WLAN Security Management

Göran Pulkkis
Arcada Polytechnic, Finland

Kaj J. Grahn
Arcada Polytechnic, Finland

Jonny Karlsson
Arcada Polytechnic, 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).

WLAN security thus requires 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 quickly 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 NIC (network interface card) and AP (access point) firmware is up to date
- Ensure only authorized people can reset the APs
- Properly install all APs
- Disable APs during nonusage periods
- Assign “strong” passwords to APs
- Do not broadcast service-set identifiers (SSIDs)
- Do not use default SSID names
- Reduce propagation of radio waves outside the facility
- Deploy access controllers
- Implement personal firewalls
- Utilize Internet Protocol Security (IPSec) based virtual private network (VPN) technology on client devices
- Utilize static Internet Protocol (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 (Wi-Fi protected access) and the IEEE (Institute of Electrical and Electronics Engineers) 802.11i standards.

WLAN SECURITY STANDARDS

WLAN standards are introduced by three major standardization organizations: IEEE (IEEE Standards, 2003), Wi-Fi Alliance (Wi-Fi Alliance Portal, 2003), and IETF (Internet Engineering Task Force; IETF Portal, 2003). 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.

Major WLAN security standards:

- IEEE 802.11/WEP
- WPA (based on Draft 3 of IEEE 802.11i)
- IEEE 802.11i (WPA2)

The security in IEEE 802.11 is weak due to the lack of user-authentication mechanisms, and the data-encryption mechanism WEP is a weak implementation of the RC4 (Ron's Code #4) algorithm using static encryption keys (Potter & Fleck, 2003).

WPA, introduced at the end of 2002, was intended to address the WEP vulnerabilities. WPA is based on Draft 3 of IEEE 802.11i (also known as WPA2) to satisfy 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 dynamic and automatically changed encryption keys

Figure 1. A comparison between WPA and 802.11i

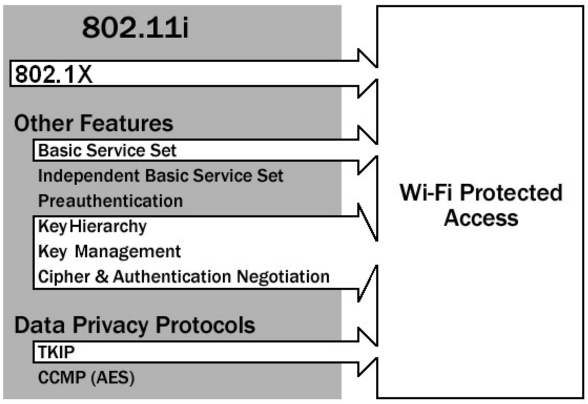
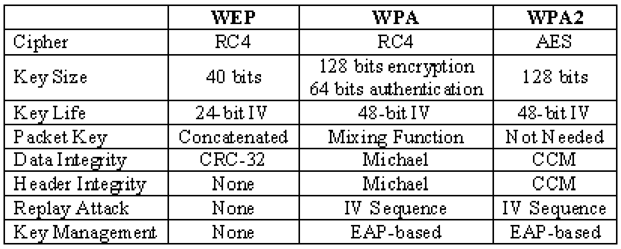


Table 1. Comparison between WEP, WPA, and WPA2



	WEP	WPA	WPA2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24-bit IV	48-bit IV	48-bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC-32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-based	EAP-based

- IEEE 802.1X in conjunction with the extended authentication protocol (EAP) to provide a framework for strong user authentication

The full IEEE 802.11i security standard was ratified by IEEE in June 2004. WPA2 uses the advanced encryption standard (AES) and the encapsulation protocol Cipher-Block Chaining Message Authentication Code Protocol (CCMP) to provide an even stronger data-encryption mechanism than TKIP. WPA2 also supports fast roaming and IBSS (independent basic service set; Edney & Arbaugh, 2003).

A brief comparison between WEP, WPA, and WPA2 is given in Table 1. IV is Initialization Vector, CRC-32 is 32 bit Cyclic Redundancy Check, and CCM is Cipher-Block Chaining Message Authentication Code.

ACCESS MANAGEMENT

Based on IEEE 802.11 Standards

The IEEE 802.11 standard defines open-system and shared-key authentication. SSID and media-access control (MAC) authentication are also commonly used (Potter & Fleck, 2003).

Open-system authentication allows any client to authenticate to a WLAN as long as it passes through a possible MAC address filter. This authentication mechanism is very vulnerable since all authentication packets, including MAC addresses, are transmitted without encryption and MAC addresses are easily "spoofed."

SSIDs are normally broadcasted by WLAN APs. This means that intruders can easily access open-