Understanding Mobile Banking Applications' Security risks through Blog Mining and the Workflow Technology

Research-in-Progress

Wu He
Old Dominion University
Norfolk, VA 23529
whe@odu.edu

Xin Tian
Old Dominion University
Norfolk, VA 23529
xtian@odu.edu

Jiancheng Shen
Old Dominion University
Norfolk, VA 23529
jshen@odu.edu

Yaohang Li
Old Dominion University
Norfolk, VA 23529
yaohang@cs.odu.edu

Abstract

This paper provides a review of the security aspect of mobile banking applications. We employed blog mining as a research method to analyze blog discussion on security of mobile banking applications. Furthermore, we used the workflow technology to simulate real-life scenarios related to attacks on mobile banking applications. Insights are summarized to help banks and consumers mitigate the security risks of mobile banking applications.

Keywords: Mobile banking applications, blog mining, workflow technology, security risks

Introduction

Mobile banking applications are increasingly becoming popular. Many bank customers are using mobile banking applications to check balance in their personal account, to transfer funds between accounts and make online payments (Elkhodr, Shahrestani & Kourouche, 2012; Panja et al., 2013). Unfortunately, mobile malware is spreading quickly and has caused a variety of security and privacy concerns including leaking of sensitive financial data, financial loss and identify theft (Claessens et al., 2002; He, 2013). As mobile banking applications are being used by a variety of users (e.g., employees, students and housewives) with varying technology experience in various places such as workplaces, coffee houses, airports and home, understanding the emerging threats, vulnerabilities and counter-measures of mobile banking applications is critical to the future of mobile banking and mobile banking users' financial security. So far there is a lack of summary paper specifically focused on the security risks of mobile banking applications, we decided to employ blog mining as a research method to analyze and summarize online blog discussions on the security risks of mobile banking applications. Furthermore, we made a contribution to the literature by using the workflow technology to simulate real-life scenarios related to attack on mobile banking applications. Best practices and future trends are summarized to help banks and consumers mitigate the security risks of mobile banking. In summary, this paper has two main objectives: 1) to summarize security risks of mobile banking applications through blog mining; 2) to simulate real-life attacks on mobile banking applications using the workflow technology.

Literature Review

Many banks such as Wells Fargo, Bank of America, Chase, and Citi Bank are offering mobile banking services to their customers. In mobile banking, banks usually provide different mobile applications for different devices. Mobile banking makes financial services easily accessible for customers through a handheld device (Singh, Srivastava & Strivastava, 2010). Mobile banking applications also helped financial institutions cut down the cost of providing banking services to customers (Heggestuen, 2014). However, security is a major concern for many mobile banking customers (Elkhodr, Shahrestani & Kourouche, 2012). Security on mobile banking is complicated because of the variety of mobile devices and platforms (Lee, Zhang, & Chen, 2013). The weak and rigid authentication provided by signature, PIN, password and Card Security Code (CSC) in mobile banking have numerous flaws and loop-holes (Edge & Sampaio, 2009). A survey found that when it comes to mobile banking, 31% of customers are willing to pay for added security features, 63% are willing to switch accounts for one with better security features, and 71% are willing to switch accounts to one that guaranteed losses would be reimbursed (Heggestuen, 2014).

