Wireless LAN Security Mechanisms

Jingan Xu, Andreas Mitschele-Thiel

Technical University of Ilmenau, Integrated Hard- and Software Systems Group
jingan.xu@tu-ilmenau.de, mitsch@tu-ilmenau.de

Abstract. The security of Wireless Local Area Networks (WLANs) is an important topic especially in corporate networks. This article provides an analysis of a variety of security technologies for WLANs, including WEP, RADIUS, VPN and 802.1x. Based on the analysis we provide proposals for the security settings in WLANs.

1 Introduction

Local Area Networks have been used for interconnecting computers and resources in various networks for a long time. Cables have typically been chosen for the physical medium in most environments. But recently, wireless connections play a more important role in Local Area Networks. They provide flexible network connection, and do not require the computers being bound to the desk. On the other hand, because WLANs use electromagnetic waves to transmit information, the radio waves can easily penetrate outside the building, it's a risk that the network can be hacked from the parking lot or the street. So it's very important to put enough attention on the WLAN's security aspects.

2 IEEE 802.11b WLAN

There are many different wireless access techniques, which lead to various WLAN standards. IEEE 802.11b is the most popular standard in nowadays WLAN market. This standard specifies multiple channels in the Industrial, Scientific and Medical (IMS) frequency range of 2.4GHz. Theoretical transport data rates are up to 11 megabits per second, depending on the SNR. The transmission range is about 100 meters outdoor and 30 meters indoor.

To set up a WLAN, we need a base station called "Access Point", and some wireless adaptor cards for the client stations. The access point will forward data from one wireless client station to another within the same WLAN, which is identified by an Extended Service Set Identification (ESSID). When two or more access points connected to a wired backbone use the same ESSID, they form a "Multiple Access Point Network". Client stations can roam inside this network and automatically change its operating channel as required when roaming.

Fig. 1 is one of the network architectures for a "Multiple Access Point Network".

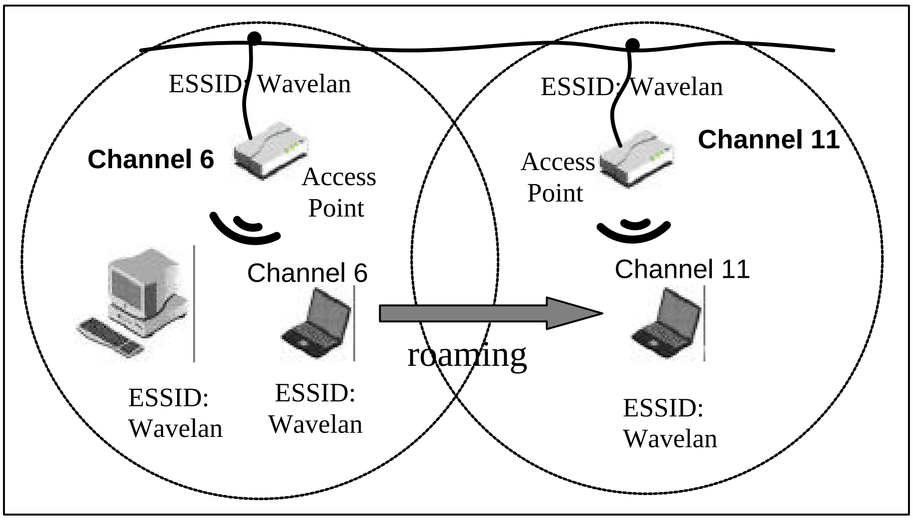


Fig. 1. WLAN network architecture

3 Security Mechanisms for WLAN

In general, the security mechanisms for WLANs can be divided into two different kinds: the first kind of mechanisms are provided by the access point. We can call them basic security mechanisms. The second kind needs an additional server to provide security services. We call them Supplemental Security Mechanisms.

3.1 Basic Security Mechanisms

In a WLAN, the access point can provide three basic security mechanisms: closed network, MAC address filtering and Wired Equivalent Privacy (WEP).

First, in a closed network, the access point will only serve those clients who provide the same ESSID as the access point. Second, every wireless client has a unique MAC address, so that the access point can set up a list of MAC addresses. Only the wireless client with the card on that list will be allowed to access the network.

The third security mechanism is specific for the WLAN transport medium. The IEEE 802.11 standard provides a protocol to make sure the transport data is "*as secure as it is inside the cable*". This is called "Wired Equivalent Privacy" –(WEP). Data will be encrypted by this mechanism during the transfer.

