December 2002

WIRELESS SECURITY: AN OVERVIEW

Robert Boncella
Washburn University

WIRELESS SECURITY: AN OVERVIEW

Robert J. Boncella
Washburn University
zzbonc@washburn.edu

Abstract

Wireless communication is different than wired communication. These differences affect how a secure channel can be established in a wireless environment. The purpose of this tutorial is to provide an overview of how a secure channel can be set up in a wireless environment.

Keywords: WLAN Security, WTLS, WAP, WEP, 802.11b

Introduction

Wireless and mobile networks are rapidly extending their capabilities. In addition to their increasing bandwidth and the because of their flexibility and freedom they are becoming the communication infrastructure of choice. Wireless communication provides a user the capability of conducting commerce at anytime, with nearly anyone, *from anywhere*, using a *mobile* communication channel. This mobile communication channel can be used as an access method the Internet.

As wireless communication and the Internet become truly interoperable a user will desire that this communication channel is secure and available when needed. For a message sent using this communication channel, the user expects assurance of:

- *authentication* (the sender and receiver are who they say they are);
- *confidentiality* (the message cannot be understood except by the receiver); and
- *integrity* (the message has not been altered).

The goal of this tutorial is to provide an overview of what is required to provide a secure communication channel in a wireless environment. The focus will be the security techniques available for Wireless Local Area Networks (WLAN) and when wireless devices are used to access the Internet.

The tutorial is organized as follows. Section 1 summarizes WLAN security specified in the 802.11 standard. Section 2 summarizes the security problems and solutions when small, low-powered devices try to use low-bandwidth wireless network technology to access services or data-intensive content via the Internet. In particular Section 2 summarizes the WAP protocol and its security features.

WLAN Security Requirements

This section discusses the access control methods and channel security of the 802.11 architecture. These techniques are best suited for home users, small networks, or networks with low security requirements. In addition, this sections presents a VPN (Virtual Private Network)-based security solution which provides better security and is suitable for large networks.

With the deployment of wireless networks in business environments, organizations are working to implement security mechanisms that are equivalent to those of wire-based LANs. An additional component of this security requirement is the need to restrict access to the wireless network to valid users. Physical access to the WLAN is different than access to a wired LAN. Existing wired network have access points, typically RJ45 connectors, located inside buildings which may be secured from unauthorized

access through the use of such devices as keys and badge access. A user must gain physical access to the building in order to plug a client computer into a network jack.

A wireless access point (AP) may be accessed from off the premises if the signal is detectable. Hence wireless networks require secure access to the AP in a manner different from wired LANs. In particular it is necessary to isolate the AP from the internal network until authentication is verified. The device attempting to connect to the AP must be authenticated. Once the device is authenticated then the user of the device can be authenticated. At this point the user may desire a secure channel for communication.

The 802.11 standard provides the means to satisfy these two security requirements - validation of the access device and a secure channel
.

Basic 802.11 Security

The three basic methods to secure access to an AP that are built into 802.11 networks are:

- Service Set Identifier (SSID)
- Media Access Control (MAC) address filtering
- Wired Equivalent Privacy (WEP)

One or all of these methods may be implemented, but all three together provide the best solution.

SSID

Control of network access can be gained by using an SSID associated with an AP or group of APs. The SSID is a mechanism to that can segment a wireless network into multiple networks serviced by one or more APs. Each AP is programmed with an SSID that corresponds to a specific wireless network. This configuration is similar to the concept of a network address used in wired LANs. To be able to access a particular wireless network the client computer must be configured with the appropriate SSID. A WLAN might be segmented into multiple WLAN based floor or department. A client computer can be configured with multiple SSIDs for users who require access to the network from a variety of different locations.

A client computer must present the correct SSID to access the AP. The SSID acts as a password and provides a measure of security. This minimal security can be compromised if the AP is configured to “broadcast” its SSID. If this broadcast feature is enabled any client computer that is not configured with an SSID will receive the SSID and then be able to access the AP. Most often, users configure their own client systems with the appropriate SSIDs. As a result these SSIDs are widely known and easily shared.

SSID provides a method to control access to an AP or set of APs . An additional technique that enhances this method is MAC (Media Access Control) Address Filtering.

MAC Address Filtering

A client computer can be identified by the unique MAC address of its 802.11 network card. To enhance AP access control each AP can be programmed with a list of MAC addresses associated with the client computers allowed to access the AP. If a client's MAC address is not included in this list and the SSID provided by the client does not match the AP's SSID the client is not allowed to access the AP.

This arrangement provides improved security that is best suited to small networks where the MAC address list can be managed efficiently. The management requires that each AP must be programmed manually with a list of MAC addresses. In addition this list must be kept up-to-date. Clearly this overhead will limit the size of the WLAN in number of APs and clients devices.

