Bank of America Mobile App Security

Anne Oursler
Mentor: Ming Chow
Tufts Department of Computer Science

Money rarely physically changes hands today, yet it moves more than it ever could before. Everything from small personal exchanges to large bank transfers happens digitally, including on phones. When a system works a few times and has a smooth user interface, it is assumed that it will function perfectly. The edge cases are never considered the way they would be with physical money. Where once carrying an entire bank account in one's pockets would have inspired fear of mugging, today these fears are forgotten, and yet they are more relevant than ever. This paper aims to look into the security of one such major app that holds trillions of dollars in finances: Bank of America. Biased on the findings, it will then make a judgment of Bank of America's security in comparison to its peers. Finally, it will make recommendations for both Bank of America and its customers in order for both to improve the security of their finances.

Bank of America is the second largest bank in America today, holding around $2.15 trillion in total assets (Bell). Among its 47 million patrons, between 15-19 million do their banking through the Bank of America Mobile App (The Birth of Mobile Banking). The mobile app is separate from Bank of America's online web portal; it is a platform that can only be run on smartphones. Bank of America offers its

Mobile app for both Android and iOS, on both on the Android Play Store, and On the Apple App store. It was created in 2007 by Bank of America, and has been updated by Bank of America software engineers since then (The Birth of Mobile Banking).

The Bank of America app is growing in popularity as a convenient method of banking. Although it only accounts for one third of online banking use from Bank of America, there are still millions of users who entrust the Bank of America app with their financial security. Bank of America advertises that users of their app can "Check balances and recent transactions, Deposit checks, Transfer funds and pay bills, Send money to virtually anyone using email address or mobile number, Schedule appointments to meet with us, Report a lost or stolen card and order replacement cards, Receive alerts, and notifications" (The Birth of Mobile Banking). With this much power over entire bank accounts, the security of the Bank of America Financial app is critically important.

Bank of America's Security Claims

Bank of America claims that its users should be confident in banking through their mobile app because of its online mobile banking security guarantee and its award winning security. Its Guarantee essentially states that fraud done on most app transactions will be fully refunded. They claim: "we guarantee that you will not be liable for fraudulent transfers or bill pay transactions*, we will help keep your financial information safe and we will process your payments based on your online or mobile banking instructions" (Online Banking Security Guarantee). The exception here is mobile check deposits, which are not part of Bank of America's Mobile Banking Security Guarantee (Online Banking Security Guarantee). This claim is quite reassuring, although it does not cover the identity theft and general inconvenience that

using the Bank of America Mobile app could lead to. Thus the security of the app is still relevant to its users, and certainly to Bank of America itself.

In the description of the security of Bank of America's Mobile app, Bank of America claims: "For 9 years in a row, Bank of America has earned the respected and coveted Best Overall Identity Safety in Banking Award by Javelin Strategy & Research" (Online Banking Security Guarantee). While this seems like a wonderful indicator of the app's security, there are two catches. The first catch is that although Bank of America won the Javelin Award, it only scored 81% of the possible points (Javelin). The break down of these points further reveals that although Bank of America did well in Detecting attacks (93%) and relatively well in resolving attacks (83%), it did very poorly in preventing attacks (69%) (Javelin). The app seems to be far more focused on paying its customers back when it gets hacked than simply preventing the hack in the first place. However, This is all a bit irrelevant because despite Bank of America listing the Javelin award on their Mobile App webpage, the Javelin award only applies to bank of America's web portal based banking. Thus even the questionable security that Javelin found may not be as solid as the security of the Bank of America Mobile App.

Aside from the Javelin award, Bank of America's mobile security website claims to use three methods to protect user data. They claims: "Authentication ensures that you are communicating with us and prevents another computer from impersonating Bank of America, Encryption scrambles transferred data so that it cannot be read by unauthorized parties, Data integrity, in terms of data and network security, assures that information can only be accessed and modified by those authorized to do so" (Online Banking Security & Support). To

supplement this, Bank of America recommends that customers update mobile devices, guard personal information, use a digital wallet, think before they app, protect their money, when in doubt don't respond, and stay informed (Mobile Banking Security). Together Bank of America claims these factors are adequate security for their app.