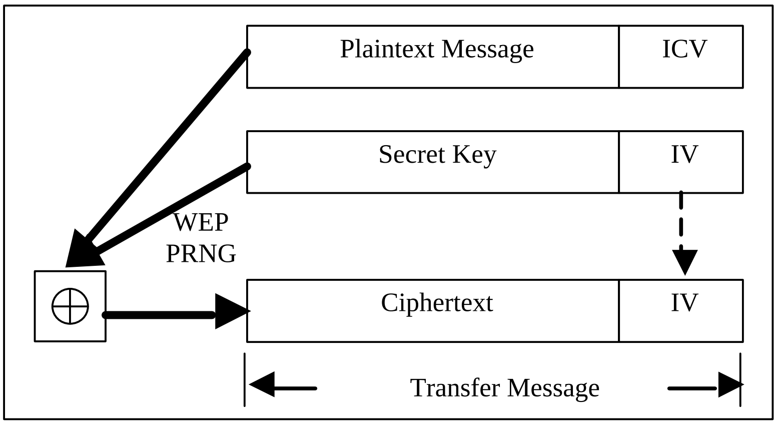


Fig. 2. WEP encryption

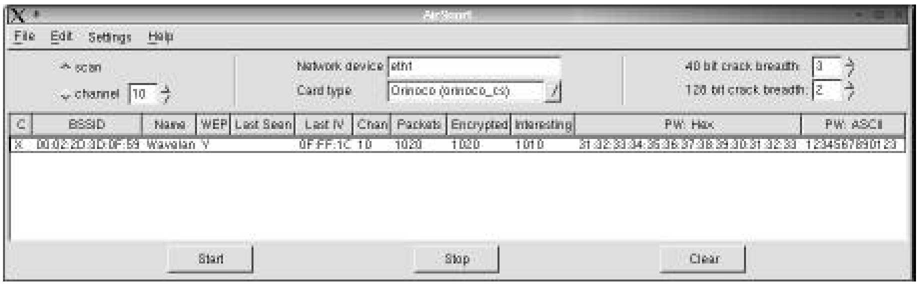
Fig. 2 outlines the WEP algorithm. The steps of WEP encryption are as follows:

a) Use CRC-32 to calculate the Integrity Check Value (ICV) over the plaintext and concatenate it at the end of the text.
b) The wireless network card chooses a random initialization vector (IV) and concatenates it to the secret key. Input the secret key and the IV into the Pseudo Random Number Generator (PRNG) to produce a pseudo random key sequence. WEP uses the RC4 algorithm to generate this key sequence.
c) Encrypt the plaintext and the ICV employing a bitwise XOR with the pseudo random key sequence to produce the cipher text.
d) Concatenate the initialization vector and the ciphertext to form the message to be transfered.

In decryption, the receiver gets the IV from the incoming message, and applies its secret key to generate a pseudorandom key sequence. Then it applies a bitwise XOR to the Ciphertex, which yields the original plaintext and the ICV. The decryption is verified by performing the integrity check algorithm on the recovered plaintext and comparing the output ICV' to the ICV received with the message. If ICV' is not equal to ICV means that there must be an error in the received message. This results in the packet being dropped.

WEP use the RC4 algorithm to generate pseudo random numbers. Unfortunately, RC4 is vulnerable to analytic attacks. Notice that the IVs are transmit as plain text in the message. Thus, weak IVs result in cases where one or more generated bytes are strongly correlated with the secret key bytes. Most of these weak IVs have the form of (KeyByte+3, 0xFF, N), in which KeyByte is the current key byte being cracking, and N is unrestricted. Each of these weak IVs with probability of more than 5% can correctly reveal a corresponding secret key byte. When a certain number of packets with weak IVs are monitored, the secret key will be cracked out by statistic analysis.

Fig. 3 shows a test result using Airsnort – a WEP cracking tool which can be downloaded from the Internet for free – to crack out WEP keys. The field channel shows which the Access Point was using, BSSID indicated the Access Point’s MAC address, Name indicated the network ID, PW:Hex and PW:ASCII show the password in Hex format and ASCII format.



scan
channel 10

Network device eth1
Card type Orinoco (orinoco_cs)

40 bit crack breadth: 3
128 bit crack breadth: 2

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	PW: Hex	PW: ASCII
X	00:02:2D:3D:0F:59	Wavelan	Y		0F:FF:1C	10	1020	1020	1010	31:32:33:34:35:36:37:38:39:30:31:32:33	1234567890123

Fig. 3. WEP cracked by using Airsnort

Closed networks and WEP can be cracked, MAC address can also be spoofed. All these means the basic security is not secure enough and advanced security mechanisms are necessary.