SSID and MAC Address Filtering satisfy the first of the two requirements of WLAN Security. The second requirement - channel security - is provided by WEP (Wired Equivalent Privacy)

WEP Security

Wireless transmissions are easier to intercept than transmissions in wired networks. In most cases users of WLANs desire secure transmissions. The 802.11 standard specifies the WEP security protocol to provide encrypted communication between the client and an AP. WEP employs the RC4 symmetric key encryption algorithm.

When using WEP, all clients and APs on a wireless network use the same key to encrypt and decrypt data. The key resides in the client computer and in each AP on the network. Since the 802.11 standard does not specify a key management protocol. Hence all WEP symmetric keys on a network will be managed manually. Support for WEP is standard on most current 802.11 cards and APs. However WEP security is not available in ad hoc (or peer-to-peer) 802.11 networks that do not use APs.

WEP specifies the use of a 40-bit encryption key and there are also implementations of 104-bit keys. The encryption key is concatenated with a 24-bit "initialization vector," resulting in a 64- or 128-bit key. This key is input into a pseudorandom number generator. The resulting sequence is used to encrypt the data to be transmitted. The shared key can be used for client authentication as well by a four step process between the AP and the client. This process is as follows:

1. the client make an authentication request to the AP;
2. the AP returns a challenge phrase to the client;
3. the client encrypts the challenge phrase using the shared symmetric key and transmits it to the AP;
4. the AP then compares the client's response with its phrase; if there is a match, the client is authorized otherwise the client is rejected.

WEP encryption is vulnerable to attack (See http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html). As a result, scripting tools exist that can be used to take advantage of weaknesses in the WEP key algorithm to successfully attack a network and discover the WEP key (see http://sourceforge.net/projects/wepcrack). Currently the industry and IEEE are working on solutions to this problem. The Advanced Encryption Standard (AES) has been identified as a possible replacement encryption technology for WEP. In addition, revised 802.11 standards (802.11i.and 802.1x) may be adopted which address the security weaknesses of the current standard (Kapp 2002) .

Despite the weaknesses of WEP-based security it can be a component of the security solution used in home networks and in small but managed networks with low security requirements. Nonetheless with these networks, 128-bit WEP should be implemented in conjunction with MAC address filtering and SSID. In addition some sort of WEP symmetric key management should be employed. For example users should change their WEP keys on a regular schedule to minimize risk of compromise.

If a network has high security requirements, or will allow many clients, an alternative to the SSID/MAC Address Filtering/WEP protocol is a VPN (Virtual Private Network) solution. VPNs are a mature technology that allow a client to use an "untrusted" network (e.g. the Internet or a wireless network) for secure communication. Briefly this solution requires both:

- a VPN server installed on the network being access by the wireless client and
- the wireless client having the VPN client software installed .

WAP Protocol 1.x

WAP was designed to solve some of the problems caused when small, low-powered devices try to use low-bandwidth wireless network technology to access services or data-intensive content via the Internet. In particular, users want to be able to access e-mail, trade stocks, find out the latest sports scores, or the most recent news event via a cell phone in a secure fashion.

The WAP protocol stack is made up of five layers. These are:

- Application
- Session
- Transaction
- Security
- Transport

The functional requirements of each layer are specified below.

Wireless Application Environment (WAE)

The WAE layer provides an environment to develop and execute applications. In addition it provides services for wireless devices. The WAE layer's primary elements are WML (Wireless Markup Language), a microbrowser, Push technology to push data proactively to clients, and multimedia messaging capability.

Wireless Session Protocol (WSP)

WSP manages the exchange of content. WSP provides applications with a consistent interface for both connection-oriented and connectionless session services. WSP lets client and server applications establish and terminate reliable sessions and agree on common protocols with which to work. WSP also includes extensions that facilitate wireless transmissions. For example, WSP's compact binary headers reduce the overhead and number of transactions necessary to support session services.

Wireless Transaction Protocol (WTP)

WTP manages transactions by facilitating requests and responses between a user agent (such as a WAP microbrowser) and an application server for such activities as browsing and e-commerce transactions. WTP works well in the low-bandwidth wireless environment because it requires the wireless device and the gateway to send each other relatively few packets to manage or maintain the connection. WTP can provide data streaming, hypermedia, and message transfer.

Wireless Transport Layer Security (WTLS)

WTLS secures, authenticates, and encrypts data transmissions between the WAP gateway and mobile devices. To support mobile networks, WTLS was designed to be more efficient than SSL, which requires client and server to exchange many messages. In wireless networks, which frequently experience considerable latency, this requirement can slow response time significantly. WAP systems translate WTLS data to SSL data for transmission over the Internet within the WAP gateway.

Wireless Datagram Protocol (WDP)

WDP lets WAP support many network technologies. WAP works with the major wireless network technologies used in different parts of the world, including CDMA (code-division multiple access), GSM (global system for mobile communication), and TDMA (time-division multiple access). WAP also supports the major operating systems used in handheld devices (e.g. JavaOS, PalmOS, and Windows CE). When working with IP bearer services, WDP functions just like the User Datagram Protocol. With non-IP bearer services, such as CDMA, WDP performs the adaptation necessary to carry transmissions.