Security Analysis

Trojan App

The Bank of America Android app is relatively easy to edit, and Bank of America's servers don't check the integrity of the app when it connects (Bowne, Bank of America). Thus a Trojan app can be built which logs or possibly sends information such as a user's ATM card number and ATM card pin to an attacker as demonstrated by Sam Bowne (Bowne, Bank of America). The attack only needs to insert four lines, and alter one line of code for this Trojan app, and all five of those lines are in the same section of the same file (Bowne, Bank of America). By altering the AtmDebitDetailsActivity.smali file, attackers can get enough data to have full access to the bank account of anyone who uses the Trojan app. Bank of America does not consider this a large threat because a user would have to download the app from a non-app-store source. However people tend to be to fundamental flaw in security, and it is never a valid assumption that a user will not do something to compromise security. The only valid security measure is to compensate when they enviably do. Bank of America has not taken this flaw seriously, and as such their servers still fail to authenticate their app. They have since updated their app multiple times, and this attack is still valid (Bowne, Bank of America).

Passwords

I was alerted to the possibly that Bank of America might require their

customers to use insecure passwords via Bad Password Rule on twitter, and because it was an easy and legal thing for me to check on my own looked into it (Rule, Bad Password). Bank of America requires its customers to have passwords that are: 8 to 20 characters, use a least 1 upper case letter, 1 lower case letter, and 1 number, do not repeat the same number or letter more than 3 times in a row, do not contain spaces, and may only use the special characters @ # * ( ) + = { } / ? ~ : , . - and _ . While some of these requirements force the average user to set more secure passwords, limiting the length of a password, forbidding spaces, and limiting special characters all make Bank of America Passwords easier to crack. As this password is used for both the Bank of America Web site, it is relevant to mobile app user and many other customers of Bank of America.

Two-Factor Authentication

Bank of America's Mobile app has two-factor authentication to support its security. However it is not required unless a particularly large transfer is being made (SafePass). This means that while customers who care about security can have easy access to two-factor authentication, customers who are less knowledgeable have weakened account security. In addition when two-factor authentication is installed, the Mobile app still gives SMS as a second factor. This is problematic on two fronts. One if the phone was stolen, both the app and the second factor are in the hands of an attacker. Secondly, SMS as a second factor is not secure. It has been demonstrated that at through social engineering, the SIM card of a customer's phone can be transfer to that of an attacker (Division of Consumer Protection) (Greenberg) (Zetter). Bank of America offers a true second factor, called SafePass, which can be bought for around

twenty dollars, however this key is only for use in large transfers, not for login, and it can be replaced with an SMS message, thus losing the security of the second factor. Over all this makes the mobile app less secure for consumers.

Analysis Results in Context

While these flaws may seem major, they are actually quite common among banking applications. Sam Bowne's Trojan App worked on five of the 8 major banking companies he tried it on (Bowne, Android Apps). Many other Banks share the same poor password practices such as upper limits and restrictions on special characters (Collins). Some of these top banks even lack two-factor authentication entirely (Collins). While Bank of America's security is inadequate in many ways, the fact that Bank of America's competitors have much the same practices means that switching to another bank doesn't increase the average consumer's security.

To Consumers

Customers of Bank of America using the mobile app should keep in mind that although the Bank of America app has many weaknesses, the user is the biggest one. Bank of America's suggestions to its consumers are extremely relevant. Be wary of phishing attacks. Emails, texts, or calls that ask for personal information are almost always scams (Mobile Banking Security). Bank of America's password practices make it doubly important to ensure that all passwords are random, unique, and long. In addition although SMS two-factor authentication is less secure than a true second factor, it is still another layer of security over a Bank of America bank account. In addition Bank of America Customers should be sure to read the fine print of the Bank of America security policies to learn when bank of America Insurance doesn't apply, such as when you are depositing checks (How to Protect Your

Financial Apps). They should consider avoiding behavior that puts them at personal risk. Finally, customers should have good general Internet practices, such as minimizing contact with public networks and keeping in mind that accessing your bank in this manner is public to anyone who wants to watch. For any customers who still feel that this level of security is inadequate, consider banking in person, without a Mobile or Web app.

To Bank of America

Customers are the biggest security risks to their own accounts, but it is Bank of America's job to minimize the damage they can do to themselves. Trojan versions of your app will almost certainly exist, however validating the app every time it contacts the servers can go along way towards user's security. In addition, although users will always attempt to create weak passwords, Bank of America help prevent this by creating rules that foster stronger passwords, and removing rules that force weaker passwords. Passwords stored in a properly salted and hashed manner should not need such a severe upper character limit. In addition Bank of America should stop its customers from creating passwords that are extremely common or recently hacked. Instead encourage customers towards passwords that are harder for machines to guess. Consider making two-factor authentication mandatory, and even mandating a true second factor. Such a second factor could be as simple as Google Authenticator, or as complicated as a physical fob, given to customers as part of setting up their Bank of America accounts. Finally Bank of America should consider either backing all of the services it provides, or ceasing support for those services it will not back, such as check deposits.

