Chapter XLIII
Security in WLAN

Mohamad Badra
Bât ISIMA, France

Artur Hecker
INFRES-ENST, France

ABSTRACT

The great promise of wireless LAN will never be realized unless there is an appropriate security level. From this point of view, various security protocols have been proposed to handle wireless local-area network (WLAN) security problems that are mostly due to the lack of physical protection in WLAN or because of the transmission on the radio link. The purpose of this chapter is (1) to provide the reader with a sample background in WLAN technologies and standards, (2) to give the reader a solid grounding in common security concepts and technologies, and (3) to identify the threats and vulnerabilities of WLAN communications.

WLAN STANDARDS AND TECHNOLOGIES, BENEFITS AND USE CASES

IEEE 802.11/wireless local-area network (WLAN) technologies (WLAN, 2003) have evolved phenomenally over the last few years. They have been widely deployed in a variety of network environments and they properly converge with actual Internet and 3G infrastructures.

IEEE 802.11 refers to a set of specifications for WLAN developed by IEEE. It specifies an over-the-air interface between a mobile station (STA) and a base station as well as between two mobile stations. Basically, WLAN networks can be seen as extensions of wired Ethernet networks. WLAN leverages on a set of newest digital communications technologies to make it possible to establish a local area network for computer communications without the use of cables.

IEEE approved the first 802.11 standard in 1997. This version is limited to only 1 and 2 Mbps data rates. Subsequently in 1999, 802.11a and 802.11b were approved, expanding to new radio bands (changing the usage of the 2.4 GHz ISM band and adding usage of the 5 GHz UNII band) and increasing the available data rates to 54 Mbps and 11 Mbps, respectively. Consequently, large deployments of

802.11 WLAN started being rolled out, especially in enterprises to replace or extend the wired local-area network (LAN) with an implementation of WLAN, and in airports and various business venues where they installed several WLAN access points offering a public Internet access (so-called hotspots), which can range from a small covered zone to many square miles of overlapping hotspots in metropolitan areas.

While the most obvious advantage of the WLAN is mobility, there are also other benefits:

- **Installing and maintaining flexibility:** Installation of a WLAN system is fast and easy and eliminates the terminal cabling costs. It extends to area where wires cannot be installed.
- **Apparent ease of use:** WLAN is easy for novice and expert users alike, eliminating the need of a large knowledge to take advantage of WLAN.
- **Transparency:** WLAN is transparent to a user network, allowing applications to work in the same way as they do in wired LANs.
- **Scalability:** WLANs are designed to be simple or complex; they range from networks suitable for a small number of nodes to full infrastructure networks of thousands of nodes and large physical area by adding access points to extend coverage and to provide users with roaming between different areas.

WLAN was developed to extend wired LAN wirelessly and therefore to minimize Ethernet cabling. It was designed to provide "data obscurity" equivalent to that provided by wired Ethernet with easier installation. However, there is some difference between WLAN and wired LAN due to constraints introduced by the first, especially the shared medium, interference, the collisions that cannot be detected reliably, the physical boundary that is difficult to control, and to the signal. These differences make the WLAN security harder to maintain in comparison to wired LAN. In WLAN, it is possible for an attacker to snoop on confidentiality communications or modify them to gain access to the network much more easily than the wired LAN. The open access to the networks permits malicious action at a distance and simplify passive interception. The temptation for unauthorized access and eavesdropping is also a reality (Khan & Khwaja, 2003) because an attacker could easily access the transport medium. This is not easy in wired LAN due to the physical access to the media. WLANs have introduced a new security threat, sometime referred to as parking lot attack (Arbaugh, 2003) (i.e., a person with a wireless computer and a makeshift antenna can gain access to your the WLAN from hundreds of feet away). Other security issues are mostly because of the lack of physical protection of the wireless network access or of the transmission on the radio that cannot be confined to the walls of an organization.

The original 802.11 standard defines authentication and encryption mechanisms based on the use of the wired equivalent privacy (WEP) protocol. Unfortunately, this protocol suffers from serious design flaws (Miller & Hamilton, 2002). Furthermore, it does not define a key management mechanism; it presumes that the secret key is conveyed between WLAN entities through a secure channel independent of 802.11 WLAN. As a result of different flaws discovered in WEP, the security of WLAN has been widely studied, and a set of standards have been developed by IEEE and IETF, especially 802.1X (802.1X, 2004), 802.11i (802.11i, 2004) and extensible authentication protocol (EAP) (Aboba, Blunk, Vollbrecht, Carlson, & Levkowetz, 2004). The 802.1X standard has been standardized by 802.1 working group. 802.1X was initially conceived to securely manage the access to different IEEE 802.1 networks. It is a framework for authenticating and controlling user traffic at the network level, as well as dynamically varying and exchanging encryption keys between a mobile station and an authentication server. By pushing the authentication method to the virtual layer, the 802.1X defines an open security architecture, which principally allows user authentication and, optionally, session key generation and derivation on a per-user and per-session basis. Because of this possibility for dynamic provisioning, 802.1X is used as the common base in the current WLAN