ZIMPERIUM®
MOBILE THREAT DEFENSE

Mobile Banking:

Big Business, Big Target, Big Opportunity

Mobile Banking:
Big Business, Big Target, Big Opportunity

Mobile devices now constitute the majority of web traffic globally, and consumers are embracing mobile banking in record numbers. Meeting customer demand for mobile banking presents opportunities for banks to differentiate themselves, but providing mobile banking applications also entails significant risk.

SC Magazine's analysis of mobile applications from 50 of the world's top 100 banks found **all** to be vulnerable to several security threats. The apps had an average of seven security flaws, and put half a billion mobile banking customers at risk[i]. Mobile strategies that mitigate security risks and provide safer transactions will gain a significant advantage in the highly competitive and fast-growing marketplace for mobile banking.

Vulnerabilities in
50
mobile banking apps put half a billion customers at risk

Introduction

The speed at which technologies evolve is all but a cliché, and nowhere is that speed more apparent than in the rise of mobile. The mobile tipping point—the point at which more people used mobile devices to access the web than desktop devices—came in the first quarter of 2017, when 50.03% of global web traffic was from mobile devices[ii]. Today, mobile is the de facto standard. Simply put, if you are not already building your business on the assumption that your digital visitors are using mobile, you are missing the mark.

Mobile banking is big business

Banking has been squarely in the center of the mobile evolution. At the beginning of 2017, even before the mobile tipping point, banks were seeing steep climbs in mobile numbers. One business publication described the situation succinctly by noting that mobile banking is "all but required — millennials, for example, will leave financial institutions that don't offer the service.[iii]"

Think of this as the tip of the iceberg. Projections vary, but research shows that mobile banking adoption by new customers is in an exceptionally "rapid phase". As a result, the number of mobile banking users globally is forecast to double to 1.8 billion by 2019[iv], with Juniper Research anticipating that **over 2 billion mobile users—1 in 3 adults globally—will have used their devices for banking purposes by the end of 2021**[v].

Mobile banking big target

Unfortunately, the market's enthusiastic embrace of mobile banking, has made the applications and users attractive targets for cybercriminals. Already, **60% of mobile malware specifically targets financial information on mobile devices**[vi]. The sheer volume of mobile transactions has already passed critical mass, where the potential payoff for cybercriminals makes attacks on mobile banking applications a priority. Even in this relatively early stage of mobile adoption, smartphone users log into their mobile banking apps an average of 18 times per month[vii].

Active mobile banking customers
for selected US banks, Jan 2017[2]

JPMorgan Chase
26.5 million

Bank of America
21.6 million

WELLS FARGO
19.6 million

As the features and capabilities of mobile banking expand, mobile banking activity will continue to increase, and the corresponding surface area that cybercriminals can attack will grow too. But the reality is that mobile banking applications already have significant vulnerabilities today.

1 in 4
mobile banking applications
in the market today includes at least
one high-risk security flaw[7]

To sketch out the scope of the problem, Accenture reports that 1 in 4 mobile banking applications in the marketplace today includes at least one high-risk security flaw[viii]. In the same report, Accenture cites additional worrisome findings, e.g., 35 percent of communications sent by mobile devices are unencrypted and 43 percent of mobile device users do not use a passcode, PIN or pattern lock.

Mobile banking developers face significant hurdles

Banks are highly security conscious. In a recent survey, **61% of respondents saw improving the security of apps and websites as one of their main priorities**[ix]. How can it be then that banking, the model of a security conscious industry, would be struggling to deliver mobile application security? The simple fact is that customer demand for mobile banking is far outpacing the industry's ability to deliver ironclad security in the fast-changing mobile device ecosystem.

To put it differently, mobile application developers face significant pressure from three different and competing market forces. First, customer demand (and competitive pressure from other banks' mobile apps) is intense. Customers continue to show a huge appetite for expanding their use of mobile banking. To keep up with customers, developers often focus on features rather than security. Moreover, as deadlines loom, development shortcuts become more appealing, and developers will at times use unvetted, open source code for mobile functions.

