Mobile Device Attacks

By: Vicki Holzknecht

East Carolina University

Contact: holzknechtvi07@students.ecu.edu

Abstract

comScore reported for the month of September, the top two smartphone market share holders in the United States are Android, 52.1% and Apple, 41.7% (Lella, 2014). Many users go about their day checking /sending email, text messaging, sharing photos on social media sites without ever thinking about the security angle of their daily activities performed on mobile device. In May 2014, ConsumerReports discovered thirty-four percent of the smartphone users did not enable any security features on device (Tapellini, 2014). Last year alone, mobile malware attacks rapidly grew to one hundred and sixty-seven percent (Vinton, 2014); approximately 100,000 malicious programs for mobile devices were detected (Hilburn, 2014). This paper is broken down into the following areas: Mobile Attacks and Don't Be A Victim.

Keywords: Android, Apple, Malware, Mobile, Attacks

I. Mobile Attacks

Ninety-seven percent of mobile malware attacks are targeted towards Android mobile devices (Kelly, 2014). Recently, Apple devices began to see their share of mobile attacks. Mobile devices are becoming popular targets for theft because of the portability, the amount of personal and the *possibility* of corporate data being stored on the device (Ruggiero, Foote, 2011). Globally, there are 4 billion mobile devices in use (10 Quick Tips to Mobile Security, 2012), as they become increasingly popular instruments for day-to-day life (Miller, 2011) hackers will try to take advantage of those not so security-savvy mobile users. Five threats are on the horizon aimed towards mobile devices see Table 1 below:

Threats
Mobile Phishing and Ransomware
Infiltrate nearby devices
Cross-platform banking Attacks
Cryptocurrency Mining Attacks
Mobile Device Owners

Table 1 New Threats
Resource: (Collett, 2014)

The first known malware that was targeted against Android was aimed towards Tibetan activist (Olson, 2013). The attack depended on a form social engineering called spear-phishing. The hackers were able to gain access into a high-profile activist, sending a mass email out to all those in the contact list. The email was sent with an attachment a .apk file, once the recipient downloaded the attachment while on Android phone, an application was installed called "Conference" (Olson, 2013). Once the mobile user tapped on the "Conference" app a text of information popped up about the conference:

"*WUC's Conference in Geneva, On behalf of all at the Word Uyghur Congress (WUC) the Unrepresented Nation and Peoples Organization (UNPO)…."*(Olson, 2013).

Notice, the misspelling of World; while the Android user was reading the text popup, the application was actually reporting back to a command-control server (C&C) waiting on the signal to collect private data such as contacts stored both on phone and SIM card, call logs, SMS messages, Geo-location, along with phone number, model and operating system version (Olson, 2013). A text message was then sent to the user attached with a certain protocol allowing the application to report back any of the information listed above back to the C&C.

In July, mobile security researchers from FireEye notified Apple about a vulnerability that affected iOS versions 7 and 8 identified as Masque Attack Technique (Xue, Wei, Zhang, 2014). On November 13, 2014, The United States Computer Emergency Ready Team released an alert for the masque attacked tagged TA14-317A (Apple iOS "Masque Attack" Technique, 2014). Approximately ninety-five percent of the Apple devices that are in use were vulnerable to the bug (Statt, 2014) so you can see the severity of the issue. The weakness lies within the bundle identifier allowing a malicious application to be seen as a legitimate application; iOS does not compare certificates that match for applications having the same bundle identifier. Attackers crafted an application that looks graphically identical to an application already on the users Apple device to carry out the attack.

