Smartphone Security Risks: Android

Lee Pin Shing and Lee Hur Shing
Virginia Tech, Blacksburg, VA, USA

Chen-Chi Shing
Radford University, Radford, VA, USA
Email: cshing@radford.edu

Meng Chu Chiang, Che Wei Yang, and Tzu-Chieh Lu
Tamkang University, New Taipei City, Taiwan

Marn-Ling Shing
University of Taipei, Taipei, Taiwan

Abstract—In the recent years, the smartphone has become one of the most popular devices of communication. Smartphones are convenient because of their small, portable size, as well as their ease of use. Many people know they need security for their computers, but they are not aware of the need for security in smartphones. In this paper, we want to discuss security of smartphones. We use list of top smartphone security risks the European Network and Information Security Agency (ENISA) and incorporate prevention actions that can be used as well as some additional security risks involved. Risks and threats are separate issues that should be known to the users of smartphones. The paper mainly focuses on risks but uses Android.Adrd as an example for threats. This paper specifically uses the Android operating system as an example. Google provides a set of cloud-based services that are available to any compatible Android device. These services are not part of the Android Open Source Project, but they are relevant to the security of most Android devices. The numerous examples in this paper show that Google could improve their services supporting the security of Android in order to increase the overall security reports of smartphones.

Index Terms—Android, security, smartphone

I. INTRODUCTION OF ANDROID

Android is an open source mobile operating system developed by Google [1]. Its applications make use of advanced hardware, software, as well as local and served data, exposed through the platform to bring innovation and value to consumers. In the security of Android, Android’s Company designed the multi-layered security that provides the flexibility required for an open platform, while providing protection for all users of the platform. In addition, Android’s company designed security controls to reduce the burden on developers. Security-savvy developers can easily work with and rely on flexible security controls and developers less familiar with security will be protected by safe defaults. Android also provides users into how applications work, and control over those applications.

The official website summarizes the security components and considerations of the various levels of the Android software stack. The core operating system is built on top of the Linux kernel. All device resources, like camera functions, GPS data, Bluetooth functions, phone functions, network connections, etc. are accessed through the operating system. Android applications are most often written in the Java programming language and run in the Dalvik virtual machine. They have two primary sources for applications:

A. Pre-Installed Applications

A set of applications already installed in Android’s operating system such as email, calendar, and web browser. Pre-installed applications are either part of the open source Android platform, or they are developed by an Original Equipment Manufacturer (OEM) for a specific device.

B. User-Installed Applications

An open development environment which be used to support any third-party application. These applications can be installed from the Google Play Store.

Google provides a set of cloud-based services that are available to any compatible Android device. These services are not part of the Android Open Source Project, but they are relevant to the security of most Android devices.

II. INTRODUCTION OF SMARTPHONES

The smartphone is a mobile phone with an operating system. It can provide advanced capabilities to users. Smartphones are now used universally by most people. Smartphones have different functions compared to traditional mobile phones.

Traditional mobile phones are portable phones before the year 2000. They are only used for calling, receiving sounds, sending messages, and play games. These
traditional phones are not smartphones and are called Feature Phones. On the other hand, a smartphone usually includes the following elements [2]:

- Pre-Installed with a modern mobile operating system, such as iOS, Android, or Windows Mobile.
- Support a carrier’s networks (2G/3G/4G), WiFi connectivity, and Bluetooth. These networks work independently and serve different purposes for voice and data services.
- Access the Internet. A smartphone provides Internet accessibility through either a carrier’s network or a local WiFi hotspot.
- Capable of running third party applications. These applications can be downloaded from application stores through the Internet.
- Support MMS messages. A smartphone supports Multi-media Message Service (MMS). A smartphone user can interact with another mobile phone subscriber through these messaging systems.
- Embedded sensors inside smartphones. Smartphone sensors usually include GPS, gyroscopic sensors, and accelerometer sensors.

III. RISK VS. THREATS

Risk is defined as the product of the likelihood and the impact of a threat against the information assets of an organization or an individual. Threats exploit one or more vulnerabilities. The likelihood of a threat is determined by the number of underlying vulnerabilities, the relative ease with which they can be exploited, and the attractiveness for an attacker [3].