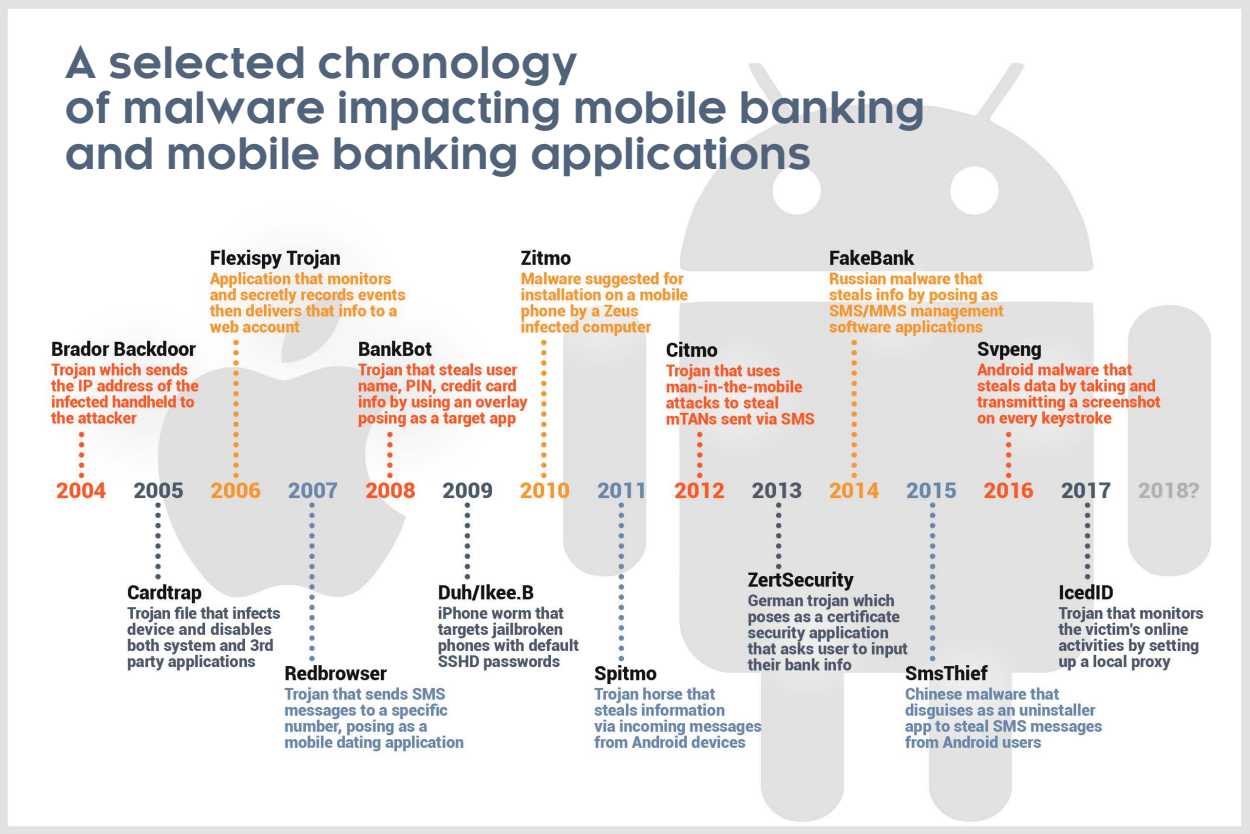
Second, mobile platforms are competing for market dominance, and do not enjoy the broad standardization that desktop technologies do. Developers therefore must either work with limited familiarity with the underlying device platforms, or become specialists in a limited, particular platform subset. This platform fragmentation[x] creates an ideal environment for security missteps.

Third, there is the reality of the way consumers use their mobile devices. Surveys consistently and clearly show that mobile banking consumers value security in principal. Indeed, one survey found that, among those who do not use mobile banking, 60% site security concerns as their main objection[xi]. Even so, consumers do not always prioritize security in practice. We noted in an earlier section, for example, that some consumers do not follow essential security practices such as the use of passwords or updating to the latest operating system. This exacerbates any vulnerabilities that developers inadvertently allow into their banking applications.

Mobile banking presents multiple attack vectors

All of the challenges that mobile banking application developers face can create vulnerabilities for cybercriminals to exploit. Although this is by no means a comprehensive list, consider the following targets for cybercriminals:

- **Credentials / Access.** Attackers may seek users' mobile banking credentials to access accounts and commit theft.
- **Personal data.** Cybercriminals focus on potentially high-value customer data such as social security numbers, dates of birth, and other sensitive information.
- **Cardholder data.** Mobile banking attacks can seek to gather card-specific data such as card numbers, expiration date information, and CVV data.
- **Network connections.** A customer's mobile banking experience can potentially be compromised even if the mobile banking application is flawless—because attackers can leverage compromised network connections.



The common goal across these attacks is ultimately to compromise and gain control of the mobile device itself. Cybercriminals aim to compromise devices—via malware, network-based attacks, phishing, etc.—so that they have long-term access and ongoing opportunities to do more damage.

Although mobile banking is only now gaining critical mass, cybercriminals have long understood the potential value of attacking mobile banking apps. Mobile banking Trojans and malware have emerged continuously over the past decade and a half.

And the frequency with which new mobile banking malware emerges, of course, is growing. In 2017, one mobile security vendor found a 40% increase in banking Trojans that can steal login credentials[xii].

Mobile banking has broad-reaching influence

Given the incredible momentum propelling mobile banking to market dominance, it is unsurprising that leading banks are also leaders in mobile banking. Best in class financial institutions, for example, have **85% of their registered end-users actively using mobile apps**[xiii]. The importance of the mobile experience pervades the bank's entire organization. For example, JD Power found that mobile banking has an impact on a bank's overall customer satisfaction, with "an immediate lift in overall satisfaction when consumers use mobile banking (+27 points on a 1,000-point scale) … [and] … an even greater impact when banks provide their mobile banking customers with a highly satisfying experience (+82 points)[xiv]".

