Examining Security Risks of Mobile Banking Applications through Blog Mining

Wu He, Xin Tian & Jiancheng Shen
Old Dominion University, Norfolk, VA, USA
whe@odu.edu; xtian@odu.edu; jshen@odu.edu

Abstract

This paper provides an in-depth review of the security aspect of mobile banking applications. The authors employed blog mining as a research method to analyze blog discussion on security of mobile banking applications. Security risks, protection strategy/best practices and future security trends are summarized to help banks and consumers mitigate the security risks of mobile banking applications.

Introduction

Many people are using their mobile devices such as smart phones to access various online services on a daily basis. In particular, mobile banking applications are increasingly becoming popular. Many banks are offering mobile banking services which allow bank customers to check balance in their personal account, to transfer funds between accounts and make online payments anywhere and at anytime by simply using mobile banking applications installed on their mobile devices (Elkhodr et al., 2012). Moreover, customers can receive alerts from banks such as overdraft alerts, low balance warnings, recent large transactions, and so on (Panja et al., 2013).

Unfortunately, mobile malware has been increasing in frequency and sophistication in the past five years and has caused a variety of damages including leaking of sensitive financial data, financial loss and identify theft (He, 2013). In particular, mobile banking apps have attracted the attention of many cyber criminals (Panja et al., 2013). There are a lot of concerns with the security aspect of mobile banking since mobile devices are vulnerable to threats, attack and loss (Claessens et al., 2002).

In an effort to address the increasing threat, researchers and security vendors have been developing new practices, techniques and solutions to reduce security risks associated with mobile banking applications. To help readers understand the state-of-the-art in this fast-moving area, the authors synthesize the related discussions in literature and provide an in-depth review of the security aspect of mobile banking. Currently, the discussion of security risks of mobile banking is disparate, fragmented and distributed in different outlets such as academic articles, white papers, security threat reports and news articles. The authors employed blog mining as a research method to analyze blog discussion on mobile banking applications. Best practices are summarized to help banks and consumers mitigate the security risks of mobile banking.

Literature Review

Mobile banking has been developed as an effective and convenient channel for financial institutions to distribute their services to clients (Mallat et al., 2004; Nie & Hu, 2008; Lin, 2011; Elkhodr et al., 2012). Mobile banking makes financial services easily accessible for customers through a handheld device (Singh et al., 2010). However, the wide use of smartphones is also accompanied with an equally alarming rise in mobile malware (Seo et al., 2012). Security is considered as a priority for many mobile banking customers. 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).

Cyber security experts suggested that the cyber-attacks against financial services institutions are becoming more frequent and more sophisticated (Cuomo, 2014; Ryan, 2014). Overall, there are several cyber security concerns with regard to mobile banking. Security on mobile banking is complicated because of the variety of mobile devices and platforms (He, 2012; Lee et al., 2013). The security and privacy of sensitive financial data is one of the main concerns in acceptance of the mobile banking applications (Elkhodr et al., 2012). The limited privacy protection experience and fewer resources of independent developers decrease the effectiveness of cyber security protection on the mobile applications (Balebako & Cranor, 2014). The weak and rigid authentication provided by signature, PIN, pass-

word and Card Security Code (CSC) in mobile banking have numerous flaws and loop-holes (Edge & Sampaio, 2009).

To prevent the cyber fraud, and facilitate a safe and robust mobile banking system, many 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 in account signatures, an innovative account profiling technology that can improve the fraud detection mechanisms. Fatima (2011) posited biometric based authentication and identification systems as new solutions to address the issues of security and privacy, which imposes restrictions to prevent individuals from accessing to certain physical spaces and electronic services. Elkhodr et al. (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. 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. Ease of use is a key factor for consumer acceptance of mobile banking services (Jeong & Yoon, 2013).

Methodology

The authors employed a relative new research method called blog mining to find blogs that discuss security of mobile banking applications. This method has been shown to be very useful in information and internet research (Rubin et al., 2011). An analysis of active blogs can add currency and relevancy to research studies (Chau & Xu, 2012; He & Zha, 2014). As mobile banking is a young and fast-moving area, many relevant discussions were posted by technology consultants and security experts on blogs. Thus, those blogs are a very useful data source for learning about concerns associated with mobile banking. A limitation with blog mining is that the information on blogs is not peer reviewed as journal publications and often represents personal opinions and attitudes. One way to mitigate this limitation is to combine blog mining with an extensive literature search for a more comprehensive understanding of the topics that are under investigation.

Specifically, we used Google blog search engine (http://www.google.com/blogsearch) to search for blogs using the keywords including "mobile banking security" and "mobile apps vulnerability". Google Blog Search is specially designed to retrieve content from blogs that are freely and publicly available on the Internet. 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. These top 100 blog posts were saved as text files on the hard drive for text mining and analysis. A well-known text analytics tool named NVivo 10 was used for text mining and analytics. We mainly used NVivo 10 software to conduct various query searches and cluster analysis in order to find interesting patterns, connections, and key themes.