IV. PURPOSE

Hackers and internet thieves can invade your computer to get important information. They can leave undetectable computer viruses. Many computer users install antivirus software like VIPRE Antivirus or Bitdefender AntiVirus to protect their system, but care less for the security of smartphones. Smartphones can also be attacked by hackers. For example, if you use popular travel applications such as Google Maps, or Apple Maps, impostors could potentially see the locations you’ve visited and figure out where you live. Each type of smartphone operating system has its own separate risks when it comes to hackers or malicious software. In fact, 79% of malware in 2012 was related to Google’s Android operating system. This is largely because the Google Play app store is built on an open model, with limited quality controls, making it easier for malicious apps to find their way onto your phone [4].

There are many different attacks that could result in having data stolen from smartphones. Having this publicly known and knowing ways to prevent these attacks can increase security awareness in smartphones.

V. METHOD OF SOLUTION

The following list provides an outlook on common smartphone security risks referred to the ENISA website and ways to lower these risks.

A. Data Leakage Resulting from Device Loss or Theft

Some users are used to saving important information on smartphones such as credit card numbers, bank account numbers, passwords, ID numbers, and home addresses. Most people don’t even use basic steps to secure their smartphones. A new nationwide survey by Consumer Reports found that 34 percent of all smartphone users in America don’t lock the screen; even with a simple code. In addition, Consumer Reports also found that only 36 percent of smartphone users in America have set a 4-digit PIN to lock their phone [5]. In Consumer Reports, they provide five steps to prevent data theft on your smartphone [6]:

Step 1: Use a strong screen lock
Skip the easy 4-digit PIN and instead create a strong password that contains a string of at least 8 characters that include some combination of letters, numbers, and special characters that don't form recognizable words or phrases, especially those that could be associated with you.

Step 2: Use a ‘find my phone’ app
An easy way to recover a missing phone is by attaching a note. Tape a tiny note on the back of your phone with your e-mail address or a work number. If an honest person finds the smartphone, he or she can contact the owner. This way may be unreliable since the note is likely to detach itself from the phone. There are apps that can find smartphones now when you give them your phone information.

The apps use the same GPS and network connections that help your phone find the best nearby restaurants and the fastest way home can help you find and protect that phone should it go missing.

Step 3: Back up your photos and videos
Phone carriers, phone makers, and operating systems typically offer free over-the-air back up for phone camera content, settings, and other features. The Android system uses Google+ to backup information. Users need to enter Google’s account number and password like accessing their Gmail account. Then Google can help users back up information to their Cloud. Not all of information can be backed up however, for instance game history cannot be backed up.

Step 4: Record your phone’s unique ID number
Smart phones have a unique serial number known as an IMEI (International Mobile Station Equipment Identity), see Fig. 1 or MEID (Mobile Equipment Identifier). These numbers are etched into its circuits and difficult to alter; just like a smartphone’s identity number. If owners lose their smartphones, they will call their network provider and instruct them to “blacklist” the phone using its IMEI number.

B. Unintentional Disclosure of Data

When users decide to download apps on the smartphone, they unintentionally disclose data on the
smartphone. Even if they have given explicit consent, users may be unaware that apps collect and publishes personal data that trace users. For example, some Apps like social networks always ask users to agree to transmit their location data. Location data is often included in image files. Users who give an app access to the image files may be unintentionally disclosing their whereabouts. Users need to read all of items clearly before you download any kinds of Apps.

C. Attacks on Decommissioned Smartphones

In the recent years, many people may choose to recycle their smartphones to reuse each year. Although most users think they have already deleted all of their information, the smartphones contain large amounts of sensitive information which may be valuable to an attacker. Attackers can use data to identify the owner or other people who have relation with owner. Users need to look for a legitimate recycling channel to protect data outflow.