For banks that aim to achieve or maintain a leadership position by harnessing the tremendous potential that mobile banking represents, they must overcome the barriers to

mobile banking security. This has become, in effect, a mandate. Some 65% of consumers want to have only one payment app on their phone, and most would prefer their bank to be the app provider. Banks must respond with secure mobile banking applications[xv]. Zimperium makes that possible.

Zimperium enhances mobile banking application security for banks and their customers

Zimperium provides a powerful tool with which developers can rapidly and easily enhance mobile banking security. Zimperium's zIAP™ (In-App Protection) software development kit (SDK) enables developers to quickly and painlessly embed Zimperium's leading machine learning-based detection engine, z9™, directly inside any mobile app.

With the zIAP SDK embedded, mobile banking apps can immediately determine if a user's device is compromised, any network attacks are occurring and even if malicious apps like BankBot are installed.

zIAP is completely configurable by app developers, who can select whatever remedial action should apply when a given threat is detected. When a device is under attack, zIAP informs the app and initiates those predetermined risk mitigation actions.

Here are some examples to make this real. If the embedded zIAP detects…

- A **man-in-the-middle (MITM)** attack is occurring, the app can automatically establish a VPN to create a secure tunnel.
- A device has phishing malware like **BankBot** installed, the app can trigger immediate steps to freeze access until the user resets their password on-line.
- A device has been **Jailbroken** by the user, the app can allow the session to continue, but raise the user's fraud score to account for the additional risk.
- A device has been compromised by an **external actor**, the app can display a dialog box asking the user to complete their transaction off-line.

With zIAP, developers can spend more time developing and less time worrying about security. zIAP quickly, easily and dramatically improves the security of any mobile banking session. With security safely embedded in mobile apps, banks can focus on innovations that will delight customers, increase customer loyalty and unleash the full potential of the mobile banking era.

Zimperium can help!

If your business could benefit from maximum mobile productivity and robust mobile security, Zimperium's zIAP™ in-app protection solution may be right for you.

Feel free to give us a call at 844.601.6760 or visit us at http://www.zimperium.com to learn more.

[i] 50 banking smartphone apps fail on security. SC Magazine UK. Feb 2017. https://www.scmagazineuk.com/50-banking-smartphone-apps-fail-on-security/article/639769/

[ii] Percentage of mobile device website traffic worldwide from 1st quarter 2015 to 3rd quarter 2017. Statista. Nov 2017. https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/

[iii] Business Intelligence. BusinessInsider.com. Jan 2017. http://www.businessinsider.com/heres-how-banks-can-deal-with-slowing-mobile-banking-growth-2017-1

[iv] International Journal of Commerce and Management Research. Volume 2; Issue 5; May 2016. http://www.managejournal.com/download/100/2-5-23-300.pdf

[v] Mobile banking users to reach 2 billion by 2020, representing more than 1 in 3 of global adult population. Juniper Research. Oct 2016 https://www.juniperresearch.com/press/press-releases/mobile-banking-users-to-reach-2-billion-by-2020

[vi] Mobile Banking Security. Vasco Data Security. https://www.vasco.com/solutions/banking-cyber-security/mobile-banking-security.html

[vii] Monkey Insights. Malauzai. Oct 2017. https://www.malauzai.com/monkey-insights-october-2017/

[viii] Mobile Banking Applications: Security Challenges for Banks. Accenture. 2017. https://www.accenture.com/t20170507T215501Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Consulting/Accenture-Mobile-Banking-Apps-Security-Challenges-Infographic.pdf

[ix] Mobile Banking Among 5 Top Security Risks: Survey. Credit Union Times, Mar 2017. http://www.cutimes.com/2017/03/10/mobile-banking-among-five-top-security-risks-surve?page=2&slreturn=1514328289

[x] Mobile Hardware Stats. Unity. 2017. https://hwstats.unity3d.com/mobile/device.html

2017 Payment Industry Outlook. First Data Corporate Strategy & Intelligence. April 2017. https://files.nc.gov/ncosc/documents/files/First%20Data%20Presentation%204.1917.pdf
[xii] The Top Challenges of Mobile Banking Security. SecuredTouch.com. Nov 2017. http://blog.securedtouch.com/top-challenges-of-mobile-banking-security
[xiii] Monkey Insights. Malauzai. Dec 2017. https://www.malauzai.com/monkey-insights-december-2017/
[xiv] Mobile Banking Drives Satisfaction and Growth. The Financial Brand. 2016. https://thefinancialbrand.com/58703/mobile-banking-satisfaction-growth/
[xv] Study of Mobile Banking & Payments: Mobile Wallet Report. First Annapolis. March 2017. http://www.firstannapolis.com/library/study-of-mobile-banking-payments