Blog Mining Results

After reviewing the generated concept themes and clusters, the authors merged some sub-clusters manually. Finally, three major clusters associated with the blog discussion about security of mobile banking apps were identified. The emergent clusters and main concept terms in the text were summarized in Table 1. A word cloud can be seen in Figure 1.

Table 1. Main Blog Themes on Mobile Banking App Security

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

Figure 1. A word cloud about 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 we were particularly interested in the main threats, attacks and vulnerabilities related to mobile banking applications, we presented a 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. Some common malware affecting mobile bank apps include Zitmo, Banker, Perkel/Hesperbot, Wrob, Bankum, ZertSecurity, DroidDream and Keyloggers. Many of mobile malware are variants of existing malware that affect computers and traditional online banking (Webroot, 2014; Shih et al., 2008). Cyber criminals have been refining these malware to target mobile devices for access to bank accounts and make them more resilient to security defenses. Below are 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 Wi-Fi networks. Public Wi-Fi networks in coffee shops, libraries, airports, hotels, and other public places are often not 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 mobile banking apps. 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 Strategy 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 et al., 2013; Chandramohan & Tan, 2012; La Polla et al., 2013; White, 2013). We listed some protection strategy/best practices for users and developers of mobile banking app respectively below.

Protection strategy and best practices for users

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

Strategy	Rationale	Best Practices
Do not use mobile banking app on jailbreak smartphone	Many people jailbreak their smart phones in order to get additional benefits. However, jailbreaking smart phones 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.

Protection strategy and best practices for developers of mobile banking apps

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

Title	**Description**	**Protection strategy/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	Application must prevent debuggers from attaching to it to avoid the leak of 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 accounts 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 addes additional security for identity verification when banking app users log in or performing certain transactions.

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). 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).

Conclusion and Future Research

Mobile banking offers a lot of benefits to both banks and consumers. However, security is a significant barrier to the wide adoption of mobile banking applications (To & Lai, 2014). As there are many security risks with the use of mobile banking applications, it is critical for both banks and consumers to be aware of these risks and take steps to mitigate the risks. Currently, there is lack of systematic discussion in the literature about the security risks with mobile banking. In this paper, we identified some key security risks, protection strategy/best practices and future security trends associated with mobile banking through mining relevant blog posts.

As for future research, we plan to use the workflow technology to simulate 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. 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.

Acknowledgment

This work was supported in part by the U.S. National Science Foundation under Grant SES-1318470 and SES-1318501.

References

Balebako, R., & Cranor, L. (2014). Improving App Privacy: Nudging App Developers to Protect User Privacy. *Security & Privacy, IEEE*, *12*(4), 55-58.

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

Chau, M., & 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., & 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 22, 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

Cuomo A. M. (2014). *Report on Cyber Security in the Banking Sector*. New York State Department of Financial Services. Retrieved on Feb 22, 2015 at http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf

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

Elkhodr, M., Shahrestani, S., & 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. *Journal of Internet Banking and Commerce*, 16(2): 2011-08.

He, W. (2012). A Review of Social Media Security Risks and Mitigation Techniques. *Journal of Systems and Information Technology*, 14(2), 171-180.

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

He, W., & Zha, S.H. (2014). Insights into the Adoption of Social Media Mashups. *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

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

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

Lee, H., Zhang, Y., & Chen, K. L. (2013). An Investigation of Features and Security in Mobile Banking Strategy. *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/

Lin, H. (2011). An empirical investigation of mobile banking adoption: The effect of innovation attributes and knowledge-based trust. *International journal of information management*, 31(3): 252-260.

Mallat, N., Rossi, M., & Tuunainen, V. K. (2004). Mobile banking services. *Communications of the ACM*, 47(5), 42-46.

Nie, J., & Hu, X. (2008). Mobile banking information security and protection methods. In *Computer Science and Software Engineering, 2008 International Conference on* (Vol. 3, pp. 587-590). IEEE.

Panja, B., Fattaleh, D., Mercado, M., Robinson, A., & 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.

Pousttchi, K., & 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.

Rubin, V. L., Burkell, J., & Quan-Haase, A. (2011). Facets of serendipity in everyday chance encounters: a grounded theory approach to blog analysis. *Information Research*, 16(3).

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

Seo, S. H., Gupta, A., Sallam, A. M., Bertino, E., & Yim, K. (2014). Detecting mobile malware threats to homeland security through static analysis. *Journal of Network and Computer Applications*, *38*, 43-53.

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

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

To, W. M., & Lai, L. S. (2014). Mobile Banking and Payment in China. *IT Professional*, 16(3), 22-27.

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/