Chapter 24
Application Security for Mobile Devices

Gabriele Costa
Università degli Studi di Genova, Italy

Fabio Martinelli
Consiglio Nazionale delle Ricerche, Italy

Aliaksandr Lazouski
Consiglio Nazionale delle Ricerche, Italy

Paolo Mori
Consiglio Nazionale delle Ricerche, Italy

ABSTRACT

In these last years, mobile devices, such as mobile phones and tablets, have become very popular. Moreover, mobile devices have become very powerful and commonly run fairly complex applications such as 3D games, Internet browsers, e-mail clients, social network clients, and many others. Hence, an adequate security support is required on these devices to avoid malicious application damage or unauthorized accesses to personal data (such as personal contacts or business email). This chapter describes the security support of the current commercial mobile devices along with a set of approaches that have been proposed in the scientific literature to enhance the security of mobile applications.

INTRODUCTION

Nowadays, mobile devices such as mobile phones and tablets, are very common among people, and a considerable part of the population owns at least one of these. In fact, Gartner Inc. (2013) says that “worldwide mobile phone sales to end users totaled 455.6 million units in the third quarter of 2013.... Sales of smartphones accounted for 55 percent of overall mobile phone sales....” In the last years, the hardware profiles of mobile devices has been growing continuously and it seems reasonable that this trend will not stop soon. Hence, mobile devices are becoming increasingly powerful, and their capabilities are growing even more rapidly than personal computers’ ones. In fact, many modern mobile devices are equipped with fast multi-core processors, high storage capacity, and they provide very good connectivity, i.e. they are able to connect to the Internet through the mobile operator network, they are able to connect to wireless networks, and they can communicate directly with other devices through Bluetooth or NFC interfaces. Many of them are also able to exploit the Global Positioning System (GPS) to determine their physical location. Hence, most of the existing mobile devices are actually comparable to personal computers, and they are

DOI: 10.4018/978-1-4666-8111-8.ch024

Copyright © 2015, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

able to run applications, developed for their specific operating system (e.g., Apple iOS, Google Android and Microsoft Windows) or exploiting Java Micro Edition (Java ME, a light version of Java for resource constrained devices), or the. NET Compact framework. By also exploiting the pervasiveness of the mobile networks, mobile devices are becoming the privileged access point for the internet of services. As a consequence, they manage several critical resources and represent an amenable target for security attacks.

A common way of distributing malware is through mobile code. This is clearly witnessed by the increasing number of reported malwares specifically designed for mobile devices. In fact, the list of threats which is currently available on the Symantec Security Response web portal[1] includes a very large number of malwares designed for mobile devices, mainly for Android OS, and Felt, Finifer, Chi, Hanna, and Wagner (2011) try to describe the motivation behind some mobile malware. A piece of malicious software receiving inadequately permissive privileges can disruptively interact with the platform hosting it. The standard approach for the distribution of mobile code relies on application stores/markets. An application store is a repository, typically managed by a trusted party, where developers upload their applications. The customers access the store, browse the applications and download those they are interested into. Google Play Store, Apple App Store and Nokia OVI store are some examples of this approach. The usage of centralized software stores is not limited to mobile devices and the same reasoning can be applied to other contexts (e.g., integrated development environments, browsers and smart TVs).

Application stores drastically increase the potential of an attacker. Indeed, applications can rapidly gain visibility and literally thousands of devices could receive a malicious software in just few seconds. However, they also represent a valuable resource for the detection and prevention of this kind of attacks. For this to happen, it is necessary that the stores implement techniques actually preventing or, when not possible, mitigating the damage caused by malicious applications. Applications for mobile devices can be developed for a specific mobile device operating system, or using Java Micro Edition, or the.NET Compact framework. Applications developed for a mobile device-specific operating system can run only on that class of devices. As an example, the applications developed for the iOS operating system runs on Apple iPhones and iPads, but cannot run, for instance, on Android devices. The applications developed in Java ME, instead, can run on all the devices that mount a Java ME runtime environment.

In this chapter, we give a brief overview of the application security support of Java ME, Android and iOS, and we introduce some existing research approaches to enhance the security of mobile devices by grouping them in three sets: credential based, static verification and runtime monitor approaches.

SECURITY OF THE MODERN MOBILE PLATFORMS: AN OVERVIEW

This section describes the application security support provided by the two main mobile OS, Android and iOS, and of Java ME. According to Garner Inc. (2013), in the third quarter of 2013 Android and iOS had 94% of the global market share. This makes them very appealing for both attackers and researchers. Moreover, since Android is based on an open source project, several authors focused on it when proposing techniques and tools.

Security Models for Java-Based Platforms

Some of the most common mobile OSs are based on (or natively support) the Java framework. For instance, Symbian OS uses a lightweight version

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/application-security-for-mobile-devices/125307

Related Content

Standards Management in the Twenty-First Century: Architectural Challenges and Management Opportunities
Michael B. Spring (2016). *International Journal of Standardization Research (pp. 34-44).*
www.irma-international.org/article/standards-management-in-the-twenty-first-century/165133

Standards for Business Component Markets: An Analysis from Three Theoretical Perspectives
Heiko Hahnand Klaus Turowski (2008). *Standardization Research in Information Technology: New Perspectives (pp. 143-162).*
www.irma-international.org/chapter/standards-business-component-markets/29686

Profiles and Motivations of Standardization Players
Cesare A. F. Riillo (2013). *International Journal of IT Standards and Standardization Research (pp. 17-33).*
www.irma-international.org/article/profiles-and-motivations-of-standardization-players/83545

The Impacts of the Cascading Style Sheet Standard on Mobile Computing
Matt Germonprezand Michel Avital (2006). *International Journal of IT Standards and Standardization Research (pp. 55-69).*
www.irma-international.org/article/impacts-cascading-style-sheet-standard/2578

Standardization, Innovation, and Organization: A Contingency Perspective
Nizar Abdelkafiand Sergiy Makhotin (2016). *Effective Standardization Management in Corporate Settings (pp. 286-308).*
www.irma-international.org/chapter/standardization-innovation-and-organization/141773