FireEye mobile security researchers used the Gmail app as an example; they manipulated the bundle identifier "com.google.Gmail" and titled it "New Flappy Bird" which is an arbitrary title it can be set to whatever the attacker wants it to be (Xue, Wei, Zhang, 2014). Next, the researchers signed the application using an enterprise certificate, now the trick is trying to get the user to install it from a third-party website. Typically users do not pay attention to what they

install, most press “install” and “update” so much they do not read what they are installing or updating. After, visiting the third-party website, the mobile device user is prompt with an install message; if click install the original Gmail application will be replaced with the malicious application looking identical to the original Gmail application. The user can see the application being replaced, but for most Apple users, they would assume the Gmail application is being updated. The cached emails from the app are uploaded to a remote server in clear text in a sqlite3 database (Xue, Wei, Zhang, 2014). This attack is performed entirely over the wireless network and does not require the devices to be connected to a USB attaching it to a Mac. The impact of this attack reaches so many levels, the attacker has now gained root privileges to the device, can monitor the device and steal credentials (Apple iOS "Masque Attack" Technique, 2014)

Some of us fear that the government is constantly monitoring our every movement whether it’s through the cell towers, or on smartphone cameras invading the privacy of citizens. The Oxford Dictionary defines privacy as “*The state or condition of being free from being observed or disturbed by other people”* (Oxford Online Dictionary). Using a smartphone camera to spy can be taken as a positive or negative approach. The positive approach is when device has been lost or stolen and the camera is remotely enabled to see who has taken the phone or who has tried to gain access to the phone by guessing the pin or patterns that secures the phone. The negative approach would be an application that was downloaded from Google Play gaining unauthorized access to device and exploiting the camera to send back information.

In March of 2014 there were one-hundred spy camera’s available in the Google Play allowing for the cameras to record video and take pictures of others without permission (Wu, Du, Fu, 2014). Why use camera-based attacks? Remember, mobile devices are portable and are

used within companies containing sensitive / private data. The basic camera attack is presented in Figure 1 below:

Figure 1 Basic Camera Attack
Resource: (Wu, Du, Fu, 2014)

Step 1: The malware should be inconspicuous and not send red flags to the user, when device battery begins to drain or becomes bearably slow natural instinct is to check if an application on the device is causing any issues. An attacker will want to make sure that there are sufficient resources available before carrying out a camera attack.

Step 2: Through the AudioManager STREAM_SYSTEM flag on an Android the attack can adjust the sound and vibration levels by turning on the flag FLAG_REMOVE_SOUND_AND_VIBRATE (Wu, Du, Fu, 2014).

Step 3: Adjusting two attributes for WindowManager.LayoutParams can cause the preview window to be on top of all the other apps TYPE_SYSTEM_OVERLAY and FLAG_NOT_FOCUSABLE creating preview for the malware that is not detected by the human eye (Wu, Du, Fu, 2014).

Step 4: The camera application malware can use either the front camera or the camera on the back to capture the data that the attacker is after. The data is stored as a disguise, so the user does not recognize the filenames.

Step 5: Once the attack is complete, the sound and vibration is restored.

Step 6: After the data is captured then it is transmitted through a multimedia messaging service causing unnecessary chargers, so the attacker may wait until the device is on a wireless network (Wu, Du, Fu, 2014).

There are two types of camera attacks Remote-Controlled Real-Time Monitoring and Video-Based Passcode Inference Attacks. The easiest way to accomplish a remote control attack is to go through a socket. Once the application is on the device it can send a ready message to an IP address and port number to the server of the attacker; from here the attacker can control the application with "orders" stop, launch etc. (Wu, Du, Fu, 2014). The application if programmed can run while the screen is turned off and periodically check to see what the screen status is through theses two receivers ACTION_SCREEN_ON and ACTION_SCREEN_OFF (Wu, Du, Fu, 2014).

Using the camera to observe the eye movements can allow an attacker to determine the passcode known as Video Based Passcode Inference. When typing on a mobile device, users tend to hold devices closer to them giving the attacker a clear advantage of the eyes (Wu, Du, Fu, 2014). There are two types of Video Based Passcode Inference Attacks: Application Oriented and Screen Unlocking Attack. Application Oriented will only work when the user is trying to authenticate, within an application (Gmail, Facebook, Twitter) the camera uses the front camera time enough to capture the users eye movements recording the entire authentication process (Wu, Du, Fu, 2014). The Screen Unlocked occurs when the user is entering a screen locking code

whether it is a pin or a passcode and stops once the device goes black. Even though the spy camera is in action, it is still not viewable to the user trying to gain access to their phone. The camera preview is right beneath the unlocking interface that was set TYPE_SYSTEM_OVERLAY and FLAG_NOT_FOCUSABLE (Wu, Du, Fu, 2014). To test the stealth of the attacks the researchers installed AVG antivirus and Norton Mobile Security on the Android's that was used as demo's and during the entire recording / capturing process neither raised a flag that something suspicious was lurking in the background (Wu, Du, Fu, 2014).

Apple has been criticized for having the tightest security built into OS X and the iOS operating systems preventing users from customizing their devices as the open source software allows for Android device users. Advanced rebel Apple users in previous iOS versions jailbroke their devices. Jailbreak is defined, as *breaking all of the protections that iOS has to offer, ie: disabling code signing of apps*, *allowing applications to run outside of the sandbox* (Miller, 2011). Sandboxing allows an app to run in its own environment without reading or leaking data into another application process. A new wave of Trojans named WireLurker discovered by the Palo Alto Networks affects Mac OS X and iOS devices jailbroken or not (Xiao, 2014). Maiyadi a third-party app store in China was used to infect four hundred and sixty-seven applications that were downloaded almost 360,000 times impacting over 100,000 users (Xiao, 2014).

What makes WireLurker special? It is the second known malware family attacking iOS devices through USB, the first of its kind to automate a range of malevolent applications via binary file replacement, the first malware that as similar infection patterns as a computer virus, and the first of a wild malware to install third-party applications that are non-jailbroken (Xiao, 2014). Once a Mac is infected with the Trojan, the machine is scanning for any devices plugged in. After an iPhone is detected the Trojan from the Mac propagates to the iOS device dispersing

the infection to another device. WireLurker reports back to a C&C server thieving all sorts of information back to the attacker when not waiting on an update request from the server (Xiao, 2014). Figure 2 is a diagram of the stages for WireLurker, beginning with Trojanizing the Mac Application reading it to upload to a third-party store and once the Trojan is finally on the iOS device what happens next.

