Chapter III
Security of Symbian Based Mobile Devices

Göran Pulkkis
Arcada Polytechnic, Finland

Kaj J. Grahn
Arcada Polytechnic, Finland

Jonny Karlsson
Arcada Polytechnic, Finland

Nhat Dai Tran
Arcada Polytechnic, Finland

ABSTRACT

Security issues of Symbian-based mobile computing devices such as PDAs and smart phones are surveyed. The evolution of Symbian OS architecture is outlined. Security threats and problems in mobile computing are analyzed. Theft/loss of the mobile device or removable memory cards exposes stored sensitive information. Wireless connection vulnerabilities are exploited for unauthorized access to mobile devices, to network, and to network service. Malicious software attacks in form of Trojan horses, viruses, and worms are also becoming more common. The Symbian OS is open for external software and content which makes Symbian devices vulnerable for hostile applications. Embedded security features in Symbian OS are: a cryptographic software module, verification procedures for PKI signed software installation files, and support for the communication security protocols IPSec and TLS. The newest version 9.3 of Symbian also embeds a platform security structure with layered trusted computing, protection capabilities for installed software, and data caging for integrity and confidentiality of private data. Fundamental security requirements of a Symbian based mobile device such as physical protection, device access control, storage protection, network access control, network service access control, and...
INTRODUCTION

Users of the Internet have become increasingly more mobile. At the same time, mobile users want to access Internet wireless services demanding the same quality as over a wire. Emerging new protocols and standards, and the availability of WLANs, cellular data and satellite systems are making the convergence of wired and wireless Internet possible. Lack of standards is however still the biggest obstacle to further development. Mobile devices are generally more resource constrained due to size, power and memory. The portability making these devices attractive greatly increases the risk of exposing data or allowing network penetration.

Mobile handheld devices can be connected to a number of different kinds of networks. Such wireless networks are cellular networks, personal area networks (PANs), local area networks (LANs), metropolitan area networks (MANs) and wide area networks (Satellite-based WANS). Network services needed for transferring data to and from a mobile device include among others e-commerce, electronic payments, WAP and HTTP services. The network connection of a mobile device can be based on a dial-up connection through a cellular network (GSM, UMTS), be based on packet communication through a cellular network (GPRS), be a WLAN or a Bluetooth connection, or be an infrared link (IrDA). Network connection examples are e-mailing (pop3, pop3s, imap, imaps, smtp, smtps), web browsing (http, https), synchronization with a desktop computer (HotSync, ActiveSync, SyncML), network monitoring/management (snmp), reception of video/audio streams, and communication of any installed application.

Realization of data services over mobile devices offers interesting new features for the user, but also a threat to security. A mobile device optimized for data services requires that the terminal becomes an open platform for software applications, i.e. the mobile device becomes more vulnerable to attacks. Mobile computing also requires operating systems supporting mobile environments. Such a widely used operating system is Symbian OS.

Symbian is a common operating system for mobile communication devices. The most important requirements are multitasking/threading, real-time operation of the cellular software, effective power management, small size of the operation system itself, ease of developing new features, reusability, modularity, connectivity and robustness (DIGIA Inc., 2003). The world’s top mobile phone manufacturers with the largest market share have chosen Symbian. According to many analysts, the major part of operation systems for mobile communication devices of the future will rely on Symbian or on Windows.

In this chapter, security issues of Symbian based mobile devices are surveyed.

BACKGROUND

Mobile computing device types are pocket PC, also called personal digital assistant (PDA), and smart phone. Symbian is the leading operating...