Chapter 7.13
Wireless LAN Setup and Security Loopholes

Biju Issac
Swinburne University of Technology, Malaysia

Lawan A. Mohammed
Swinburne University of Technology, Malaysia

ABSTRACT

This chapter gives a practical overview of the brief implementation details of the IEEE802.11 wireless LAN and the security vulnerabilities involved in such networks. Specifically, it discusses about the implementation of EAP authentication using RADIUS server with WEP encryption options. The chapter also touches on the ageing WEP and the cracking process, along with the current TKIP and CCMP mechanisms. War driving and other security attacks on wireless networks are also briefly covered. The chapter concludes with practical security recommendations that can keep intruders at bay. The authors hope that any reader would thus be well informed on the security vulnerabilities and the precautions that are associated with 802.11 wireless networks.

INTRODUCTION

Over the recent past, the world has increasingly becoming mobile. As mobile computing is getting more popular each day, the use of wireless local area network (WLAN) is becoming ever more relevant. If we are connected to a wired network, our mobility is undoubtedly affected. From public hotspots in coffee shops to secure WLAN in organizations, the world is moving to ubiquitous and seamless computing environments. IEEE 802.11 has been one of the most successful wireless technologies, and this chapter would be focusing more on this technology.

Mobility and flexibility has been the keynote advantages of wireless networks in general. Users can roam around freely without any interruption to their connection. Flexibility comes in as users can get connected through simple steps of authentication without the hassle of running

cables. Also, compared to the wired network, wireless network installation costs are minimal as the number of interface hardware is minimal. Radio spectrum is the key resource, and the wireless devices are set to operate in a certain frequency band. 802.11 networks operate in the 2.4 GHz ISM band, which are generally license free bands. The more common 802.11b devices operate in the S-band ISM.

In the next sections, we will be explaining the wireless LAN basic setup and implementation, WEP encryption schemes and others, EAP authentication through RADIUS server and its brief implementation, WEP cracking procedure, war driving, 802.11b vulnerabilities with security attacks, and finally concluding with WLAN security safeguards.

WIRELESS LAN NETWORK AND TECHNOLOGIES INVOLVED

Network Infrastructure

To form the wireless network, four generic types of WLAN devices are used. These are wireless station, access point (AP), wireless router, and wireless bridge. A wireless station can be a notebook or desktop computer with a wireless network card in it. Access points act like a 2-port bridge linking the wired infrastructure to the wireless infrastructure. It constructs a port-address table and operates by following the 3F rule: flooding, forwarding, and filtering. Flooding is the process of transmitting frames on all ports other than the port in which the frames were received. Forwarding and filtering involve the process of transmitting a frame based on the port-address mapping table in AP, so that only the needed port is used for transmission. Wireless routers are access points with routing capability that typically includes support for dynamic host control protocol (DHCP) and network address translation (NAT). To move the frames from one station to the other, the 802.11 standard defines a wireless medium that supports two radio frequency (RF) physical layers and one infrared physical layer. RF layers are more popular now (Held, 2003, pp. 7-14).

Modes of Operation

IEEE802.11 WLAN can operate in two modes, namely ad hoc (or peer-to-peer) and infrastructure mode. These modes come under the basic service set (BSS), which is a coverage area of communication that allows one station to communicate to the other. *Ad hoc* mode has WLAN stations or nodes communicating with one another without an access point to form an independent basic service set (IBSS). In contrast, *infrastructure* mode has WLAN nodes communicating with a central AP that is, in turn, linked to a wired LAN to form a basic service set. Here, the AP acts as a relay between wireless stations or between wired and wireless stations. A combination of many BSS with a backbone distribution system (normally ethernet) forms an extended service set (ESS).

IEEE 802.11 Architecture and Standards

802.11 is a member of IEEE 802 family, which defines the specifications for local area network technologies. IEEE 802 specifications are centered on the two lowest layers of OSI model, namely the physical layer and the data link layer. The base 802.11 specification includes the 802.11 MAC layer and two physical layers namely, the frequency hopping spread spectrum (FHSS) layer in the 2.4 GHz band, and the direct sequence spread spectrum (DSSS) layer. Later revisions to 802.11 added additional physical layers like high-rate direct-sequence layer (HR/DSSS) for 802.11b and orthogonal frequency division multiplexing (OFDM) layer for 802.11a.

The different extensions to the 802.11 standard use the radio frequency band differently. Some of the popular 802.11 extensions are as follows: