WLAN Security Management

Göran Pulkkis
Arcada University of Applied Sciences, Finland

Kaj J. Grahn
Arcada University of Applied Sciences, Finland

Jonny Karlsson
Arcada University of Applied Sciences, Finland

INTRODUCTION

In a wired local area network (LAN), the network ports and cables are mostly contained inside a building. Therefore, a hacker must defeat physical security measures, such as security personnel, identity cards, and door locks, to be able to physically access the LAN. However, the penetration capability of electromagnetic waves exposes the data transmission medium of a wireless LAN (WLAN) to potential intruders (Potter & Fleck, 2003).

The fast development of wireless technologies implies that wireless communications will become ubiquitous in homes, offices, and enterprises. In order to conserve power and frequency spectrum, the wireless device computation overhead is most often reduced. The conventional security design thus uses smaller keys, weak message integrity protocols, and weak or one-way authentication protocols (Hardjono & Dondeti, 2005). WLAN security thus requires a more reliable protection of data communication between WLAN units and strong access management mechanisms.

BACKGROUND

Today, WLANs provide acceptable security for most applications, but only if the security requirements are accurately identified and addressed. In addition, active monitoring of WLAN security is needed to detect intrusion attacks, to detect improperly configured security options, and to maintain acceptable security.

A new generation of WLAN management and security tools based on the released 802.11i security standard now offers secure user authentication and protected data communication. These upgrades will rather fast replace traditional network and security management tools. Therefore, administrating, maintaining, and monitoring WLAN security requires familiarity with the available security technology and corresponding tools and products.

WLAN SECURITY POLICY ISSUES

The rule set in Geier (2002) is an example of a basic WLAN security policy:

- Activate WEP (Wired Equivalent Privacy) at the very least
- Utilize dynamic key exchange mechanisms
- Ensure that NIC (Network Interface Card) and AP (access point) firmware is up-to-date
- Ensure that only authorized people can reset the APs
- Properly install all APs
- Disable APs during non-usage periods
- Assign "strong" passwords to APs
- Don't broadcast Service Set Identifiers (SSIDs)
- Don't use default SSID names
- Reduce propagation of radio waves outside the facility
- Deploy access controllers
- Implement personal firewalls
- Utilize IPSec (IP Security Protocol) based Virtual Private Network (VPN) technology on client devices
- Utilize static IP addresses for clients and APs
- Monitor for rogue APs
- Control the deployment of WLANs

These security policy issues should of course be updated to reflect recent evolution of WLAN security standards, such as the adoptions of the WPA and the IEEE 802.11i standards.

WLAN SECURITY STANDARDS

WLAN standards are introduced by four major standardization organizations: IEEE (IEEE Standards, 2007), Wi-Fi Alliance (Wi-Fi Alliance Portal, 2007), IETF (IETF Portal, 2007), and 3GPP (3GPP Portal, 2007). Most of the standards are issued by IEEE. Wi-Fi Alliance handles the practical implementation of these standards through interoperability testing and certification. IETF is engaged in the evolution of Internet architecture. The primary standards development community for Wi-Fi roaming in the 3G mobile cellular networking (UMTS/GPRS/GSM) context is 3GPP (3rd Generation Partnership Project).

Major WLAN security standards are:

- IEEE 802.11/WEP
- WPA (based on Draft 3 of IEEE 802.11i)
- IEEE 802.11i (WPA2)
- 3GPP TS 33.234 (3G security; Wireless Local Area Network (WLAN) internetworking security)

The security in IEEE 802.11 is weak, due to the lack of user authentication mechanisms and the data encryption mechanism WEP uses static encryption keys with the RC4 algorithm (Potter & Fleck, 2003).

Wi-Fi Protected Access (WPA), introduced at the end of 2002, was intended to address the WEP vulnerabilities. WPA is based on Draft 3 of IEEE 802.11i to satisfy a part of the requirements of the full IEEE 802.11i standard (see Figure 1).

The main features of WPA are:

- The Temporal Key Integrity Protocol (TKIP) to provide dynamical and automatically changed encryption keys; and
- IEEE 802.1X in conjunction with the Extended Authentication Protocol (EAP) to provide a framework for strong user authentication.

In order to patch the many vulnerabilities of WEP, the TKIP protocol is used for secure encapsulation of frames in legacy 802.11 devices. A per media access control data unit (MSDU) fresh key generation scheme for proper use of RC4, a longer IV, the integrity protection scheme Michael and a counter-based replay protection mechanism are used. Michael is a lightweight integrity algorithm for the purpose of providing integrity protection to TKIP traffic (Hardjono & Dondeti, 2005).

The full IEEE 802.11i security standard (also known as WPA2) was ratified by IEEE in June, 2004. WPA2 uses the Advanced Encryption Standard (AES) and the encapsulation protocol CCMP to provide an even stronger data encryption mechanism than TKIP. WPA2 also supports fast roaming and independent basic service set (IBSS) (Edney & Arbaugh, 2003).

Wi-Fi hotspots interworking with the rest of the 3GPP architecture include, among others, the following concepts from the GSM world (Hardjono & Dondeti, 2005):

Figure 1. A comparison between WPA and 802.11i