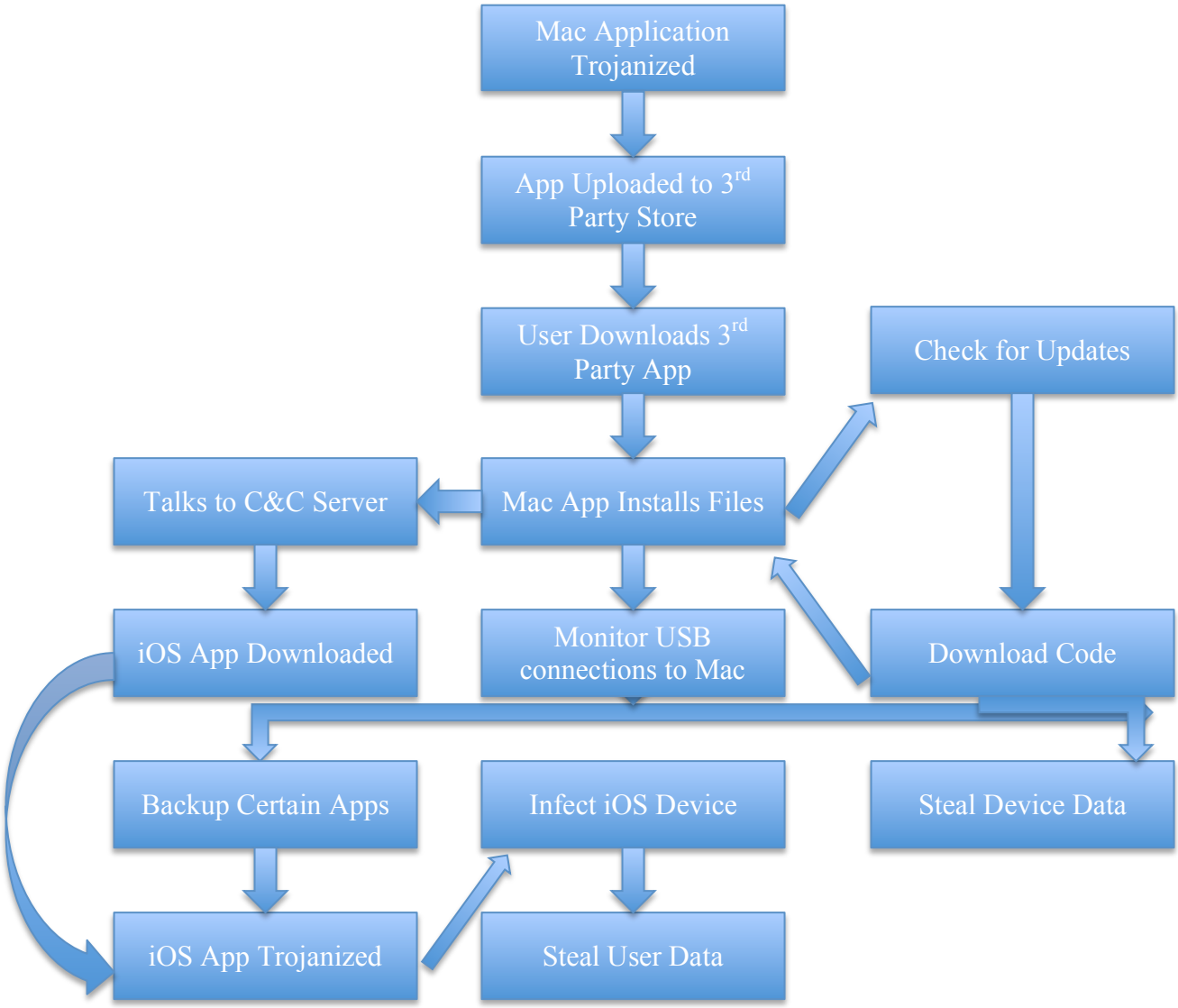

Figure 2 WireLurker Workflow Resource (Xiao, 2014)

II. Don't Be A Victim

There's an estimate of two hundred threats every minute according to a McAfee Labs from a Summer 2014 report, 1 million is said to be ransomware and 5.7 million to be malign signed binaries (Vinton, 2014). It's alarming to know as rampant malware is today, thirty-four percent of mobile device owners have not taken proactive approaches and enabled extra security measures (Tapellini, 2014) provided by the mobile device's operating system. Protecting data on the device is crucial; misplacing or losing a device is just as bad as company breach. In 2011 Lookout who is a mobile security company based in San Francisco reported 9 million smartphones had been lost (Yu, 2012). Phones that were lost and stolen in the year of 2013, never recovered is estimated to be about 4.5 million (Tapellini, 2014**).** Taking precautionary advances in safeguarding the mobile device is a couple steps in the right direction.

For both Android and iOS platforms there are simple pin numbers that can be used generally four numbers, to be a little bit more complex a pin code at least to seventeen alphanumeric characters long can be set. On Android you can set lock patterns in the form of a 3 x 3 grid of dots, there is even a setting for a facial pattern recognition to unlock the device and Apple offers fingerprint scanners arriving on iPhone 5s models for the first time and on some newer Android devices HTC and Samsung offer fingerprint scanning capabilities. Also, each platform gives the mobile device user the capability of erasing the phone after multiple failed attempts of getting into the device, some will even allow for remote wipe to occur if device is lost of stolen. When a user is shopping for a mobile device the security features of that device should be taken in consideration (Ruggiero, Foote, 2011) it's always good to have a fail-safe option in place. Apple by default encrypts iOS 8 to keep out prying eyes such as law enforcement and FBI (Timm, 2014), Google has recently done the same thing before you had to

manually go into your device settings and encrypt it. Table 2 is a summary of security measures found on mobile devices and the percentage of people who actually use them.