To create a safe and robust mobile banking system, cyber security experts have provided pertinent frameworks and methods for mobile banking security solutions. Edge and Sampaio (2009) provided a comprehensive survey of existing research into account signatures, an innovative account profiling technology that can improve the fraud detection mechanisms. Fatima (2011) recommends using biometrics to enhance existing authentication. Elkhodr, Shahrestani and Kourouche (2012) proposed the Transport Layer Security (TLS) protocol combined with a proposed trust negotiation method, which authenticates the client, the mobile device used in accessing the bank account information, and the server. Ryan (2014), as a practitioner from Conference of State Bank Supervisors, suggested a four-step mobile banking risk assessment method, including classification of information, identify threats and vulnerabilities, measure risk and communicate risk. The new plans and solutions on mobile banking cyber security are required in the mobile application development and implementation process. The New York State Department of Financial Services in 2013 has conducted an industry survey on cyber security and collected information on 154 financial institutions' information security framework and their future plans on cyber security (Cuomo, 2014). The survey results indicated that increasing sophistication of threats and emerging technologies pose many challenges to security protection. On the other hand, Pousttchi and Schurig (2004) suggested the security requirement for mobile banking: data needs to be encrypted, access to the data must be authorized and the authorization has to be simple. In practice, security cannot be achieved with technology that decreases usability since we cannot expect the entire workforce to become security professionals (Potter, 2006). Ease of use is a key factor for consumer acceptance of mobile banking services (Jeong & Yoon, 2013).

Methodology

As there are few academic research papers discussing and summarizing security risks of mobile banking applications, we used two approaches to examine this specific topic. First, we employed blog mining as a research method (Rubin et al., 2011; Chau and Xu, 2012; He & Zha, 2014) to analyze blog pages that discuss security of mobile banking applications. As mobile banking is a very new topic, it is hard to find enough academic papers on this topic. Thus, blog mining offers a feasible way to learn about the recent development about mobile banking applications. As blogs represents personal opinions and often contain bias, we combine blog mining with our previous academic literature research for better understanding the security of mobile banking applications. Specifically, Google blog search engine (http://www.google.com/blogsearch) was used to retrieve blogs with several keywords including "mobile banking security" and "mobile apps vulnerability". As result, over 200,000 results were found mostly from 2012-2015 in 0.49 seconds. We selected the top 100 records as the data set. We saved the top 100 blog posts for text mining and analysis. A well-known text analytics tool named NVivo 10 was used to conduct various query searches, clustering analysis and text analysis to find security risks and countermeasures.

Second, we used the workflow technology to simulate complex real-life scenarios within a laboratory setting to analyze attacks on mobile banking. Workflow tools such as Kepler offer GUI interfaces to easily create various security scenarios. Using the Kepler scientific workflow system (Ilkay et al., 2004), we

developed a security attack scenario as an example to illustrate how the attack on mobile banking application works. According to Allen (2001), a workflow is "*The automation of a business process, in whole or part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules*." The basic element in a workflow is a task, which is defined by three parameters: input description, transformation, and output description. Typically, a workflow consists of a set of serial or parallel tasks that perform the operations of accessing services or executing specific functions (Yu & Buyya, 2005).

Results

Blog Mining Results

Two researchers used NVivo 10 to cluster and analyze the content of the collected data and generated the results of the word frequency and a few clusters. After examining and analyzing the generated results such as clusters by NVivo 10, the two researchers had an in-depth discussion to finalize the clusters since there were many sub-clusters generated by NVivo. A third researcher was invited to join in the discussion and provided additional input when there were conflicts and disagreement about certain themes and clusters. As a result of the discussion, we merged some of the clusters and sub-clusters based on our knowledge and finalized the clusters manually. As a result, we reduced the final number of the clusters to three major clusters to make the results more meaningful. Table 1 lists the finalized clusters and main themes.

Concept clusters	**Main content**
Mobile Banking App Threats & Vulnerabilities	Mobile malware (Trojans, root kits and viruses), phishing, third-party apps, unsecured Wi-Fi networks, risky consumer behavior.
Countermeasures & best practices	Anti-virus app, Encryption, two-factor authentication, security image, SiteKey, one-time password, app update, layered security control
Emerging security trends	Biometric-powered bank applications, big data for fraud detection, mobile security SDK, intelligent behavioral monitoring and analysis

Table 1. Main Blog Themes on Mobile Banking App Security

Furthermore, we manually examined the blog posts that have the most appearance of the keywords to better understand their discussions and contexts. As the main threats, attacks and vulnerabilities related to mobile banking applications are of particular interest, we presented a summary and synthesis of main threats, attacks and vulnerabilities below based on what we found from the blog mining.

