IBM Security
July 2016

Worried about mobile security? You should be.

Thought Leadership White Paper

Contents

Introduction

How important is mobile?

For most businesses, mobile represents a highly profitable channel, and one that is critical in attracting new customers, especially the millennial generation.

For example, in one survey of U.S. mobile banking customers, 60 percent of smartphone and tablet users ranked mobile banking as “important or extremely important” when switching banks.[1] In addition, according to Forrester Research, by 2020 there will be more than 5.4 billion active smartphones in the hands of more than 3.6 billion subscribers across the globe.[2]

Where there is growth, there is fraud.

If you’re thinking, “Mobile threats and malware are still in their infancy and the risk isn’t significant enough yet,” it’s time to think again.

The rise of advanced, PC-grade mobile malware, innovative fraud schemes, such as SIM swap fraud, and fraudsters’ increasing use of mobile devices in cross-channel attacks pose a significant threat.

How are fraudsters infiltrating mobile devices? How can you tell if a mobile customer is who they claim to be? Why don’t legacy fraud protection systems catch mobile fraud?

This white paper provides answers to mobile security questions we frequently hear from clients and outlines what capabilities you need to better detect compromised or vulnerable mobile devices and reduce fraud risk across all your channels.

Why should I be worried about mobile security?

Mobile security isn't just about mobile fraud. Fraudsters are using mobile malware and social engineering not only to initiate fraudulent transactions from a victim's mobile device, but also as part of carefully planned and well-coordinated cross-channel attacks. As a result, businesses that fail to monitor and take into account mobile risks and compromises may be missing the bigger picture, which can lead to greater overall exposure and potential loss.

At the same time, mobile fraud costs are rising. LexisNexis found that fraud costs via the mobile channel were 20 percent higher per dollar than via the online channel.[3]

In response to the increased risk, the Federal Financial Institutions Examination Council (FFIEC) in the U.S. and the European Central Bank (ECB) have issued guidelines to help organizations strengthen security for mobile financial services.[4]

5.4B

By 2020, Forrester Research estimates there will be more than 5.4 billion active smartphones.

What should I worry about most when it comes to mobile security?

The three areas organizations must be particularly mindful of in terms of mobile security include:

1. Credentials theft

Fraudsters are stealing account credentials and other personal information from customers using SMiShing (SMS phishing) and mobile malware, and by intercepting data from non-secure Wi-Fi networks.

Fraudsters can leverage these credentials in both mobile fraud and cross-channel fraud, since organizations typically use the same username, password and security questions across channels for customer convenience.

2. Interception of out-of-band authentication

Fraudsters are using social engineering campaigns to fool end users into downloading SMS forwarders that can be later used by the fraudster to authenticate fraudulent transactions through the online channel. In addition, in recent years, they've initiated SIM swap schemes that enable them to commandeer a victim's mobile account, intercept or initiate calls, texts and authorizations, such as those used for cash transfers, and even request changes to security settings to prevent victims from accessing their own accounts.

In these sophisticated attacks, a fraudster, posing as a customer, calls a mobile provider to report a lost or damaged phone. Using information gathered from the victim's social media accounts to answer security questions, the fraudster convinces the mobile provider to cancel the old SIM card, and issue and activate a new one on their behalf.

◀ Previous Next ▶

3. Account takeover via the mobile channel

Device ID limitations make direct account takeover on mobile apps or via mobile browsers possible. This is especially true for iPhone users, as one iPhone typically looks the same as any other iPhone to device ID systems because they all have the same operating system, language(s), browser, video player and defaults out-of-the-box.

As a result, fraudulent login attempts will not trigger risk indicators and a fraudulent transaction is simply a matter of time.

As you can see, mobile security doesn't just protect the mobile channel. Mobile security is vital in helping organizations prevent fraud across all channels.

Isn't mobile malware still in its infancy?

Mobile malware has grown up considerably in recent years and business technology leaders are taking notice. In fact, 64 percent of the organizations that IDG surveyed as part of its mobile enterprise study reported that mobile is a high priority, and more than half of respondents said that security is "the greatest concern" when it comes to mobile.[5]

Today, PC-grade mobile malware, such as SVPENG, GM Bot and Mazar Banking software, offer fraudsters all the sophisticated capabilities they need to steal account credentials, circumvent two-factor authentication and block phone calls after an attack. With the recent disclosure of GM Bot source code by a dissatisfied fraudster, we believe that fraudsters' use of mobile malware is only going to expand.[6]

Fraudsters can take advantage of vulnerabilities using malware and other means to infiltrate vulnerable apps, steal sensitive user information, and subsequently attempt to perform illicit transactions on behalf of a legitimate user.

