Security Architectures of Mobile Computing

Kaj Grahn
Arcada Polytechnic, Finland

Göran Pulkkis
Arcada Polytechnic, Finland

Jonny Karlsson
Arcada Polytechnic, Finland

Dai Tran
Arcada Polytechnic, Finland

INTRODUCTION

Mobile Internet users expect the same network service quality as over a wire. Technologies, protocols, and standards supporting wired and wireless Internet are converging. Mobile devices are resource constrained due to size, power, and memory. The portability making these devices attractive also causes data exposure and network penetration risks.

Mobile devices can connect to many different wireless network types, such as cellular networks, personal area networks, wireless local area networks (WLANs), metropolitan area networks (MANs), and wide area networks (satellite-based WANs). Wireless network application examples are e-mailing, Web browsing, m-commerce, electronic payments, synchronization with a desktop computer, network monitoring/management, and reception of video/audio streams.

BACKGROUND

Major security threats for mobile computing devices are (Olzak, 2005):

- theft/loss of the device and removable memory cards,
- wireless connection vulnerabilities, and
- malicious code.

Mobile computing devices are small, portable, and thus easily lost/stolen. Most mobile platforms only include support for simple software-based password login schemes. These schemes are easily bypassed by reading information from the device without login. Memory cards are also easily removed from the device.

Mobile devices support wireless network connections such as Bluetooth and WLAN. These connections are typically by default unprotected and thus exposed to eavesdropping, identity theft, and denial-of-service attacks.

Malware has constituted a growing threat for mobile devices since the first Symbian worm (Cabir) was detected in 2004. Mobile devices can be infected via MMS, Bluetooth, infrared, WLAN, downloading, and installing from the Web. Current malware is focused on Symbian OS and Windows-based devices. Malware may result in (Olzak, 2005):

- loss of productivity,
- exploitation of software vulnerabilities to gain access to resources and data,
- destruction of information stored on a SIM (subscriber identity module) card, and
- hi-jacking of airtime resulting in increased costs.

WIRELESS SECURITY PRINCIPLES

Security Policy

Examples of rules proposed for mobile device end users are:

- I agree to make sure my device is password protected and that latest security patches are installed.
- I agree to keep a firewall/anti-virus client with latest anti-virus signatures installed, and to use a remote access VPN client, if I will connect to the corporate network.
- I agree to use the security policies recommended by the corporate security team.

Examples of rules proposed for administrators of mobile devices in corporate use are:

- End-users get mobile network access after agreeing to the end-user rules of behavior.
- Handheld firewalls shall be configured to log security events and send alerts to *security-manager@company.com*.
- Handheld groups and Net groups shall have restricted access privileges and only to needed services.

Handheld security policies should be automated by restrictive configuration settings for handhelds, firewalls, VPNs, intrusion detection systems, and directory servers (Handheld Security, 2006).

Storage Protection

Mobile device storage protection is online integrity control of all stored program code and all data, optional confidentiality of stored user data, and protection against unauthorized tampering of stored content. Protection should include all removable storage modules used by the mobile device.

The integrity of the operating system code, the program code of installed applications, and system and user data can be verified by checksums, cyclic redundancy codes (CRCs), hashes, message authentication codes (MACs, HMACs), cryptographic signatures, and so forth. However, only hardware protection of verification keys needed by MACs, HMACs, and signatures provide strong protection against tampering attacks. Online integrity control of program and data files must be combined with online integrity control of the configuration of a mobile device for protection against malware intrusion attempts.

User data confidentiality can be granted by file encryption software. Such software also protects integrity of stored information, since successful decryption of an encrypted file is also an integrity proof.

Security Layers

Mobile computing security layers are based on the OSI (Open Systems Interconnection) Security Model. Defined security services are *authentication, access control, non-repudiation, data integrity, confidentiality*, *assurance/availability,* and *notarization/signature* (ISO/IEC 7498-1, 1994; ISO 7498-2, 1989).

Specific wireless security architecture issues include Mobile IP security features, and link-level and physical-level security protocols of wireless access technologies like WLAN, GPRS, and Bluetooth

Mobile IP security means that:

- a mobile node, which is a mobile device, has the same connectivity and security in a visited foreign network as in its home network; and
- the home network and visited foreign networks have protection against active/passive attacks.

These security goals require:

- that Mobile IP registration and location update messages have *data integrity protection, data origin authentication,* and *anti-replay protection*;
- *access control* to foreign network resources used by visiting mobile nodes; and
- that IP packet redirecting tunnels provide *data integrity protection, data origin authentication,* and *data confidentiality.*

Moreover, mobile nodes should have *location privacy* and *anonymity* (Zao et al., 1999).

Replay prevention with timestamps or nonces for all mobile IP messages is specified in Perkins and Calhoun (2000). Other mobile IP security solutions are authentication schemes and protection of data communication (Calhoun et al., 2005; Barun & Danzeisen, 2001; Hwu, Chen, & Lin, 2006).

Identification Hardware

Identification hardware contains user information and cryptographic keys used to authenticate users to mobile devices, applications, networks, and network services.

The following identification hardware types are used:

- subscriber identity module (SIM),
- public key infrastructure SIM (PKI SIM),
- universal SIM (USIM), and
- IP multimedia services identity module (ISIM).

SIM

A basic SIM card is a smartcard securely storing a key (Ki) identifying a GSM network user. A SIM card is a microcomputer executing cryptographic operations with Ki. The SIM card also stores SMS (short message service) messages, MMS (multimedia messaging system) messages, and a phonebook. The use and content of a SIM card is PIN protected (Rankl & Effing, 2003).

PKI SIM

A PKI SIM card is a basic SIM card with added PKI functionality. An RSA co-processor is added for public key-based encryption and signing with private keys. The PKI SIM card stores private keys and certified public keys needed for digital signatures and encryption (Setec, 2006).