

Securing the Mobile Device...and its User

by Angela Orebaugh

Have you ever asked someone for the time and they pulled out their phone to get the answer? Today, smart phones have become as common as wristwatches in the 1900s. In fact, most of today's youth do not wear this old-fashioned form of mobile technology; they use their phones to tell time. Today's mobile technology includes handheld computing devices such as smart phones, personal digital assistants, tablet computers, electronic book readers, portable media players, and handheld gaming consoles. Mobile devices provide convenient access to information, entertainment, and communication by combining many functions into a single wireless device, including voice and video calling, texting, Web access, gaming, music, and movies. Some also include advanced features such as cameras, GPS, and the ability to pay for goods at point-of-sale terminals.

With such rich features and capabilities comes vulnerability. Imagine a scenario where an attacker has access to all of the data stored on your device, can follow your exact location and travel on a map, listen in on your cell phone conversations, and listen to conversations you have near your cell phone. This scenario is real and is happening to users across the world. Mobile malware and legitimate applications, such as FlexiSPY, provide an attacker with robust capabilities to

access and monitor a mobile device without the victim's knowledge. [1] In addition to personal privacy violation, these types of applications also pose risks to business, politics, and even national security, depending on who is listening.

Challenges and Issues for Organizations

Due to the transformation in how users access and consume data with mobile devices, many organizations are now confronted with supporting the use and security of a number of mobile devices in the organization. Some organizations are even subscribing to the Bring Your Own Device operating model, which allows users to supply their own laptops and mobile devices for performing work and accessing company resources. Both organizations and users are faced with the fact that mobile devices often lack the security features available to personal computers. In some cases, this is due to slow market maturity for these products, and in other cases, the mobile device processing power does not support the overhead of traditional security tools such as firewalls and intrusion detection systems. Users also do not view their mobile devices as computers and often take more risks, such as opening attachments and downloading software. Mobile devices are susceptible to attacks similar to those targeted at personal computers, and criminals are taking advantage of



What's Stored on Your Mobile Device?

- ▶ Photos
- ▶ E-mails (including deleted ones)
- ▶ Text messages (including deleted ones)
- ▶ Calls placed and received
- ▶ History of locations with geographic coordinates and timestamps
- ▶ Google maps and routes
- ▶ Web browsing history and browser cache
- ▶ Screenshots of applications in use
- ▶ User names
- ▶ Stored passwords
- ▶ Keystrokes. [2]

vulnerabilities in mobile device operating systems and their users. The Norton Cybercrime Report states mobile vulnerabilities jumped 42% from 2009 to 2010 and 10% of adults have experienced mobile device-related cybercrime. [3]

2011 became the year of mobile malware as mobile devices became a primary target for scammers and criminals. Mobile malware is increasing in volume and complexity with features such as botnet functionality and rootkits. Mobile devices are attractive to criminals because they hold a wealth of personal information including access to e-mail, social media, and bank accounts. Mobile malware attempts to steal personal data stored on the mobile device, access accounts using information stored on the device, and/or to use the features of the device for other cybercrime purposes.



Examples of Malware

- ▶ **Zitmo (Zeuz in the Mobile)**—Intercepts SMS messages to capture bank authentication codes;
- ▶ **DroidDream Botnet**—Steals phone identifier numbers;
- ▶ **Plankton**—Collects device ID and list of permissions and sends to a remote server;
- ▶ **Androidos_Nickispy.c**—Disguises itself as a Google+ app to capture instant messages, GPS location, call logs, and other sensitive data. Can automatically answer and record phone calls. Sends stolen data to remote site;
- ▶ **Pjapps/SteamyScr**—Turns the mobile device into a bot that an attacker can control;
- ▶ **Bgyoulu and GGTracker**—Sends messages to premium SMS services from the victim phone; and
- ▶ **SpitMo (Spyeye for Mobile)**—All incoming SMS messages are intercepted and transferred to the attacker's command-and-control server.

Main Attack Vectors

Mobile malware uses a number of different attack vectors to infect the mobile device. Some of the more common attack vectors include—

1. **Creating malware that looks like a legitimate application**—The most common attack on mobile devices is the result of repackaging. Cyber criminals add malicious code to a legitimate application and republish it to an application market or download site. [4] A variation of this is the upgrade attack, where an attacker first

publishes a clean application, then later adds malicious code to an update of the application.