Mobile Banking App Threats

We identified a variety of mobile banking app threats from the blog mining results. They are listed below:

- The mobile malware mainly include Trojans, root kits and viruses. Many of mobile malware are variants of existing malware that affect computers and traditional online banking (Webroot, 2014; Shih et al., 2008). Some common malware affecting mobile bank apps include Zitmo, Banker, Perkel/Hesperbot, Wrob, Bankum, ZertSecurity, DroidDream and Keyloggers. Cyber criminals have been refining these malware to target mobile devices for access to bank accounts and make them more resilient to security defenses. Table 2 lists some common malware that affect mobile banking apps.
- Threats from third party applications. Third party applications on mobile devices could secretly tamper an existing banking app that is already in the mobile device and steal account information. Users are advised to download apps or app updates only from official sources or trusted app stores.

- Phishing: Fraud Apps / Fake App Update. There are many fake banking applications that claim to be official on third party app marketplace. Cybercriminals also often offer a downloadable update for the banking apps on third party app websites. These fake apps or fake app updates contain malicious codes to steal users' bank account information (Huang, 2015).
- Unencrypted wireless networks. Wireless networks in public places like coffee shops and hotels are not so secure. When mobile banking app users use unsecure wireless networks to check account balance, deposit checks and pay bills, cybercriminals can eavesdrop and steal their sensitive information (Legnitto, 2013).
- Vulnerability of the app. For example, many banking apps lack protection against reverse engineering of code (whiteCryption, 2014). Cybercriminals can analyze the source code to steal account information and other sensitive information.

Protection Strategies and Best Practices

A number of security mechanisms such as second factor authentication, data encryption, site key with security questions and images, registered mobile device authentication, and anti-virus apps can be adopted to enhance the security of mobile banking applications (Cognizant, 2013; Constantin, 2014; Lee, Zhang, & Chen, 2013; Chandramohan & Tan, 2012; La Polla, Martinelli, & Sgandurra, 2013; White, 2013). Some protection strategies/best practices that we found for users and developers of mobile banking app are summarized below.

Protection strategies/best practices for users

Strategy	Rationale	Best Practices
Do not use **mobile banking app on jailbreak** smartphone	Many people route or jailbreak their smartphones in order to get additional benefits. However, jailbreaking smartphones brings vulnerabilities to the operating system.	To protect smartphone from various security threats, users need to avoid jailbreaking or routing their phone.
Do not install mobile banking app from third parties	Many people try to install applications from third parties, because they are free there. However, many free apps from third parties contain virus	Install mobile banking apps only from official bank website.
Use mobile anti-virus apps	Mobile anti-virus apps will provide partial protection from malware to help mitigate risks.	Install recommended antivirus products by leading organizations such as PC Magazine who have been testing those antivirus products annually
Use secured Wi-Fi network when using mobile banking app	Unsecured or unencrypted Wi-Fi networks may let the sensitive data exposed to the hackers.	Do not connect to public Wi-Fi network when you use mobile banking app.
Update mobile banking app	Banks regularly update their apps to fix bugs and vulnerabilities.	Update the mobile banking app when the new version is released.
Update mobile OS	Mobile OS should be updated timely because hackers may leverage the vulnerability of the OS to attack the mobile banking app	Update the mobile OS as soon as possible after the update becomes available.