Won't the built-in security controls from vendors protect mobile devices?

Despite the built-in security controls on mobile devices and across the mobile ecosystem, fraudsters have found a number of ways to trick users into divulging credentials.

1. Malware-infected mobile apps

Fraudsters are developing malware-infected mobile apps, attempting to trick users into providing credentials. Fake mobile gaming or security applications embedded with malware are routinely found in application stores and marketplaces. Once installed, the malware can intercept sensitive information, including credentials, SMS messages and other communication.

Fraudsters are even developing malware-infected mobile banking apps that look and feel like real banking applications to capture login information, personal information and banking information.

Even Apple, which rigorously controls which apps appear in its App Store, removed more than 300 malware-infected apps from its App Store in September 2015.[7]

>50%

>50% of respondents in IDG's mobile enterprise study cited security as "the greatest concern" for mobile.

2. Phishing and eavesdropping

Phishing attacks can occur via SMS messaging (called SMiShing) or in the mobile browser, just as they occur on the PC.

Mobile users have a stronger tendency than online users to click through malicious links—in part because the shortened URLs commonly used on mobile devices do not convey enough information to show that they are potentially malicious.

Mobile use also ingrains the habit of quickly clicking through links and, as a result, mobile users may connect to a phishing site more quickly than online users and may not realize their mistake as readily.

In parallel, users trying to save carrier data plans fees or travelling are often on the lookout for "free Wi-Fi," and fraudsters are taking advantage of router vulnerabilities as well as setting up "free Wi-Fi" access points using their computers to eavesdrop on traffic and steal user information.

3. OS and app vulnerabilities

Just like PCs, mobile devices can be infected simply if a user visits a hacked or malicious website via the mobile browser (known as a drive-by download in which fraudsters exploit vulnerabilities in the mobile OS or browser to infect mobile devices with malware).

In the summer of 2015, a mega vulnerability, dubbed Stagefright, was identified in the Android Media Library affecting 95 percent of users' Android devices.[8] If exploited, this vulnerability could allow an attacker to send victims a malicious MMS (Multimedia Messaging Service) message, which automatically loaded the malicious video file, downloaded a malware, and even deleted the attacking MMS message to avoid leaving any traces of the infection vector behind.

Fraudsters are also taking advantage of vulnerabilities in the operating system and apps themselves to gain access to data and other resources on the device. Users that remove manufacturer restrictions from their devices to gain additional functionality (known as jailbreaking on iOS devices or rooting on Android devices) are basically breaking the inherent security measures put forth by the manufacturer and opening themselves to even greater risks.

Won't our existing fraud protection systems flag fraudulent mobile activity?

Unfortunately, legacy fraud protection solutions weren't designed to address the challenges of mobile fraud or cross-channel fraud that involves mobile devices.

For example, legacy solutions typically can't cope with real-time device and location data or detect behavioral anomalies regarding mobile device use. As a result, they're not able to flag if two different devices are accessing the same account or if the mobile device is face down during an online transaction—both possible signs that a fraudulent activity is being initiated.

Server-side device ID systems can't distinguish between a customer's mobile device and a fraudster's mobile device as device characteristics—such as hardware type, operating system, browser and fonts—are often the same from one smartphone to another.

And separate enterprise fraud management tools for Web, phone, branch and mobile channels make it difficult to build a contextual picture of anomalous account activity, such as a user transferring funds from their online banking account after malware has been detected on their mobile phone.

20%

Fraud costs via the mobile channel are 20% higher per dollar than via the online channel.

If fraudsters can effectively “fly under the radar” when it comes to mobile devices, how can we tell if a customer is who they claim to be?

Mobile security solutions that provide financial institutions with visibility into a wide range of risk indicators and behavioral anomalies will be key in meeting not only today’s fraud challenges, but also tomorrow’s.

Risk factors to monitor include:

- Is the device jailbroken (iOS) or rooted (Android)?
- Is it infected with malware?
- Is the operating system outdated or is it missing critical patches?
- How secure is the Wi-Fi connection?
- Are there suspicious applications?
- Has the user’s SIM data changed?
- Has the user account been taken over or compromised?
- Where is the device located?

Additionally, it’s important to look for mobile solutions that can create a persistent mobile device ID, which allows organizations to distinctly identify any mobile device (iOS or Android). Through a persistent mobile device ID, fraudsters can no longer take advantage of device ID limitations to elude detection.

I’ve read about SIM swap fraud. How can I address it?

As mentioned earlier, in a SIM swap scheme, fraudsters take over a user’s mobile device by convincing the mobile provider to cancel an old SIM card and activate a new one on their behalf.