2. **Creating malware that executes from ads**—Some pop-up ads that are displayed on mobile applications will redirect the user to a site that downloads mobile malware.
3. **Creating malware that claims to be for security**—A traditional method of malware infection that tricks the user into installing a counterfeit version of security software is also making its way into mobile devices.
4. **Tricking the user into installing malware from an installation request originating from the victim's PC**—Some traditional malware that target PCs are now incorporating mobile components as well. For example, the Zeus Trojan that steals banking credentials on an infected PC has incorporated the Zitmo Trojan to capture SMS messages with banking authentication credentials sent to the infected mobile phone.

Most of these attack vectors are successful because users give applications permissions with no scrutiny.

Application Distribution

The method of mobile application distribution plays a significant role in the proliferation of mobile malware. Google and Apple have different philosophies and operational processes for vetting and distributing applications for their Android and iOS devices, respectively. Google allows flexibility for developers to create and distribute applications through a variety of channels including the Android Market and other third-party sites; however, Google does not vet the applications to ensure they are free of malware. Although this process allows increased flexibility, it comes with increased risk, as seen throughout 2011 with the increase of mobile malware for Androids. Thousands of free applications were found to have malware hidden in them. Once malicious applications are reported, Google removes access to them on the Android Market, but these applications still exist on third-party sites.

Malware is growing quickly with Androids, including some that steal personal information, send SMS messages to premium services, and record phone calls to upload to a remote server. [5] One example of Android malware is the DroidDream botnet that activates at night and steals phone International Mobile Equipment Identity (IMEI) numbers. Botnets are often sold in underground forums for spammers

and other cybercriminals.

Cybercriminals can use the phone's IMEI number to make a clone of the phone and place calls, send text messages, and even order products, all of which will be charged to the victim's bill. After Google became aware of the malware, it flipped the "kill switch" that enables it to access Android phones without user permissions and delete the malicious software. About 260,000 Android users were infected with DroidDream. [6] Although it has been removed from the Android Market, DroidDream and its variants can still be found on third-party sites. [7]

Although some iOS malware exists, Apple has experienced less of an impact of malware due to its tightly controlled application distribution policy. Apple requires application developers to register and pay to obtain a signing certificate, making it easy to identify and prosecute authors of malware. Apple also tests every application that is submitted for publication to the App store for malware and policy violations. Apple also uses a code signing model that prevents tampering with published applications. Most iOS malware exists for devices that have been jailbroken, which allows the devices to run third-party software not vetted by Apple. Jailbreaking removes security settings and opens the device to malware and possible compromise.

Security Starts with the User

The main objectives for securing mobile devices are configuring security features and creating user awareness. The following recommendations include

Mobile Device Attack Scenario

A security researcher at the 2010 Defcon conference launched a man-in-the-middle attack on cell phones, allowing him to eavesdrop on conversations. He built a fake cell phone tower for \$1,500 and used it to stealthily intercept phone calls and pass them on to a real tower. This research only works on GSM-based networks but serves as a proof-of-concept of the ease of interception of cell phone communications. [9]

both security settings and user awareness—

- ▶ **Use strong passcodes**—Whether it is a swipe pattern, numeric PIN, or password to lock your device, make sure to use something that is difficult to guess. Avoid the most commonly used passcodes. [8] Enable the fingerprint lock option if supported by your device. Remember to also use strong passwords for applications that contain sensitive information. Some devices also have the ability to erase all data on the phone if the passcode is entered incorrectly after a certain number of attempts. Enable this feature and configure it to a reasonable number, such as 10 failed attempts.
- ▶ **Configure the screen lock**—Configure the screen lock to enable after a short period of inactivity, such as 1 to 5 minutes.
- ▶ **Disable Wi-Fi autoconnect**—Access the Internet using the service provider's network (e.g., 3G) or a secure wi-fi network. Unsecured wireless networks may expose sensitive data to attackers on that network. Do not use a public Wi-Fi, even if secure, for financial transactions or other personal transactions.
- ▶ **Scrutinize links**—Do not click suspicious or unknown links regardless of the sender.
- ▶ **Scrutinize text messages**—Do not respond to text messages from unknown sources or strange requests from known sources.
- ▶ **Download applications from trusted sources**—Only download applications from trusted sources and distribution channels.
- ▶ **Understand permissions**—Make sure you understand the permissions an application is requesting before accepting. If the application is asking for permission to access something that seems unusual for its purpose, such as access to your location or contacts,

There are still many organizations that are not yet addressing the proliferation of mobile device usage.

ensure the application is legitimate and free of malware before granting permissions.

