Chapter 12

Application Security for Mobile Devices

Gabriele Costa
Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Italy

Aliaksandr Lazouski
Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Italy

Fabio Martinelli
Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Italy

Paolo Mori
Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Italy

ABSTRACT

In these last years, mobile devices, such as mobile phones or Personal Digital Assistants, became very popular among people. Moreover, mobile devices became also very powerful, and most of them are also able to execute applications, such as games, Internet browsers, e-mail clients, and so on. Hence, an adequate security support is required on these devices, to avoid that malicious applications damage the device or perform unauthorized accesses to personal data (such as the contact list). This chapter describes the approaches that have been proposed in scientific literature to guarantee the security of mobile devices.

INTRODUCTION

Nowadays, mobile devices, e.g. Smart Phones and Personal Digital Assistants (PDAs), are very common among people and a considerable part of the population owns at least one of them. For instance, if we query the Wolfram Alpha engine for the number of mobile phones in the European Union and we compare it with the overall EU population, we find that the 497 million EU citizens own about 605 million devices, that is, an average of more than 1.2 devices each.

Also, mobile devices are becoming increasingly powerful, and their capabilities are growing even more rapidly than personal computers’ ones. Actually, many modern mobile phones are very powerful devices, with fast processors and high storage capacity. They have embedded cameras...
and typically very good connectivity capabilities, 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 the Bluetooth interface. Some of them are also able to exploit the Global Positioning System (GPS) to determine their physical location. As an example, the Nokia E72 mobile phone embeds an ARM 11 600 MHz CPU, can host up to 16GB memory and it supports 802.11 b/g wireless network and 10.2Mbps HSDPA network.

Hence, most of the existing mobile devices are actually comparable to personal computers, and they are able to run applications, developed for their specific operating system or in Java Micro Edition (Java ME, a light version of Java for resource constrained devices), such as games, Internet browsers, e-mail clients, chat tools, document viewers and editors, multimedia players navigation tools, and so on.

Moreover, in the last years, the main telco operators started offering cheap and fast mobile broadband connections, and this increases the downloading of software for mobile devices and, consequently the offer for these applications. As an example, the Nokia OVI store and the Apple AppStore offer a very large number of applications that can be easily downloaded and installed on Nokia phones and on Apple devices.

However, this increased availability of applications for mobile devices introduces new threats, because these applications could perform some operations that are critical from the security point of view, such as connecting to the Internet, sending and receiving SMS/MMS messages, connecting to other devices through the Bluetooth interface, browsing the user’s contact list, and many others. The attacks performed by malicious applications could be more dangerous if sensitive, personal data is stored on mobile devices (as it commonly happens). As an example, a malicious application could establish a network connection to a remote server and transfer to this server all the contacts or all the SMS messages stored in the mobile device.

Malicious software for mobile devices already appeared. As an example, in June 2004 the first virus for the Symbian operating system, called Caribe, was created. This virus exploited the Bluetooth interface for infecting other devices. In the same year, another virus, Duts, was created to infect devices with the Windows Mobile operating system. Many other viruses appeared from that moment on. An important point is that most of these viruses, to infect mobile phones, do not exploit any vulnerability of the systems; it is the user that confirms that the file including the virus can be downloaded and installed on the mobile device.

Hence, despite the growth of both the number of mobile devices and their capabilities, the security support currently available on mobile devices did not follow the same evolution. In fact, most of the mobile devices available on the market adopt a security model which simply relies on informal trust based assurances. For instance, Java ME applications, namely MIDlets, are assigned to a specific privilege class depending only on their provider. There are no other guarantees that downloaded applications will not damage the resources of mobile devices during execution. However, some new approaches have been recently proposed in the scientific literature to improve the security model of mobile devices, and this chapter surveys the most promising ones.

Applications for mobile devices can be developed for a specific mobile device operating system, or using JavaME, or the.NET Compact framework for mobile device. Applications developed for the mobile device specific operating system can run only on that class of devices. As an example, the applications developed for the Symbian operating system that runs on most of the NOKIA devices cannot run, for instance, on Apple iPhones. The applications developed in Java ME, instead, can run on all the devices that provide a support for Java ME. Since most of the mobile