Chapter 4
Development and Mitigation of Android Malware

Vanessa N. Cooper
Kennesaw State University, USA

Hossain Shahriar
Kennesaw State University, USA

Hisham M. Haddad
Kennesaw State University, USA

ABSTRACT

As mobile applications are being developed at a faster pace, the security aspect of user information is being neglected. A compromised smartphone can inflict severe damage to both users and the cellular service provider. Malware on a smartphone can make the phone partially or fully unusable, cause unwanted billing, steal private information, or infect every name in a user's phonebook. A solid understanding of the characteristics of malware is the beginning step to prevent much of the unwanted consequences. This chapter is intended to provide an overview of security threats posed by Android malware. In particular, the authors focus on the characteristics commonly found in malware applications and understand the code level features that allow us to detect the malicious signatures. The authors also discuss some common defense techniques to mitigate the impact of malware applications.

INTRODUCTION

Android is an open source operating system for mobile devices. Statistics indicate that Android is having the fastest growth in the market share of the operating systems in the United States. Android has become the leading smartphone Operating System (OS) in the world with staggering sales figure of 60 million phones in the third quarter of 2011, 50% market share (Aaron, 2011). A recent study shows that more than 50% of mobile devices running Android OS have unpatched vulnerabilities, opening them up to malicious applications (malware) and attacks. A compromised smartphone can inflict severe damage to both users and the cellular service provider. Malware applications on Android can make the phone partially or fully unusable, cause unwanted billing, steal private information, or infect every name in a user's phonebook (Reza & Mazumder, 2012).

DOI: 10.4018/978-1-4666-6324-4.ch004

Recently, a malware affected more than 100,000 Android devices in China (known as *MMarketPay*). This malware is a hidden application that appeared to be legitimate and is designed to purchase applications and contents without the consent of the device users (victims). As a result, victims saw a staggering amount of bills (Baldwin, 2012). The incident prompted Google to introduce stricter rules for applications on Android such as naming of applications and banning applications that disclose personal information without user permission. An Android SMS malware firm was fined £50,000 by the UK premium phone services regulator *(“PhonePay Plus”, 2013)*. The company, *SMSBill*, produced a malicious Facebook link that led to the downloading of malware in Android phones (Baldwin et al. 2012).

Possible attack vectors into smart phones include Cellular networks, Internet connections (via Wi-Fi, GPRS/EDGE or 3G network), USB and other peripherals (Shabtai, Fledel, & Elovici, 2010). Given all these possible outcomes, it is important to study malicious Android applications and their characteristics. A solid understanding of the characteristics of malware is the beginning step to prevent much of the unwanted consequences. This chapter is intended to provide an overview of security threats posed by Android malware. In particular, we focus on the characteristics commonly found in malware applications and understand the code level features that allow us to detect the malicious signatures. We also discuss some common defense techniques to mitigate the impact of malware applications.

The chapter is organized as follows. Section 2 discusses an overview of Android OS structure as well as common security features offered. We also discuss the three types of applications that affect the security and privacy of users in general: grayware, spyware, and malware. Section 3 discusses code level examples showing malicious activities as well as some signatures that can be used to identify them. Section 4 discusses selected defense techniques to mitigate malware activities. Finally, Section 5 concludes the chapter.

BACKGROUND

In this section, we first provide an overview of the Android OS including its features and programming guidelines in Section 2.1. Section 2.2 highlights the architecture of the Android Operating Systems (OS) as well as brief discussion on security and privacy features. Section 2.3 highlights different types of malware that we consider in our discussion.

Overview of Android

Android is an open source operating system based on the Linux first launched in 2007 and intended for mobile phones (Rehm, 2012). Between the two major variants of smartphone (Android and iOS), Android is the most popular one. As of October 2013, the latest version of Android OS is 4.4 (commonly known as KitKat, API level 19). Being developed and supported by Google, all Android devices allow users to synchronize access to storage and communication services provided by Google. For example, users can login to Google Gmail to check email and access contact list, calendar, and other free applications automatically. The default desktop of Android has five screens that can be switched by tapping. A user can move any icon to any place on the desktop by tapping and hovering. Android devices allow users to download and install new applications for legitimate purposes that may include game, business, communication, photography, and services. The common place to find applications is Google Play Store (“Google Play”, 2013).

The Android Developer manual recommends some common practices for programmers for developing applications (“Android Design”, 2013). These include the guidelines for developing applications that are visually appealing to users. A developer can reuse standard theme that control visual properties of the elements for user interface of an application such as color, height, padding, and font size. Recommended guidelines for color and illumination of icons are provided to represent