Mobile Banking: Privacy and Security Vulnerabilities

Julia Grace

December 12th, 2016

1 Abstract

In recent years, mobile banking has become extremely popular for its overwhelming convenience. In a matter of seconds, users of apps such as the Bank of America mobile banking app can check their account balance, deposit checks, and move money between accounts. However, many people are wary of mobile banking out of fear that their money and information aren't safe. While mobile banking is much easier and more convenient than visiting a bank or ATM in person, exchanging financial information via the internet, or any information for that matter, exposes that information to many new potential threats. This paper will examine several privacy and security vulnerabilities pertaining to mobile banking and discuss some steps mobile banking app users can take to help protect their money and data.

2 Introduction

2.1 A Brief History

PayBox, a European company backed by Deutsche Bank, released the first mobile banking application in 1999. This application, which used SMS,

gained little traction at first due to the high cost of data plans, slow network speed, and general lack of hardware and software support for such a service at the time. Mobile Banking wasn't introduced in the U.S. for another 7 years until Wachovia bank introduced an application in 2006. In the years following, millions of users began to use mobile banking applications in tandem with online banking, as mobile banking offered only a subset of the services offered online at the onset [10]. As the apps and their host devices advanced and caught up with the online banking applications, more users turned to mobile banking as their primary bank interaction. Unfortunately, as the popularity for mobile banking grew, so did the interest of the hacker community. Ten years after the introduction of mobile banking in the United States, security remains one of the greatest concerns for users and banking institutions.

2.2 To the Community

Banking is an integral part of society and has been for thousands of years. With the growing popularity of mobile banking applications, banking is more convenient than ever. Customers no longer have to take time off of work or travel to visit their bank for small actions such as depositing checks or transferring money. Their account balance and other important information is now available anywhere they go at the touch of a few buttons. One of the most important features of a bank is to protect and keep track of customers' money so they don't have to. Most users of mobile banking applications trust their banks to protect them from dangers such as identity theft, blackmail or ransom and are thus unconcerned about the potential security vulnerabilities associated with mobile banking. This paper is intended to educate the community about several potential vulnerabilities so users can protect themselves with smart practice when possible and demand more protection from their banks when control is out of their hands.

3 Vulnerabilities

3.1 Social Engineering and Fake or Tampered Applications

Malcolm Allen of the SANS Institute describes Social Engineering as "a threat, often overlooked but regularly exploited; to take advantage of what has long been considered the 'weakest link' in the security chain of an organization -- the 'human factor'" [4]. Social Engineering is a common tactic used to trick users of an application into providing private data or subjecting themselves to malicious technology often used in relation to mobile banking. A common tactic for "Trojan Bankers", as *SecureList* Blogger Fabio Assolini calls them, is to trick users into downloading a fake version of a mobile banking app from an app store such as the Google Play store. In his article, *Brazilian Trojan Bankers – now on your Android Play Store!*, Assolini writes about an incident in 2014 when 2 Brazilian men hosted malicious banking apps on the Google Play store. The Trojans tricked users into downloading these applications by using the logos of local Brazilian Banks. When users logged into these apps, their credentials were recorded and sent to the apps creators [5]. A similar tactic was used in 2010 when a First Tech Credit Union mobile banking application appeared on the Google Play store. At the time, First Tech Credit union did not have a mobile banking app and released a statement warning users not to use to download this app [3]. Often, malicious social engineers are more direct with their attacks. As Professor Sam Bowne of City College of San Francisco suggests, attackers may post a link to their malicious apps on a web site or send one in an email. Bowne found that several mobile banking apps including the Citibank and Capital One apps do not check if their apps have been tampered with when connecting to their servers. Thus, hackers can tamper with an application, send unsuspecting users an email with a tampered version of a real mobile banking app, and use the tampered app to collect important financial and personal information [6, 7].

