Mobile Apps Threats

Donovan Peter Chan Wai Loon
University of Malaya, Malaysia

Sameer Kumar
University of Malaya, Malaysia

INTRODUCTION

In recent times smart mobile devices have become ubiquitous. More than half of all the mobile phones are now smartphones, and this statistic does not take into account the other devices such as tablets that are operating on similar systems (Gates, Chen, Li, & Proctor, 2014). With the abundant usage of smartphones, the way we go around our daily lives has certainly been transformed. The smartphones of today are more like mini computers than mobile phones of a few years back. Essentially, smart phones are computers with additional hardware—namely, a Global System for Mobile Communications or GSM radio and a baseband processor to control it (Miller, 2011).

Although this is great, there is also a threat emerging. In 2012 alone, Google estimated that more than 400 million Android devices had commenced operations. Android devices have been adopted widely for both personal and business use (Wang, Sun, Wang, & Jing, 2015). From adults to children, beginners to experts, and in numerous different countries around the world, there is a diverse user base for mobile devices (Gates et al., 2014). Attackers are now targeting these devices in the same way computers have been targeted for a long time. The extensive usage of mobile devices poses new threats to privacy and security of our digital lives (Zhou & Jiang, 2012; Zhou, Zhang, Jiang, & Freeh, 2011). Email messages, contact lists, passwords and files are often stored both locally and in the cloud. Illegal access to this private information by any unknown parties puts users at risk. Threats become even more dangerous as these devices may provide deep insights by integrating our digital to our daily lives. The GPS unit can pinpoint exact information of our whereabouts, while the microphone can record audio and the camera documents images (Khan, Xiang, Aalsalem, & Arshad, 2013). Moreover, mobile devices are frequently connected directly to monetary risks, via SMS authentication messages, as a means to validate financial transactions, or directly linked to bank account through a ‘digital wallet’ (Gates et al., 2014). Getting access would mean that any application (app) that operates on the devices has the potential to tap into and to provide certain details of information of the users.

The purpose of this article is to gauge the trends and challenges posed by malicious mobile applications. Specifically the authors look at the some of the current research to detect malicious applications and remedy for poor risk communications on Android-based devices.

The rest of the paper is organized as follows: In Section 2 we provide a background on mobile threats from an adapted threat model. Emerging mobile threats and an overview of mobile malware for Android and iOS is presented in Section 3 followed by an example of detecting malicious apps presented in Section 4. Future research directions are discussed in Section 5. Section 6 concludes the paper.

DOI: 10.4018/978-1-5225-2255-3.ch539

BACKGROUND

Understanding Mobile Threats

In order to offer a wide indication of threats facing mobile devices, it is first important to understand the objectives, reasons and distribution techniques of potential attacks. In this paper, we adapted a threat model from prior research by Delac, Silic, & Krolo (2011 p. 2-3) and divided into two main components: attack goals and attack paths. This is model is further supported by a similar study in the same year by Leavit (2011 p. 11-13) and has similar descriptions of the main components.

Attack Goals

Attack goals are motives for penetrating mobile devices. The objectives may be hidden or destructive intents. Hidden attacks are executed while eluding a user's detection. Destructive attacks on the other hand, are meant to interfere with the usual function of the mobile device.

- **Collect Private or Personal Data:** Attackers usually target confidential information stored on the device. An effective attack may permit the attacker with capability to read SMS messages, emails to contact details and call history. Additionally, attackers may retrieve classified information by accessing applications stored on the device. Furthermore, once the mobile device has been compromised, attackers may use the hardware features to gather extra data from an individual's environments. For example, the attacker may use the microphone to record audio, the camera to take photos and pinpoint a user's exact location information through the GPS component.
- **Exploiting Processing Properties:** Attackers target mobile devices for the raw processing capabilities. Most modern mobile devices come with high-powered CPU and multi core processors. Coupled with high speed Internet connectivity, mobile devices are appealing for malicious activities, such as distribution of botnets.
- **Destructive Activities:** These actions are meant to cause distress to the mobile users compared to benefiting the attackers. While easy to detect, attacks of this nature are designed at causing as much harm as possible. The attacks may vary from data corruption, draining the battery from the device, and generating huge network traffic (Delac et atl., 2011). Eventually, by acquiring controls to key systems, attacks could even deactivate the device rendering it useless.

Attack Paths

Attack paths are routes provided by mobile platforms for the distribution of malevolent packages. Mobile malware is malicious software malicious software developed particularly to attack mobile devices. Most attacks done are often a combination of several variants of mobile malware.

- **Mobile Network Services:** Initially, attackers used cellular services such as SMS, MMS and voice calls. False URL links are sent via SMS to unsuspecting users. When a user clicks the link, it automatically opens a browser allowing the device to be prone to an attack. MMS messages facilitated the delivery of malicious content through hidden codes embedded within the message as users downloaded the content. Voice calls on the other hand allowed attackers to maintain contact with the users by portraying to be a legal entity such as a bank asking for sensitive information such as credit card details. This act is also known as "phishing".
- **Internet Access:** Most modern mobile devices have Internet access through the use mobile networks such as 3G/4G or Wi-Fi networks. The chance for an attack rises