Table 2. Protection strategy/best practices for users (Cognizant, 2013; Constantin, 2014; White, 2013)

Protection strategy/best practices for developers of mobile banking apps

Title	Description	Protection strategies/best practices
Secure transfer protocols	Make sure all connections and communications are secure.	Ensuring all connections are made using secure transfer protocols
Root Certificate Check	Securing the communications between the client-side app and the backend server.	Enforcing SSL certificate validation. The bank app needs to check the SSL certificate to see if it is signed by the respective authority.
Encrypt sensitive data	Protecting the confidentiality of data	Encrypting sensitive data stored by the applications by using the data protection API
Jail-Break/ Rooted Device Check	To lower security risks, bank apps must check whether the device is rooted or jail-broken.	Improving jailbreaking detection
Anti-debugging Mechanism	To prevent debuggers from stealing sensitive data	Obfuscating the assembly code and using anti-debugging techniques to make reverse-engineering more difficult.
Debugging statement removal	Do not leave any debugging statement and development information to the hackers.	Removing debugging statements and development information from the final products.
Security Logging	Log all security events related to the baking application and then sent them to the back-end server for further checking and analysis.	Store all security events stored on the device first. When users log out of the application, the security events are sent to the server.
Blacklisting Older Versions of the App	Older versions of the bank apps often have more security bugs and vulnerabilities	Checking the version of the app on the server side. If the version is old, block it and reminder the user to update the app from official bank website to avoid security breach.
SiteKey with Security images and questions	They are mainly used as part of the login process to help users identify and deter phishing.	Adding an additional layer of identity verification to make phishing harder
One-time password	A token is generated and sent to users by SMS message after the user name and password have been verified. Then the user enters the received token in the appropriate field to access the mobile banking services.	It provides second-factor authentication which adds additional security for identity verification when banking app users log in or performing certain transactions.

Table 3. Protection strategy/best practices for developers of mobile banking apps (Cognizant, 2013; Constantin, 2014; White, 2013)

Emerging Security Trends

Some security experts and vendors propose new ways to mediate security risks associated with mobile banking apps. Below are some emerging trends we found from the blog mining results.

- Integrating biometrics into mobile banking apps to enhance user authentication. Biometric authentication such as fingerprint scanning and voice recognition offers a promising way for identity and access management (Fatima, 2011). Schneider (2012) suggest the use of voiceprint ID such as random digitsand random phrases. As personal biometric also has vulnerability, it is better to combine personal biometric with other authentication such as one-time password (OTP) and SiteKey for stronger personal identification and verification.
- Integrating intelligent behavioral monitoring and analysis technology with mobile banking apps. Webroot (2014) recently developed mobile security SDK which is designed to embed security within a mobile banking app, run in the background and deliver real-time threat intelligence to the bank for further data analysis and action. By employing a behavioral monitoring and analysis approach, banks can detect abnormal behavior more accurately and early. Specifically, behavior analysis can detect the behavior of the person who is using the mobile app and compare it with previous behavior or usage patterns. If abnormal behavior is identified, alert messages will be sent out.
- Deployment of advanced big data analytics technology for fraud detection and behavioral analysis. Accurate and efficient behavioral analysis requires banks to deploy advanced big data analytics to mine enormous volumes of security data to better identify trends of malicious behavior or abnormal behaviors indicative of an attack at the outset (Khosla, 2015).

Developing workflows that illustrate attacks on mobile banking

The above blog mining identifies a wide variety of security risks. To help readers better understand the security risks, we used the Kepler scientific workflow system (Ilkay et al., 2004) to develop several security attack scenarios. One of the security attack scenarios is to simulate an emerging attack on mobile remote deposit capture (RDC), which is a popular feature of mobile banking apps. A man-in-the-middle attack, which recently emerged as a major threat for mobile banking apps, is simulated in this workflow demo (Figure 1). As some mobile banking apps do not implement SSL validation correctly, an attacker can substitute a legitimate SSL certificate with one under his control and look at data exchanged between the mobile device and remote server or manipulate private information submitted by the mobile banking customers (Regalado, 2014). The workflow demo provides simulation of the solutions by banks (Wisniewski, 2013; Regalado, 2014) to mediate such attacks. In addition to implementing correct SSL/TSL certification process, mobile banking apps include video deposit, which allows the user to capture a check image with the video setting on their smartphone rather than the still camera. This makes the hacking of the check image more difficult. Real-time early warning services are also implemented to send mobile bank users real-time notice to reduce possible frauds such as duplicate checks. The workflow provides an intuitive way to simulate, visualize, and analyze these business processes.