However, a SIM swap isn’t necessarily conclusive evidence of fraud. Consumers often swap the SIM card in their mobile phones when travelling abroad in order to reduce data usage and call costs. As a result, detecting and preventing SIM swap fraud requires three key capabilities:

1. The ability to create a persistent mobile device ID to distinguish each user’s mobile device

2. The ability to detect behavioral anomalies, such as if the SIM card is swapped

3. The ability to correlate real-time information with additional aggregated risk factors/information, such as recent malware infections or phishing attempts, on both the mobile and online banking channel

Mobile users have a stronger tendency than online users to click through malicious links.

Conclusion: Balancing mobile security and the user experience

The growing sophistication of mobile malware and use of the mobile channel in cross-channel attacks is increasing the risk for both businesses and their customers, and impacting user confidence.

To help prevent fraud, businesses must now be able to detect compromised or vulnerable mobile devices and incorporate the data into their fraud and identity detection solutions.

However, one of the biggest concerns organizations have when it comes to mobile security is the impact it will have on the user experience, as mobility is often synonymous with convenience.

IBM® Security Trusteer® mobile solutions are designed to help protect mobile activity in a non-intrusive manner, without excessive resource consumption, and without negatively impacting the user experience.

When integrated with your mobile app, the IBM Security Trusteer Mobile SDK collects a variety of parameters (indicators)—from geolocation and SIM data, to hashed user IDs, to malware infections and Wi-Fi security, to behavioral anomalies, such as device orientation and changes in time of access.

It can also create a persistent device ID to help organizations confirm users are who they say they are and help combat SIM swap fraud attempts.

Your mobile app can make use of this data to restrict functionality based on the device's risk level. The data can also be shared with fraud detection solutions to help in better analyzing cross-channel risk.

If you're using the IBM MobileFirst™ Platform to develop your mobile apps, you can incorporate the functionality of the Trusteer Mobile SDK by simply checking a box. IBM MobileFirst Platform will automatically add the SDK to the app development project using prebuilt, pretested and optimized integration.

Finally, IBM Security mobile security solutions are highly adaptable to address new threats and can incorporate new countermeasures provided by IBM without any intervention by security staff and with minimal impact to your end users.

For more information

To learn more about mobile security and IBM Security Trusteer mobile security solutions, please contact your IBM representative or IBM Business Partner, or visit the following websites:
ibm.com/software/products/en/trusteer-mobile-sdk and
ibm.com/software/products/en/trusteer-mobile-browser

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2016

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

♲ Please Recycle

[1] As Consumer Banking Behavior Continues to Evolve, Mobile is Now Mainstream, Says AlixPartners Study," AlixPartners (press release), March 2014. Retrieved from: http://www.alixpartners.com/en/MediaCenter/PressReleases/tabid/821/articleType/ArticleView/articleId/1060/As-Consumer-Banking-Behavior-Continues-to-Evolve-Mobile-Is-Now-Mainstream-Says-AlixPartners-Study.aspx#sthash.tmpoZlhR.gvzlpfxj.dpbs

[2] "Forrester Research World Mobile And Smartphone Adoption Forecast, 2015 To 2020 (Global)," Forrester Research (report), September 2015. Retrieved from: https://www.forrester.com/report/Forrester+Research+World+Mobile+And+Smartphone+Adoption+Forecast+2015+To+2020+Global/-/E-RES127942

[3] "LexisNexis True Cost of Fraud Study," LexisNexis (report), August 2014. Retrieved from: http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf

[4] For more information on FFIEC and ECB guidelines related to mobile financial services visit the FFIEC IT Examination Handbook, Appendix E: Mobile Financial Services at http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/appendix-e-mobile-financial-services.aspx and ECB Recommendations for the Security of Mobile Payments at https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf

[5] "Building the Mobile Enterprise Survey 2015," IDG (report), September 2015. Retrieved from: http://www.idgenterprise.com/resource/research/2015-idg-enterprise-building-the-mobile-enterprise-survey/

[6] Limor Kessem, "Android Malware About to Get Worse: GM Bot Source Code Leaked," IBM Security Intelligence (blog), February 2015. Retrieved from: https://securityintelligence.com/android-malware-about-to-get-worse-gm-bot-source-code-leaked/

[7] Joseph Cox, "Apple Removes 300 Infected Apps from AppStore," Wired, September 21, 2015. Retrieved from: https://www.wired.com/2015/09/apple-removes-300-infected-apps-app-store/

[8] Matt Burgess, "Millions of Android devices vulnerable to new Stagefright exploit," Wired, March 16, 2016. Retrieved from:http://www.wired.co.uk/news/archive/2016-03/16/stagefright-android-real-world-hack