- ▶ **Install theft location applications**—There are applications for some devices that allow the device to be located and certain features managed remotely. For example, Apple's Find My iPhone and Find My iPad applications are used to locate a lost device. They include features to remotely set or enable the passcode lock and remotely wipe the device.
- ▶ **Do not jailbreak the device**—Jailbreaking a device removes limitations and security parameters and exposes the device to increased security threats.
- ▶ **Make sure the device OS is up to date**—Promptly apply updates as they are released for your device.
- ▶ **Think about the type of data stored on your device**—Whenever possible, do not store sensitive data on mobile devices. If sensitive data is stored on your device, make sure the data is encrypted.
- ▶ **Use security software and keep it up to date**—A number of security vendors have developed applications to add third-party mobile device security, including Trend Micro, ESET, McAfee, Symantec, and Webroot. Install a security application appropriate for your device and usage.

Enterprise Mobile Device Security

Mobile devices are changing the way organizations manage security. Many information technology departments

are now treating users as shared owners of the end-user technology, giving them flexibility to use their own personal devices, but also holding them responsible for proper device usage and security; however, there are still many organizations that are not yet addressing the proliferation of mobile device usage. “More than one out of five organizations do not have a security policy governing the use of personal mobile devices at work, even though two out of three said they allow personal mobile devices on the corporate network,” according to a survey by Courion. [10] The survey also stated that “one in 10 organizations has had a data breach following the loss of a personal mobile device.” Organizations must implement a mobile device policy to define, assess, and enforce access and also to outline incident response procedures. Redspin provides an example Mobile Device Security Policy available for download at http://www.redspin.com/docs/WP_Redspin_Mobile_Device_Security_Policy.pdf.

Some additional recommendations for mobile device security for organizations include—

- ▶ Centralize mobile device administration to enforce and report on security policies;
- ▶ Strongly enforce security policies, such as mandating the use of strong passcodes;
- ▶ Enforce mobile device security applications to protect against malicious applications, spyware, and other attacks;
- ▶ Use SSL VPN clients to require authentication and protect data in transit;
- ▶ Centralize location and remote lock, wipe, backup, and restore capabilities for lost and stolen devices;
- ▶ Use software to monitor device activity for data leakage and inappropriate use; and

- ▶ Incorporate planned internal phishing exercises to measure security awareness and educate users who are falling for these attacks.

Mobile Device Pioneers in Government

A number of government agencies are adopting enterprise strategies for mobile devices. The state of West Virginia uses software from Good Technology that enables users to securely access business-related information from any device, including personal mobile devices. State personnel can also request iPhones, iPads, and Android-based smart phones for business and personal use. The Good Technology software enables secure calls and messaging by segregating business and personal information in “containers” with individual encryption and policy controls. [11] The United States Department of Agriculture (USDA) is testing the ability to secure personal mobile devices using technologies such as a virtual desktop infrastructure that mimics a secure PC environment. The USDA maintains an inventory of several thousand government-issued devices such as iPads, iPhones, and other smart phones. They are also creating mobile device management standards and policies for use by all government operations. [12] Other government agencies supporting mobile devices include the State Department, the General Services Administration, the Department of Interior, and the Department of Defense.

Many health-care providers are also embracing mobile devices. Just 1 year after the iPad was released, 30% of the U.S. physicians began using it and an additional 28% plan to purchase an iPad within the next 6 months. [13] Doctors at the Veterans Affairs are also using smart phones and tablets to access patient records. [14]

The rapid adoption of mobile devices has created a rich opportunity for cybercriminals.

The Mobile Future

The rapid adoption of mobile devices has created a rich opportunity for cybercriminals. As criminals create malware and other attacks on mobile devices, it is likely that they will become the primary target for cybercrime and a key element of financial crime in the future. With an increasing number of users bringing mobile devices into the enterprise, we will see more cross-platform attacks that target enterprise assets. Mobile devices will become the stepping-stones to protected information in the cloud and other data stores. As mobile device security evolves, it is important to educate users, enable available security settings, and continue to stay on the forefront of attack methods and countermeasures. ■

About the Author

Angela Orebaugh | is a technologist, researcher, and cybersecurity executive, who is passionate about helping clients embrace tomorrow’s technology today. Ms. Orebaugh was recently selected as Booz Allen Hamilton’s first and currently only Cyber Fellow, a distinction reserved for an elite group of the firm’s most noted authorities. She evangelizes social media and mobile technologies by highlighting the powerful ways in which these technologies are changing business, communications, and information sharing. Ms. Orebaugh is also the Information Assurance Technology Analysis Center Director of Research and Academic Integration. She is an international author and invited speaker for technology and security events. Follow her on

▷ ▷ *continued on page 33*

Q

In general, what are the biggest challenges to mobile application security testing?