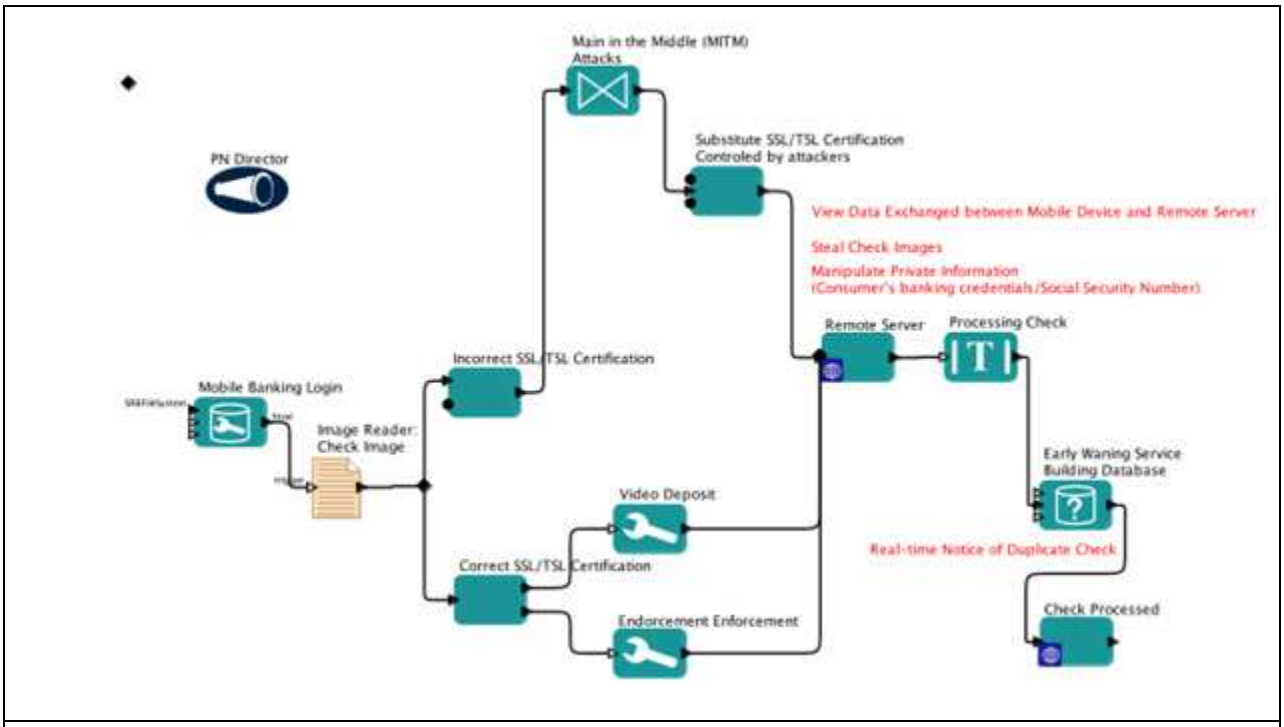

Figure 1. An attack on mobile remote deposit

We demonstrated the workflow technology and the developed scenarios to students in our class. Students were asked to rate the following three statements and provide comments through a brief survey. The three survey questions were adapted from a learning-related survey in Abdous & He (2008). The majority of the students agreed that using the security scenarios implemented by workflow technology was helpful in deepening their understanding of the details involved in the attack and increased their interest and knowledge in developing countermeasures against such attacks. The workflow technology increases their interest in learning more security concepts and techniques (see Table 4).

