk of malicious attacks, which can occur via (a) Bluetooth, (b) flashcard readers, (c) instant messaging and (d) email (Lawton, 2008). These attacks can pull sensitive data used in financial transactions through applications used on the smartphone to store data.

Existing Smartphone Security Controls and Frameworks

Proper smartphone security education is the responsibility of the company that provides the banking applications (Banuir et al., 2011). Software engineers who develop native applications can provide additional protection by using application frameworks. A *security framework* provides software engineers development patterns to prevent security events. Banuri et al. (2012) state that the openness of the Android leads to rapid adoption of the platform, which increases the amount of applications that are available in the marketplace. This increases the security vulnerability on smartphones running the Android operating system. A different situation exists on the Apple smartphone, which provides a security review of all applications before publishing them to the application store (Wang et al., 2012). It is shown that development techniques such as software differentiation, which is the practice of protecting application flows from outside access, can provide a control to reduce the impact of malware viruses (Mylonas et al., 2011).

Smartphone security begins with education designed for the smartphone user about existing security controls that can provide protection when conducting financial transactions. Potential dangers include disclosing credit card numbers, social security information, bank transaction details, client records, and other electronic artifacts (Dourish et al., 2004). Without proper education and awareness, the smartphone user will continue to practice risky computing habits. Existing controls designed to protect the smartphone user include (a) password protection for devices, (b) installation of security protection software that includes remote phone erase and malware protection software, and (c) using application alerting features to indicate large transactions occur (Larkin, 2009).

References

Banuri, H. , Alam, M. , Khan, S. , Manzoor, J. , Ali, B. , et al. (2012). An android runtime security policy enforcement framework. *Personal and Ubiquitous Computing, 16*(6), 631-641.

Bell, C. & Frantz, P. (2013). Critical evaluation of information sciences. *UO Libraries*. Retrieved from http://library.uoregon.edu/guides/findarticles/credibility.html

Botha, R. , Furnell, S. , & Clarke, N. (2009). From desktop to mobile: Examining the security experience. *Computers & Security, 28*(3-4), 130-137.

Chandramohan, M. , & Tan, H.(2012). Detection of mobile malware in the wild. *Computer*, *45*(9), 65-71.

Chang, D. , Hines, S. , West, P. , Tyson, G. , & Whalley, D. (2012). Program differentiation. *Journal of Circuits, Systems & Computers*, *21*(2), 1240007-1240001.

Creswell, J. (2008). Research design: Qualitative, quantitative, and mixed methods approaches (Kindle Edition) Sage Publications - A. Kindle Edition.

Damopoulos, D. , Kambourakis, G. , Anagnostopoulos, M. , Gritzalis, S. , & Park, J. (2013). User privacy and modern mobile services: Are they on the same path?. Personal & *Ubiquitous Computing, 17*(7), 1437-1448.

Dourish, P. , Grinter, R. , de la Flor, J. , & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, *8*(6), 391-401.

Kim, J. , Kang, S. , & Cha, H. (2013). Smartphone banking: The factors influencing the intention to use. *Transactions on Internet and Information Systems, 7*(5), 1213-1235.

Konidala, D. , Dwijaksara, M. , Kim, K. , Lee, D. , Lee, B. , et al. (2012). Resuscitating privacy-preserving mobile payment with customer in complete control. *Personal and Ubiquitous Computing, 16*(6), 643-654.

Larkin, E. (2009). Banking by phone: Convenient and safe?. *PC World, 27*(11), 39.

Lawton, G. (2008). Is it finally time to worry about mobile malware?. *Computer, 41*(5), 12-14.

Lin, C., & Varadharajan, V. (2010). Mobiletrust: A trust enhanced security architecture for mobile agent systems. *International Journal of Information Security*, *9*(3), 153-178.

Mylonas, A. , Kastania, A. , & Gritzalis, D. (2013). Delegate the smartphone user? security awareness in smartphone platforms. *Computers & Security*, *34*, 47-66.

Our history in depth. (2013). Retrieved December 18, 2013, from http://www.google.com/about/company/history/

Rosencrance, L. (2007). Bank of America to launch mobile banking. *ComputerWorld* Retrieved from http://www.computerworld.com/s/article/9011221/Bank_of_America_to_launch_mobile_banking_

Waehlisch, M. , Trapp, S. , Schiller, J. , Jochheim, B. , Nolte, T. , et al. (2012). Vitamin c for your smartphone: The skims approach for cooperative and lightweight security at mobiles. *Computer Communication Review, 42*(4), 271-274.

Wang, Y. , Streff, K. , & Raman, S. (2012). Smartphone security challenges. *Computer*, *45*(12), 52-58.

Wilcox, J. (2007). Iphone finish line. *EWeek*, *24*(24), 8.

Zonouz, S. , Houmansadr, A. , Berthier, R. , Borisov, N. , Sanders, W. , et al. (2013). Secloud: A cloud-based comprehensive and lightweight security solution for smartphones. *Computers & Security, 37*, 215-227.