Conclusions

Thorough this paper I have shown that Bank of America has insufficient

security considering their control over finances. However I suspect that the flaws in their security are far more widespread than those I could uncover online. Were it not for Bank of America's strong dislike of third parties testing their code I would have liked to do a more complete review of the app's security. However Bank of America does not offer bug bounties, and upon speaking to a member of the Bank of America security team I got the distinct impression that Bank of America did not want anyone touching their work. I would have liked to try some common attacks, more specifically the owasp top ten and the owasp top ten mobile. I would be quite surprised if all of these attacks failed, however being able to test and prove this with their permission would add an air a legitimacy to Bank of America's security. Without this, and with Bank of America's false claim of the Javelin award, I must instead conclude that Bank of America is not confident in their own security, perhaps because they have no reason to be.

References

Bell, Claes. "Americas 10 Biggest Banks | Bankrate.com." Americas 10 Biggest Banks. Bankrate, n.d. Web. 02 Dec. 2016. <http://www.bankrate.com/finance/banking/americas-biggest-banks-1.aspx>.

Bowne, Sam. "Android Apps Vulnerable to Code Modification." Android Apps Vulnerable to Code Modification. N.p., n.d. Web. 06 Dec. 2016. <https://samsclass.info/android/codemod.html>.

Bowne, Sam. "Bank of America Android App Vulnerability." Bank of America Android App Vulnerability. N.p., n.d. Web. 06 Dec. 2016. <https://samsclass.info/android/boa.htm>.

Collins, Keith. "Your Checking Account Is Probably Easier to Hack into than Your Email." Quartz. N.p., 01 Mar. 2016. Web. 06 Dec. 2016. <http://qz.com/626404/hackers-arent-trying-to-guess-your-online-banking-password/>.

"Division of Consumer Protection." Division of Consumer Protection. New York State, n.d. Web. 06 Dec. 2016. <https://www.dos.ny.gov/consumerprotection/scams/att-sim.html>.

Greenberg, Andy. "So Hey You Should Stop Using Texts for Two-Factor Authentication." Wired. N.p., n.d. Web. 06 Dec. 2016. <https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication/>.

"How to Protect Your Financial Apps from Hackers." CNBC. CNBC, 06 Aug. 2016. Web. 06 Dec. 2016. <http://www.cnbc.com/2016/08/06/how-to-protect-your-financial-apps-from-getting-hacked.html>.

Javelin Strategy and Research. "Javelin's 2014 'Identity Safety in Banking' Award Winners." (n.d.): n. pag. Web. <https://www.javelinstrategy.com/sites/default/files/2014_Identity_Safety_Banking_JavelinAward_0.pdf>.

"Mobile Banking Security from Bank of America." Mobile Banking Security from Bank of America. Bank of America, n.d. Web. 06 Dec. 2016. <https://www.bankofamerica.com/privacy/online-mobile-banking-privacy/mobile-banking-security.go>.

"Online Banking Security Guarantee from Bank of America." Bank of America. Bank of America, n.d. Web. 02 Dec. 2016. <https://www.bankofamerica.com/onlinebanking/online-banking-security-guarantee.go>.

"Online Banking Security & Support FAQs from Bank of America." Bank of America. Bank of America, n.d. Web. 06 Dec. 2016. <https://www.bankofamerica.com/onlinebanking/online-banking-security-faqs.go>.

Rule, Bad Password. "Insecure Password Rules @BankofAmerica: Limiting Max Length and Special Chars and Enforcing Upper, Lower, and Number Pic.twitter.com/h85M0q6Sly." Twitter. Twitter, 25 Apr. 2016. Web. 06 Dec. 2016. <https://twitter.com/BadPasswordRule/status/724733593990254592>.

"SafePass® Online Banking Security Enhancements." SafePass® Online Banking Security Enhancement. Bank of America, n.d. Web. 06 Dec. 2016. <https://www.bankofamerica.com/privacy/online-mobile-banking-privacy/safepass.go>.

"The Birth of Mobile Banking." About Bank of America. Bank of America, 12 Aug. 2014. Web. 02 Dec. 2016. <http://about.bankofamerica.com/en-us/our-story/the-birth-of-mobile-banking.html>.

Zetter, Kim. "The Critical Hole at the Heart of Our Cell Phone Networks." Wired. N.p., n.d. Web. 06 Dec. 2016. <https://www.wired.com/2016/04/the-critical-hole-at-the-heart-of-cell-phone-infrastructure/>.