Statement	Strongly agree	Agree	Neither Agree Nor Disagree	Disagree	Strongly disagree
Workflow technology is very useful for learning information security concepts.	12 (28.6%)	21 (50.0%)	7 (16.7%)	0 (0.0%)	2 (4.8%)
I am interested in learning more about using workflow technology for information security.	9 (21.4%)	20 (47.6%)	11 (26.2%)	1 (2.4%)	1 (2.4%)
I enjoyed learning information security concepts using workflow technology	8 (19.0%)	25 (59.5%)	8 (19.0%)	0 (0.0%)	1 (2.4%)

Table 4. Student Evaluation on the workflow-based scenario (n= 42 students)

Discussion

Due to the sensitive nature of financial data, mobile banking applications are considered to be one of the most critical mobile commerce applications (Elkhodr, Shahrestani & Kourouche, 2012). Security is a priority for mobile banking applications and enhancing the security of mobile banking applications is

critical to the adoption of mobile banking. Financial industries should increase the security standards they use for their mobile banking solutions. On the other hand, successful mobile banking applications should offer simple and easy-to-use user experience while keeping the data safe (Braz, Seffah, & M'Raihi, 2007). Banks must continually consider how best to enhance usability without sacrificing security, which is also a research challenge faced by mobile banking apps.

To minimize the security risks, our main recommendation for mobile banking app users is that they should download apps or app updates only from official sources or trusted app stores and need to install reputable mobile antivirus products to protect their mobile devices against malware attack. The mobile antivirus products need to do so without bringing down the performance and erroneously blocking valid programs on mobile devices. Thus, selecting mobile antivirus products is important to mobile users since there are over a dozen mobile antivirus products on the market. We recommend users to stick with the recommended antivirus products by leading organizations such as PC Magazine who have been testing those antivirus products annually. If the user notices something suspicious with their mobile banking applications, they should contact their bank to temporary block their account right away until the issue is solved. The adoption of security software along with good security behavior will substantially lower the security risk.

Our recommendation for developers of mobile banking apps is that they should encrypt all data that's transmitted or stored and enforce SSL certificate validation. The app-related codes need to improve jailbreaking detection, obfuscate the assembly code and use anti-debugging techniques to minimize reverse-engineering attempts, remove all development information from the final products. Efforts could be made to integrate security mechanisms into the app development process instead of an afterthought. The workflow technology introduced in this paper help mobile banking app developers better analyze specific security vulnerabilities, understand user requirements, integrate security mechanisms into part of their requirements engineering and development workflow, and help address security early in development. Banks who fail to implement well known security requirements may have to spend more money on improving the mobile banking app's security later (Hibshi, Slavin, Niu, & Breaux, 2014).

At last, we want to emphasize that mobile banking apps should be both user-friendly and secure. With this in mind, authentication based upon biometrics may offer the most appropriate means of improving protection without further increasing the level of inconvenience (Clarke & Furnell, 2005). Mobile banking apps should leverage biometrics such as facial recognition, handwriting recognition and speaker recognition to authenticate users.

Conclusion and Future Research

In this paper, we identified key security risks of mobile banking applications and used the workflow technology to simulate complex real-life scenarios within a laboratory setting about attacks on mobile banking. Our work shows that conducing blog mining and developing security scenarios using the workflow technology can be very beneficial to help banking app developers increase security awareness. In particular, blog mining provides raw data and ideas for building security scenarios using the workflow technology. The workflow-based security scenarios can be used as security development training materials for banks when they train their developers to integrate security into banking apps. However, we must point out that since blog posts are not peer-reviewed or rated for credibility, they often contain personal biases. To overcome this limitation, one method is to combine blog mining with other research methods such as traditional literature review and interviews, for a more comprehensive or accurate understanding of the topics that are under investigation.