3.2 Malware

According to a 2015 study published by RiskIQ, 11 percent of all mobile applications referencing banking contain some sort of malicious or suspicious code. Out of 350,000 applications, 40,000 were flagged as containing adware, Trojan malware, spyware, exploit code, or malicious JavaScript [8]. However, these malicious mobile applications are not all mobile banking users have to worry about. In 2014, Kaspersky Lab discovered that a Russian malware called Svpeng targeting users of mobile banking applications had made its way

from Europe to the U.S. Svpeng is loaded onto mobile devices through a social engineering campaign using text messages. Once on the device, the malware searches for particular mobile banking applications including the American Express, Wells Fargo, and Bank of America apps. If one of the apps is found on the phone, the screen locks and a fake FBI penalty letter and $200 ransom appear on the screen in addition to a photograph of the user captured by the phone's camera. The phone remains locked until users purchase MoneyPak vouchers and provide the voucher numbers according to Svpeng's instructions. According to Roman Unuchek of Kaspersky Lab, "Customers who fall victim to Svpeng can do almost nothing" [1, 9].

3.3 Excessive Permissions

In the same 2015 study by RiskIQ mentioned in section 4.1, researchers found that 40,000 of the 35,000 apps pertaining to mobile banking were found to exhibit excessive permissions. Of the 40,000 applications, nearly 9,000 could capture device logs and nearly as many could record audio. Around 7,000 apps could access contact lists, nearly 5,000 could actually read SMS messages and around 4,000 could disable key guard and read a mobile device's settings. Other permissions commonly found on these applications included accessing GPS information, writing to contacts and installing packages. Peter Zavlaris, a RiskIQ blogger, explained that permission for a mobile app to access data stored on a phone "isn't always a bad thing". However, should an app be compromised, he warns, an attacker instantly has "access to information he or she can use to exploit the user, sometimes even without using any malware at all" [8].

3.4 Information Leaking and Insecure Transmission

Senior Security Consultant at IOActive Ariel Sanchez performed static and dynamic analysis of 40 iOS mobile banking apps from among the 60 most influential banks in world. His analysis revealed that a staggering number of these application contained major security flaws often pertaining to information leakage via insecure transmission of information between the

client and server side. For example, Sanchez found that 90 percent of these applications were vulnerable to traffic interception and JavaScript and html injection due to the use of non-SSL links. This vulnerability allows for scams such as injecting a fake login prompt to collect users login credentials. 50 percent of these applications were vulnerable to cross-site scripting "via insecure UIWebView implementations... allowing actions such as sending SMS or emails from the victim's device." Among his other findings were log files that exposed sensitive data, unencrypted SQLite databases, and hardcoded development credentials. Sanchez also concluded that 40 percent of these apps were vulnerable to "man in the middle" attacks as they do not validate the authenticity of SSL certificates presented by the client to the server. Sanchez's findings reveal that many of the worlds top financial institutions have drastically low standards for securing the private information of their users and the integrity of their mobile banking applications [2].

4 In the Future

4.1 Advice to Users

As hackers commonly target mobile banking application users through social engineering, it is important that users educate themselves on popular social engineering tactics. One such tactic described in this paper was emailing or texting potential mobile banking users fake or tampered applications. Users who are aware of this tactic can protect themselves by blocking suspicious emails. Users can also log on the their online banking account to search for similar information or updates. If the bank's official website is not advertising the application it is likely fake. If it is, it is best to follow links from the official website to the App or Google Play stores to ensure that you choose the correct application. Often, malicious software such as Svpeng, which targets mobile banking users, is downloaded from infected websites via "drive-by" attacks as Editor of BankInfoSecurity Tracy Kitten calls them. The best defense for users from such attacks is to keep anti virus applications up to date and to install software to detect ransomware and malware when available [1]. In regard to excessive permissions for mobile applications, users should be sure not to store any login credentials in plain text on their device and to turn off unnecessary services such as location services when they are not needed for the functionality of an application. This paper also identified many security vulnerabilities in the data transmission and storage process that users

still have little ability to protect themselves from. Thus, it is always important to use multi-factor authentication when available and use different passwords for different accounts, as login credentials for mobile banking applications are often still not totally secure.

