Chapter 2.27
Developing a Theory of Portable Public Key Infrastructure (PORTABLEPKI) for Mobile Business Security

Sashi Nand
Rushmore University, BWI

INTRODUCTION

This chapter looks at how a public key infrastructure (PKI) can increase the wireless network's security by requiring certificate-based authentication for access. It also develops a theory of PORTABLEPKI. Finally, a framework for testing PORTABLEPKI and future research opportunities are discussed.

MOBILE BUSINESS

Mobile Business (m-business) can simplistically be understood as follows:

M-Business = Internet + E-Business + Wireless

M-business is the application infrastructure required to maintain business relationships by means of mobile devices. M-business is also the logical extension of electronic business (e-business) to address new customer channels and integration challenges. There is an interconnection of business processes within an organization and between external parties. For the notion of "business without boundaries" to prevail, back-end applications and data must be re-engineered to take complete advantage of the features offered by m-business (Kalakota & Robinson, 2002).

The most challenging and complex aspects of the m-business revolution are the design implementation, security, and integrity of mobile-enhanced business processes because they transcend traditional and regulatory boundaries (Stanley, 2004).

WIRELESS NETWORK

Wireless technologies are based on communication without land-based physical connections.

For example, traditional telephone handsets use continuous cabling for connectivity, hence it is wired. Wireless telephony, on the other hand, uses radio waves rather than cables to broadcast network traffic and data transmission.

The two primary areas of wireless technology are mobile phones and mobile computers. Mobile implies portability—a device such as a mobile phone, PalmPilot, or laptop that travels with the user and can be used either off-line or online:

- *Mobile and off-line* means that the device can be used to run self-contained applications while not connected to the Internet or other telephony devices.
- *Mobile and online* is commonly called wireless. This means that the experience is based on a live connection supplied via satellite, cellular, or radio transmission. An online device will always be 'on' in the presence of any wireless network—seamlessly connecting to the Internet or some other system (Kalakota & Robinson, 2002).

What is a Wireless Network?

In a wireless network, radio waves carry the signal at least part of the way. The greater the proportion of the wireless to wired, the more wireless we consider the network. Three basic wireless networking technologies include:

- **Wireless Private Area Networks (WPANs):** Refer to confined short-range networks, for example computers connected while traveling such as mobile phones, laptops, and personal digital assistants (PDAs).
- **Wireless Local Area Networks (WLANs):** Refer to same local-range networks, for example computers connected within the same area such as an office building or home.
- **Wireless Wide Area Networks (WWANs):** Refer to long-range networks, for example computers connected over long distances such as a university campus, city, or town (Shaw, 2003).

SECURITY

With any new technology—especially wireless networking—concerns and questions arise about security of data transmission (Shaw, 2003). Security is a process of minimizing risk, threat, or the likelihood of harm (Pipkin, 2000).

Wireless communications are inherently more open to attack than wired data transfer because the physical layer is the uncontained cyber-space (Campbell, Calvert, & Boswell, 2003).

An insecure wireless connection exposes users to intrusion, which can lead to a loss of protection for confidential information, interception of messages, or abused connections. Some examples are:

- E-mail can be intercepted, read, or changed.
- A hacker who hijacks a session can replace a user's credentials with false information gaining access to the system.
- An unauthorized person can log on to a wireless network that is not secure and use the resources, or obtain financial gain through deception including free connectivity to the Internet (Chan, 2004).

Security dominates discussions about wireless communication. The reason is simple: removing the wires simultaneously removes the access restrictions. In fact, many wireless networks begin life completely unsecured because vendors design wireless access points (WAPs) and WLAN cards with ease of installation and usage in mind. Configuration of security settings does not equate with ease of use. For this reason, a secure network needs to be set up intentionally and consciously (Randall & Sosinsky, 2005).

Even the most technically efficient and well-