Security Measure	Percentage
4 Digit Pin	36%
Backup Data	29%
Location Software	22%
Antivirus Install	14%
Unlock Pattern/ longer pin	11%
Erase Software	8%
Encryption Features	7%

Table 2 Security Measure Percentage
Resource: (Tapellini, 2014)

To prevent masque attacks the solution is to not download from third-party developers, download applications from the genuine Apple App Store where the developers have been approved by Apple and signed with Apple's certificate (stamp of approval). Next is to read the install app dialog and not download when an installation mention is presented when on a website (Apple iOS "Masque Attack" Technique, 2014). Last but not least when an application is said to be from an "untrusted developer" quickly cancel out of the alert and uninstall the application (Xue,Wei, Zhang, 2014). iOS 7 operating system users can check their setting for provisional profiles to see if an application has performed a masque attack by access their Settings → General → Profiles in the example previously mentioned says "New Flappy Birds" or "Provisional Profile" (Xue,Wei, Zhang, 2014) there's a good chance the device has been used for a masque attack.

Open Wi-Fi accessibility is an open target for cyber criminals to execute man in the middle attacks, sniffing out the network, intercepting data when a mobile user is making a bank transaction over an open Wi-Fi network. Best advice is to wait until the device is on a securer connection and some open Wi-Fi networks are not as legitimate as they may seem and attacker could have created a fake Wi-Fi hotspot making it easier to capture data (Ruggiero, Foote, 2011). It is best to always install applications from trusted sources (10 Quick Tips to Mobile Security, 2012), tip number one when interested in an application to install, read the reviews of other users who installed the application and in Google Play take notice of the amount of downloads of the application (Miller, 2011).

To avoid phishing scams beware of suspicious emails or text messages that are received (Ruggiero, Foote, 2011); it never hurts to call the sender when an email or text message is in question. Just like PCs and laptops mobile devices can backup to a computer or a cloud base services, for Android's there are applications out there that can backup data Google can back up photo's to your Google account and Samsung devices can do the same, for Apple users there is always iCloud and iTunes to backup any data. One issue that many users face is not having the operating system patched with the latest updates, eventually the updates are pushed out to device if neglected for so long, but it is in good practice to periodically check for operating system updates because updates can address major security flaws making the device in its current state vulnerable.

Bluetooth is the rage; it's a low range connection permitting devices in discoverable mode to connect to newer modeled cars, headphones, MP3 players, keyboards, mice, etc. If not using any Bluetooth simply turn it off, Bluetooth capable devices can be placed in non-discoverable mode so the device is not visible to unauthenticated devices (Ruggiero, Foote,

2011). Built-in security is there for a reason; there is not a sound explanation as to why some users hack or jailbreak a device. Removing default security switches weakens the device creating security holes (10 Quick Tips to Mobile Security, 2012) and making it more susceptible to attacks.

Social media is a huge sector; seventy-four percent of adults in January of this year use social networking sites (Social Networking Factsheet, 2014) Facebook, Twitter, Instagram, LinkedIn etc. Privacy has always been a concern in social media applications, exactly what kind of data is being reported back to Facebook or Twitter when you make a post or send a tweet. The more personal information that is out there on the media sites the better off an attacker is if compromised an account (Ruggiero, Foote, 2011). Thirty-two percent of the mobile device users do not believe anti-virus protection needs to be installed (10 Quick Tips to Mobile Security, 2012). The device may have the latest and greatest security but it never hurts to have an antivirus client installed that can frequently check for incoming malware being installed, run a scan on current installed applications, block malicious websites, etc. One last note if selling a used device or recycling it, always erase the contents of the device to protect private data from getting into the wrong hands.