D. Phishing Attacks

Phishing attacks are a well-known threat for users of traditional PCs. Phishing attacks are platform independent because the attacker does not need to attack the user’s device in any way. However, phishing attacks probabilities slowly grow because number of smartphone users increase. For example, attackers can easily disguise trust cues that users rely on to decide on submitting credentials because of the smaller screen of smartphone. App-stores provide a new way of phishing by allowing attackers to place fake apps in the app-store, disguising them as legitimate apps. Smartphones provide additional channels that can be used for phishing. Finally, many users who don’t know about phishing attacks may appear on smartphones, so we need to take more care to prevent it.

E. Spyware Attacks

Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer’s consent, or that asserts control over a computer without the consumer’s knowledge [7]. The amount of personal data, sensitive documents and credentials stored and processed by smartphones are collected by spyware. Users can download some security applications on Android but are limited to the same restricted environment as every other Android application. Even applications that claim to “block malware, spyware and phishing apps” require a rooted device in order to obtain the necessary permissions to perform these functions. Without security tools available, users cannot identify malicious content and the burden falls on the device manager [8]. Android.Tapsnake is an example of spyware that pretends to just be a game of snake, actually including a fully functional copy of the game. However in the background, the application is uploading the GPS coordinates of the device every 15 minutes. The attacker then uses another program to view the saved locations.

F. Network Spoofing Attacks

Rogue WiFi hotspots and Bluetooth devices can be used to intercept and tamper with the network communication to the smartphone. In this attack, a spoofed service configuration SMS is used to change the default access point used by the phone. Users can be mounted against control transfer. Those attacks will take advantage of the lack of secure application identity indicators in mobile operating systems and browsers. The user cannot always identify whether a link has taken him or her to the expected application [9].

G. Surveillance Attacks

Smartphones can be used to keep a targeted individual under surveillance because it contains multiple sensors such as microphones, cameras, accelerometers and GPSs. Sometimes the user can be tricked into helping the attacker by installing malicious apps. For example, some people can use your GPS to conjecture what time you are not at home. Other apps obtain read and write access to the address book by default, which allows an attacker to add a rogue email address to existing email addresses and receive email correspondence. There are many Android apps that turn the phone into a security surveillance camera, such as the Android Eye. This malicious camera app can periodically check the screen status and run the stealthy video recording only when the screen is off, which means that the user is not using the phone and the camera device is idle [10].

H. Diallerware Attacks

Certain smartphone API calls cost the user money, e.g. SMS (including micropayments), phone calls, and data over metered GSM/UMTS. If an attacker can install an app on the user’s smartphone, which can make covert API calls or trick the user into giving consent to its use, people can steal money from the smartphone user. One of the simplest security problems is the problem of decommissioning and recycling smartphones. The vast numbers which are passed on to third parties without the data have been properly wiped. The ENISA recommends that government officials don’t store sensitive data locally. Encryption software is used and smartphones should be periodically wiped (using secure deletion) and reloaded with a specially prepared and tested image [11].

I. Financial Malware Attacks

Financial malware is software specifically designed to steal credentials or perform man-in-the-middle attacks on financial applications or web services. Like PCs, smartphones are also vulnerable to banking malware. It may be a key-loggger collecting credit card numbers, or it may be more sophisticated and intercept SMS authentication codes to attack online banking applications. The strategy is for an attacker to submit an app impersonating a real banking app. Users need to download legal and secure financial apps from app-store.

J. Network Congestion

The uptake of smartphones and mobile Internet increases the risk of network congestion. Network
congestion can occur in two ways: signaling overload and data capacity overload. Signaling overload means always-on smartphone apps are constantly polling the network for updated information. On data capacity overload, solutions such as LTE and WiMAX promise improvements in spectral efficiency, the amount of data that can be transmitted over the air using the same amount of allocated spectrum.

Next, we want to introduce more security risks in the Android operating system.

1) Search engine poisoning

Some search engines recommend sites or change search engine rankings by monitoring the user’s visit rates. Malicious applications can initiate multiple requests to these sites, manipulating the hit rates monitored by the search engines to spread malware and viruses. Android.Adrd is an example of a threat that was poisoning the Baidu mobile search. The results were affected when the threat generated artificial visits to a news site when big news comes out. The artificial visits potentially increased their rank in the Baidu search results creating more opportunity for people to click on their links.