As for future research, we will reach out to mobile banking customers and conduct in-depth interviews with them about their experience, concerns and perception with security and privacy of mobile banking applications. We will use workflow technology to simulate other mobile banking security risks such as how to simulate the attack on mobile check deposit so that we can better increase the security awareness of mobile banking app developers and users. These developed workflow-based scenarios will be a good resource to train mobile app developers to integrate security into the development process. We are also interested in studying the use of biometric mechanism in mobile banking applications and the balance between security and usability for mobile banking applications.

Acknowledgements

This work was supported in part by the U.S. National Science Foundation under Grant SES-1318470.

References

Abdous, M., and He, W. 2008. "A Design Framework for Syllabus Generator", in *Journal of Interactive Learning Research*, 19(4), 541-550. Chesapeake, VA: Association for the Advancement of Computing in Education (AACE).

Allen, R. 2001. "Workflow: an introduction", In L. Fischer (Ed.), *Workflow Handbook* (pp. 15-38). Lighthouse Point, Florida: Future Strategies Inc.

Chandramohan, M., and Tan, H. B. K. 2012. "Detection of mobile malware in the wild", in *Computer*, (9), 65-71.

Chau, M., and Xu, J. 2012. "Business intelligence in blogs: Understanding consumer interactions and communities", *MIS quarterly*, 36(4), 1189-1216.

Claessens, J., Dem, V., De Cock, D., Preneel, B., and Vandewalle, J. 2002. "On the security of today's online electronic banking systems", *Computers & Security*, 21(3), 253-265.

Cognizant. 2014. "*Mobile Banking Security: Challenges, Solutions",* Retrieved on Feb 25, 2015 at http://www.cognizant.com/InsightsWhitepapers/Mobile-Banking-Security-Challenges-Solutions-codex898.pdf

Constantin, L. 2014. "*Security analysis of mobile banking apps reveals significant weaknesses",* Retrieved on Feb 21, 2015 at http://www.pcworld.com/article/2086320/security-analysis-of-mobile-banking-apps-reveals-significant-weaknesses.html

Edge, M. E., and Sampaio, P. R. F. 2009. "A survey of signature based methods for financial fraud detection", in *computers & security*, *28*(6), 381-394.

Elkhodr, M., Shahrestani, S., and Kourouche, K. 2012. "A proposal to improve the security of mobile banking applications", In *ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2012 10th International Conference on* (pp. 260-265). IEEE.

Fatima, A. 2011. "E-banking security issues–Is there a solution in biometrics", in *Journal of Internet Banking and Commerce,* 16(2): 2011-08.

He, W. 2013. "A Survey of Security Risks of Mobile Social Media through Blog Mining and an Extensive Literature Search", *in Information Management and Computer Security,* 21(5), pp.381–400.

He, W., and Zha, S.H. 2014. "Insights into the Adoption of Social Media Mashups", in *Internet Research*. 24(2), pp. 160-180.

Heggestuen, J. 2014. "*The Future Of Mobile And Online Banking: 2014".* Retrieved on Feb 02, 2015 at http://www.businessinsider.com/the-future-of-mobile-and-online-banking-2014-slide-deck-2014-10?op=1

Huang, S. 2015. "*The South Korean Fake Banking App Scam*", Retrieved on Feb 02, 2015 at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-south-korean-fake-banking-app-scam.pdf

Ilkay, A., Berkley, C., Jaeger, E., Jones, M., Ludascher, B., and Mock, S. 2004. "Kepler: an extensible system for design and execution of scientific workflows", in *Proceedings of the 16th Conference on Scientific and Statistical Database Management (SSDBM)*, pp. 423-424, Santorini Island, Greece.

Jeong, B. K., and Yoon, T. E. 2013. "An Empirical Investigation on Consumer Acceptance of Mobile Banking Services", in *Business and Management Research*, 2(1), 31-40.

La Polla, M., Martinelli, F., and Sgandurra, D. 2013. "A survey on security for mobile devices", in *Communications Surveys & Tutorials, IEEE*, 15(1), 446-471.