Conclusion

Mobile devices have coalesced into our lives to where society would be lost without them. As society moves into a new era of mobility cyber criminals will prey upon the weakest device users who lack security authentication measures, jailbreak device and store private information without any device data encryption in action. Cyber criminals today use several vectors to pilfer data from devices. The camera on a mobile device can be used to monitor authentication information as a user is typing with in an app, to record corporate meetings

containing trade secret information that would be used as an advantage for corporate rivalry. Then phishing scams, via email, SMS (text messaging); that lure the user into downloading applications so the malicious application can report information, back to a C&C server. Another vector is the use of third party application stores to distribute trojanized applications to infect not one operating system but another through USB connections. Attacks on mobile devices are only going to get worse not better. Device users need to be taught how to safeguard their device from unwanted eyes. Mobile system developers need to keep being proactive in securing their operating system from present day and future attacks. Future risks targeted towards mobile devices are: attacks on decommissioned devices, network spoofing, diallerware attacks and network congestion to name a few (La Polla, Martinelli, Sgandurra, 2013).

References

Apple iOS "masque attack" technique. (2014). Retrieved from https://www.us-cert.gov/ncas/alerts/TA14-317A

Collett, S. (2014). Five new threats to your mobile device security. Retrieved from http://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-device-security.html

Hilburn, M. (2014). Cyber thieves increasingly attack mobile devices. Retrieved from http://www.voanews.com/content/cyber-thieves-increasing-attacks-on-mobile-devices/1860943.html

Kelly, G. (2014). Report: 97% of mobile malware is on android. Retrieved from http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/

*La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. *Communications Surveys & Tutorials, IEEE, 15*(1), 446-471. doi:10.1109/SURV.2012.013012.00028

Lella, A. (2014). comScore reports septermber 2014 U.S. smartphone subscriber market share. Retrieved from http://www.comscore.com/Insights/Market-Rankings/comScore-Reports-September-2014-US-Smartphone-Subscriber-Market-Share

*Longfei Wu, Xiaojiang Du, & Xinwen Fu. (2014). Security threats to mobile multimedia applications: Camera-based attacks on mobile phones. *Communications Magazine, IEEE, 52*(3), 80-87. doi:10.1109/MCOM.2014.6766089

McAfee. (2012). 10 quick tips to mobile security. Retrieved from http://www.intel.com/content/dam/www/public/us/en/documents/guides/10-quick-tips-to-mobile-security-guide.pdf

*Miller, C. (2011). Mobile attacks and defense. *Security & Privacy, IEEE, 9*(4), 68-70. doi:10.1109/MSP.2011.85

Olson, P. (2013). First-known targeted malware attack on android phones steals contacts and text messages. Retrieved from http://www.forbes.com/sites/parmyolson/2013/03/26/first-known-targeted-malware-attack-on-android-phones-steals-contacts-and-text-messages/

Oxford Online Dictionary.Privacy. Retrieved from http://www.oxforddictionaries.com/us/definition/american_english/privacy?searchDictCode=all

Ruggiero, P., & Foote, J. (2011). Cyber threats to mobile phones. Retrieved from https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

Social networking fact sheet. (2014). Retrieved from http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/

Statt, N. (2014). Apple iOS bug lets fake apps sneak onto iPhones, iPads. Retrieved from http://www.cnet.com/news/apple-ios-bug-lets-fake-apps-sneak-onto-iphones-ipads/

Tapellini, D. (2014). Smart phone thefts rose to 3.1 million last year. Retrieved from http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm

Timm, T. (2014). Your iPhone is now encrypted: Retrieved from http://www.theguardian.com/commentisfree/2014/sep/30/iphone-6-encrypted-phone-data-default

Vinton, K. (2014). Mobile malware is on the tise, McAfee report reveals. Retrieved from http://www.forbes.com/sites/katevinton/2014/06/24/mobile-malware-is-on-the-rise-mcafee-report-reveals/

Xiao, C. (2014). WireLurker: A new era in iOS and OS X malware. Retrieved from https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

Xue, H., Wei, T. & Zhang, Y. (2014). Masque attack: All your iOS apps belong to us. Retrieved from https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html

Yu, R. (2012). Lost cell phones added up in 2011. Retrieved from http://usatoday30.usatoday.com/tech/news/story/2012-03-22/lost-phones/53707448/1

***References journals**