I want to ensure that the applications I develop for mobile devices do not pose any significant security risks.

A

Mobile application security testing is still relatively new compared to general application testing. There are several challenges in adapting existing approaches to mobile device applications. These challenges include—

- ▶ Mobile devices usually have one user only, which is very different from systems having multiple user profiles.
- ▶ In the interest of making a mobile device easier to use, many users purposefully configure it to have weaker security settings. Many

users do not know how to configure their devices to maximize security features.

- ▶ Most mobile devices do not have encryption capabilities at the network or system level; therefore, encryption must happen at a higher level.

Key organizations are investigating ways to address mobile application security and its testing more effectively. For example, the National Security Agency is looking at how the intelligence community can access Top Secret information securely from mobile devices. [1] The Open Web Application Security Project is working diligently to identify mobile device security risks and solutions to address them. It is in the process of identifying top 10 lists for

mobile risks and for controls that users can implement. [2]

Overall, ensuring mobile devices are secure will remain a challenge moving forward. ■

References

1. http://www.nextgov.com/nextgov/ng_20110325_5941.php
2. https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project/Roadmap

To read more about mobile device security, read “Securing the Mobile Device...and its User” by Angela Orebaugh in this edition of the *IAnewsletter*.

▷ continued from page 23

SECURING THE MOBILE DEVICE...AND ITS USER

Twitter @AngelaOrebaugh and connect with her on Google+ at <http://gplus.to/angelaorebaugh>. She can be contacted at iatac@dtic.com.

References

1. Lieff, Laura. Mobile Spyware is Here. http://www.glendalecherrycreek.com/t_news_template/m_news_detail?id=168.
2. Katalov, Vladimir. ElmSoft Breaks iPhone Encryption, Offers Forensics Access to File System Dumps. <http://blog.crackpassword.com/2011/05/elcomsoft-breaks-iphone-encryption-offers-forensic-access-to-file-system-dumps/>.
3. Symantec. Norton Study Calculates Cost of Global Cybercrime: \$114 Billion Annually. http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02.
4. Hickey, Kathleen. 3 of 10 Android users now face malware attack. <http://gcn.com/articles/2011/08/03/android-hacks-rise.aspx>.
5. Brodtkin, Jon. Android Trojan records phone calls. <http://www.networkworld.com/news/2011/080111-android-trojan.html>.
6. Krehel, Ondrej. Worse Than Zombies: The Mobile Botnets are Coming. <https://www.infosecisland.com/blogview/14413-Worse-Than-Zombies-The-Mobile-Botnets-Are-Coming.html>.
7. Infosecurity-magazine.com. Analyst spots major changes in Android DroidDream malware. <http://www.infosecurity-magazine.com/view/20821/analyst-spots-major-changes-in-android-droiddream-malware/>.
8. Cluley, Graham. The top 10 passcodes you should never use on your iPhone. <http://nakedsecurity.sophos.com/2011/06/14/the-top-10-passcodes-you-should-never-use-on-your-iphone/>.
9. <http://www.pcmag.com/article2/0,2817,2367247,00.asp>
10. Infosecurity.com. One in five firms have no policy regarding personal mobile device use at work. <http://www.infosecurity-us.com/view/19765/one-in-five-firms-have-no-policy-regarding-personal-mobile-device-use-at-work/>.
11. Kenyon, Henry. State Using App that Separates Personal, Work Data on iPhones, Androids. <http://gcn.com/articles/2011/06/20/west-virginia-secure-app-for-iphone-android.aspx>.
12. Government Executive. Cybersecurity and Mobility Expert Dialogues. http://dialogues.govexec.com/govexec_archive/discussion160.html.
13. Gillis, Tom. Doctors Love the iPad. But What's the Prescription for Tablet Security? <http://www.forbes.com/sites/tomgillis/2011/07/30/doctors-love-the-ipad-but-whats-the-prescription-for-tablet-security/>.
14. Marks, Joseph. Going Mobile. http://www.nextgov.com/nextgov/ng_20110906_7177.php?oref=rss&utm_source=twitterfeed&utm_medium=twitter.