4.2 Advice to Bankers and Developers

It is clear that the standard for security in mobile banking applications is not as high as it needs to be in order to protect the privacy of its users. Senior Security Consultant at IOActive Ariel Sanchez suggests the following lists of defense recommendations:

- Ensure that all connections are performed using secure transfer protocols
- Enforce SSL certificate checks by the client application
- Protect sensitive data stored on the client-side by encrypting it using the iOS data protection API
- Improve additional checks to detect jailbroken devices
- Obfuscate the assembly code and use anti-debugging tricks to slow the progress of attackers when they try to reverse engineer the binary
- Remove all debugging statements and symbols
- Remove all development information from the production application [2]

Additionally, Professor Sam Bowne of City College of San Francisco suggests that server-side code should check the integrity of the client-side, the mobile banking application, before connecting, blocking tampered applications from access to server-side data [6, 7]. Bankers and developers also need to educate users about safe habits and how to recognize signs of social engineering. Jeremy Demar, director of the threat research team at Damballa, suggests that the best people for the job are the national Computer Emergency Readiness Teams. He also suggests that the best way to reach a large audience is through Radio and Television PSAs. Etsy Maor, malware researcher at IBM security firm Trusteer, recommends combatting present security concerns in mobile banking applications by requiring a more robust authentication process for users such as two-factor authentication [1].

5 Conclusion

Mobile Banking has obvious utility, but also many inherent risks. With its growth in popularity, mobile banking applications have become a popular target for the hacker community. Vulnerabilities to users include fake and tampered applications distributed through social engineering, malware targeting mobile banking applications, excessive permissions, and information leaking and insecure data transmission. It is up to users, banks, and developers to educate themselves on such vulnerabilities and take actions to protect users from threats such as blackmail, identity theft and ransom. Users must know the common signs of social engineering and developers and bankers must provide a higher standard of security for their mobile banking customers.

References

[1] *New Ransomware Targets Mobile.* Accessed: 2016-12-11. BankInfoSecurity. URL: http://www.bankinfosecurity.com/-a-6867.

[2] *Personal banking apps leak info through phone.* Accessed: 2016-12-11. IOActive. URL: http://blog.ioactive.com/2014/01/personal-banking-apps-leak-info-through.html.

[3] *Fake Mobile Banking App Discovered in Android Marketplace.* Accessed: 2016-12-11. PhoneNews. URL: http://www.phonenews.com/fake-mobile-banking-app-discovered-in-android-marketplace-9949/.

[4] *Social Engineering: A Means To Violate A Computer System.* Accessed: 2016-12-11. SANS. URL: https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529

[5] *Brazilian Trojan Bankers = now on your Android Play Store!* Accessed: 2016-12-11. Kaspersky Lab. URL: https://securelist.com/blog/virus-watch/67661/brazilian-trojan-bankers-now-on-your-android-play-store/.

[6] *Citibank Android App Vulnerability*. Accessed: 2016-12-11. Sam Bowne. URL: https://samsclass.info/128/proj/citi.htm.

[7] *Capitol One Android App Vulnerability*. Accessed: 2016-12-11. Sam Bowne. URL: https://samsclass.info/128/proj/cap1.htm.

[8] *11 percent of mobile banking apps include harmful cod.* Accessed: 2016-12-11. Security Affairs. URL: http://securityaffairs.co/wordpress/33212/malware/mobile-banking-apps-suspect.html

[9] *First Major Mobile Banking Security Threat Hits the U.S.* Accessed: 2016-12-11. American Banker. URL: http://www.americanbanker.com/issues/179_114/first-major-mobile-banking-security-threat-hits-the-us-1068100-1.html

[10] *Examining The History of Mobile Banking Information Technology Essay*. Accessed: 2016-12-12. UK Essays. https://www.ukessays.com/essays/information-technology/examining-the-history-of-mobile-banking-information-technology-essay.php.

[11] *How to Spot a Fake Android App*. Accessed: 2016-12-13. Symantec Corporation. URL: https://community.norton.com/en/blogs/norton-protection-blog/how-spot-fake-android-appjp.