Lee, H., Zhang, Y., and Chen, K. L. 2013. "An Investigation of Features and Security in Mobile Banking Strategy", in *Journal of International Technology and Information Management*, *22*(4), Article 2.

Khosla, V. 2015. "*Behavioral Analysis Could Have Prevented The Anthem Breach*", Retrieved on Feb. 22, 2015 at http://www.forbes.com/sites/frontline/2015/02/24/behavioral-analysis-could-have-prevented-the-anthem-breach/

Legnitto, J. 2013. "*Mobile Banking On Unsecure Wireless Networks Is Risky Business*", Retrieved on Feb 22, 2015 at http://www.privatewifi.com/title-mobile-banking-on-unsecure-wireless-networks-is-risky-business/

Panja, B., Fattaleh, D., Mercado, M., Robinson, A., and Meharia, P. 2013. "Cybersecurity in banking and financial sector: Security analysis of a mobile banking application", In *Collaboration Technologies and Systems (CTS), 2013 International Conference on* (pp. 397-403). IEEE.

Potter, B. 2006. "User education–how valid is it?", in *Network Security*, 2006(4), 15-16.

Pousttchi, K., and Schurig, M. 2004. "Assessment of today's mobile banking applications from the view of customer requirements", In *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on* (pp. 10-pp). IEEE.

Regalado, P. 2014. "*SSL Vulnerabilities in Your Mobile Apps: What Could Possibly Go Wrong?*", Retrieved on Feb 22, 2015 at https://www.venafi.com/blog/post/ssl-vulnerabilities-in-your-mobile-apps-what-could-possibly-go- wrong/

Rubin, V. L., Burkell, J., and Quan-Haase, A. 2011. "Facets of serendipity in everyday chance encounters: a grounded theory approach to blog analysis", in *Information Research*, 16(3). Retrieved on Feb 22, 2015 at http://www.informationr.net/ir/16-3/paper488.html

Ryan W. J. 2014. "A Resource Guide for Bank Executives: Executive Leadership of Cybersecurity", in *proceedings of the Conference of State Bank Supervisors*. Retrieved on Feb 22, 2015 at http://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf

Schneider, I. 2012. "*Five Bank Security Trends Shaping the Future of Fraud Fighting*", Retrieved on Feb 22, 2015 at http://www.banktech.com/five-bank-security-trends-shaping-the-future-of-fraud-fighting/d/d-id/1295580?

Shih, D. H., Lin, B., Chiang, H. S., and Shih, M. H. 2008. "Security aspects of mobile phone virus: a critical survey", in *Industrial Management & Data Systems*, 108(4), 478-494.

Singh, S., Srivastava, V., and Srivastava, R. K. 2010. "Customer acceptance of mobile banking: A conceptual framework", in *Sies journal of management*, *7*(1), 55-64.

Webroot. 2014. "*The risks & rewards of mobile banking apps*", Retrieved on Feb 22, 2015 at http://www.brightcloud.com/pdf/RisksRewardsofMobileBankingAppsWhitepaper_20140619115948_311111.pdf

whiteCryption. 2014. "whiteCryption Introduces New Level of Security for Mobile Payment Applications", Retrieved on Feb 22, 2015 at http://www.prweb.com/releases/2014/01/prweb11531529.htm

White, A. 2013. "*Six Main Rules Of Safe Mobile Banking. Where, When And How?",* Retrieved on Feb 22, 2015 at http://blog.jammer-store.com/2013/05/six-main-rules-of-safe-mobile-banking-where-when-and-how/

Wisniewski, M. 2013. "Mobile Check Deposit Boom Brings Risks", Retrieved on Feb 22, 2015 at http://www.americanbanker.com/issues/178_133/the-lesser-known-risks-of-mobile-check-deposit-1060543-1.html?pg=2

Yu, J. and Buyya, R. 2005. "A taxonomy of workflow management systems for grid computing", in *Journal of Grid Computing*. 3(3-4), pp. 171-200.