On top of search engine poisoning, Android.Adrd also attacked users through advertising. Users who search using a search box that Baidu affiliates can place on their site will be shown search results along with some advertisements. When users click the ads on some of the result websites, the company can receive money. Android.Adrd repeatedly contacts the following URL, mimicking searches from the search box on the “Focus Online” website: http://wap.baidu.com/s?word=[ENCODED SEARCH STRING]&vit=uni&from=[ID]. This is how people used Android.Adrd to increase revenue. When accompany increases their number of average daily searches, they also increase their revenue share.

2) Pay-per-click

A variety of services, such as advertising networks, pay each time an affiliate refers a user to a particular website (pay-per-click). Attackers can create and register video channels with a carrier. The carrier generates revenue for the attackers each time a user views their video or channel. The attackers use malicious applications to surreptitiously download video content, generating revenue for the attackers. For example, Android.Bgsvr is a threat that utilizes this monetization scheme. First, it changes the Access Point Name (APN) settings to cmnet/mmsc.monternet.com, which services a Chinese mobile TV network. The threat downloads a configuration file that specifies which video to download.

This paper can help smartphone users understand how vulnerable smartphones are, using Android as an example. With all the examples discussed, the Android Company should give developer and user security risk support to reduce the number of malicious attacks.

VI. CONCLUSION

Most smartphone users don’t care enough about the security of smartphones. They don’t have enough knowledge about the risks. We discuss, analyze these risks, and propose some ideas to solve or reduce these risks that come from ENISA. We also talked about two other risks: Search Engine Poisoning and Pay-Per-Click.

REFERENCES

[6] 5 steps to protect your smart phone from theft or loss also learn what to do when your phone goes missing and when you get it back. [Online]. Available: http://www.consumerreports.org/cro/2014/04/5-steps-to-protect-your-smart-phone-against-theft-or-loss/index.htm

Lee-Pin Shing has graduated (from College of Science) with biology major and business minor (from Pamplin College of Business), Virginia Tech, Blacksburg, VA, USA in 2015. He is now working on his MS degree in Information Technology at Virginia Tech.

Lee Hur Shing has graduated (from Pamplin College of Business) with Business Information Technology major, at Virginia Tech, Blacksburg, VA, USA in 2015. She is currently working on her MS degree in Information Technology at Virginia Tech. During the summer of 2015 she has also worked at Academica Sinica, Taipei, Taiwan.
Chen-Chi Shing holds a B.S. degree (Physics) from the Chen-Kung University, Taiwan and M.S. (Physics) and M.S. (Computer Science) degrees from Virginia Tech, an M.S. (Statistics) degree from the Ohio State University and a PhD (Experimental Design) degree from Virginia Tech, U.S.A. Dr. Shing also earned a graduate certificate in Information Assurance (supported by NSA) from Purdue University in the summer of 2004. He is a Professor teaching in the Computer Science concentration at the department of Information Technology (ITEC) at Radford University, Radford, Virginia. His research interests are related to modeling and simulation in security, security assurance, digital forensics, cloud security, data analytics, web survey tool development, repeated measurement designs, course outcome assessment and interface between computer science and statistics. He has been serving as the Editor-In-Chief for the International Journal of Computer Science and Security since June 2012.

Chiang Meng Chu was born in Taiwan on April 14, 1992. She graduated from Tamkang University, Ilan, Taiwan. She studies “Computer Science and Information Engineering” in graduate school at Tamkang University and is doing researches in the office of “Development and Application of Information Systems for Clinical Medicine” in Taiwan.

Marn-Ling Shing is Associate Professor at University of Taipei in the Department of Early Childhood Education. She received her Ph.D. in Psychology at the Ohio State University.

Che-Wei Yang is currently a graduate student in the Department of Computer Science and Information Engineering at Tamkang University, New Taipei City, Taiwan.

Tzu-Chieh Luis is currently a graduate student in the Department of Computer Science and Information Engineering at Tamkang University, New Taipei City, Taiwan.