WAP and Internet Access

WAP uses proxy technology to connect wireless technology with the Web. The WAP proxy server consists of a gateway, encoders, and decoders. The gateway translates requests from the WAP protocol stack to the WWW stack so they can be submitted to Web servers. Encoders and decoders translate WAP content into compact encoded formats that reduce the amount of data being sent over the low-bandwidth wireless network. Wireless technology's bandwidth and latency constraints cannot support the Internet standards of HTML, HTTP, IP, TCP, and TLS (transport layer security). These are inefficient over mobile networks. For example, HTTP sends its headers in text format, instead of compressed binary format. Meanwhile, to work with HTTP and HTML, machines must have fast network connections, powerful processors, and large memories, components not currently found in handheld devices.

WAP 1.x Security

The layer of the WAP protocol that provides security is the WTLS layer. WTLS functions similar to SSL (also known as Transport Layer Security (TLS)). WTLS provides for server and/or client authentication via certificates similar to X.509

certificates. WTLS also allows for the negotiation of encryption parameters between the client and server, thus ensuring a secure channel for communication. Although WTLS does not provide end-to-end security, the chances of a problem are small because hackers can breach security only when sensitive data passes through the WAP gateway. WTLS provides the security necessary to conduct e-commerce on handheld wireless devices.

WAP Protocol 2.0

In January, 2002 the WAP Forum released version 2.0 of the Wireless Application Protocol - http://www.wapforum.org/what/WAPWhite_Paper1.pdf.

WAP 2.0 extends bearer services to include GPRS (General Packet Radio Service) and 3G (3rd Generation) cellar thus providing access to higher bandwidth and speeds. Because of providing these extend services WAP 2.0 contains support for the standard Internet protocols of IP, TCP and HTTP.

To interoperate with these Internet Protocols, the WAP 2.0 Protocol stack contains:

1. WP-HTTP (Wireless Profiled HTTP) - A profile of HTTP for wireless environment that is interoperable with HTTP/1.1;

2. TLS (Transport Layer Security) - a profile of the TLS protocol that will allow for secure transactions. And provide for end-to-end security at the transport layer. This is similar to what wire users expect with the SSL layer; and

3. WP-TCP (Wireless Profiled TCP) WP-TCP will provide connection-oriented services.

The WAP 2.0 enabled device now contains the following layers:

- WAE Layer
- WP-HTTP
- TLS
- P-TCP
- IP
- Wireless

As a result, a WAP 2.0-enabled device will be able to interact efficiently with a wired web server through a WAP Proxy which only contains only the wireless to wired, IP to IP, TCP to TCP layers.

Finally, to remain backward compatible with existing WAP 1.x applications, newer WAP devices will support both stacks (WAP 1.x and WAP 2.x) independently. As a result the WAE layer will be accessible to both stacks.

WAP 2.0 Security

Since WAP 2.0 includes a version of TLS (Transport Layer Security) in its WAP Device stack, version 2.0 security is improved over version 1.x. In particular the WAP proxy no longer has to translate the WTLS protocol into the TLS protocol when sending data to a wired web server and visa versa. Overall WAP 2.0 provides better end-to-end security.

References

Dornan, A. "LANs with No Wires, but Strings Still Attached", *Network Magazine*, (17:2), 2002, pp. 44-47.
Dornan, A. "Fast Forward to 4G?", *Network Magazine*, (17:3), 2002, pp. 34-39.
Fratto, M. "Tutorial: Wireless Security", *Network Computing*, January. 22, 2001, http://www.networkcomputing.com/1202/1202f1d1.html.
Garber, L. "Will 3G Really Be the Next Big Wireless Technology?" *IEEE Computer*, (35:1), 2002, pp.26-32.
Kapp, S. "802.11: Leaving the Wire Behind", *IEEE Internet Computing Online*, January/February, 2002, http://www.computer.org/internet/v6n1/w102wire2.htm.

Internet Security Systems. "Wireless LAN Security: 802.11b and Corporate Networks", 2001, http://www.iss.net/support/documentation/otherwhitepapers.php.

Macphee, Allan "Understanding Digital Certificates and Wireless Transport Layer Security (WTLS)", *Entrust Whitepaper*, 2001 http://www.entrust.com/resources/whitepapers.htm.

Nichols, R. K., and Lekkas, P. C., *Wireless Security: Models, Threats, and Solutions*, New York, NY: McGraw-Hill, 2002.

Varshney, U. and Vetter, R. "Emerging Mobile and Wireless Networks", *Communications of the ACM*, (43:6), 2000, pp. 73-81.

WAP Forum., "Wireless Application Protocol WAP 2.0", *WAP Forum Technical White Paper*, 2000, http://www.wapforum.org/what/WAPWhite_Paper1.pdf.