3.2 Supplemental Security Mechanisms

Remote Authentication Dial-In User Service (RADIUS), Virtual Private Network (VPN) and IEEE 802.1x, the port-based network access control mechanism are the most common and recommended supplemental security mechanisms for WLANs. RADIUS is designed to provide user-based authentication, but many access points support only MAC address authentication on the RADIUS server. Although still insecure when facing MAC address spoof, RADIUS enables the access point to serve more wireless clients with the MAC address filtering, while access points only support 32 MAC addresses.

The VPN technology depends on data encryption to make sure they are secure during the transfer. The client and the server employ mutual authentication. After that, data will be encrypted and transferred over the network as in a virtual tunnel between the sender and the receiver.

Fig. 4 outlines the VPN network architecture, and Fig. 5 describes the mutual authentication steps.

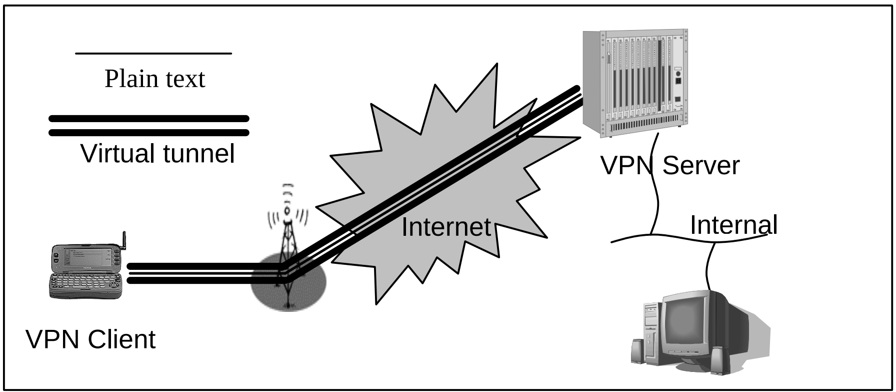


Fig. 4. VPN architecture in mobile communication network

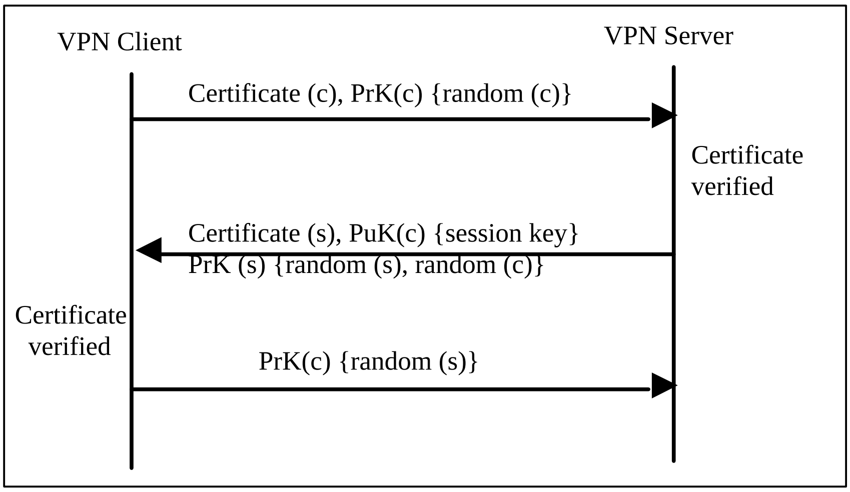

VPN Client
VPN Server
Certificate (c), PrK(c) {random (c)}
Certificate verified
Certificate (s), PuK(c) {session key}
PrK (s) {random (s), random (c)}
Certificate verified
PrK(c) {random (s)}

Fig.5. Mutual authentication

The steps for mutual authentication are as follows:

a) The VPN client sends its certificate and a random number (encrypted with its private key) to the VPN server. The server verifies the integrity of the received certificate using its Certificate Authority (CA) public key. This verification also involves checks whether the certificate is on a revocation list, the validation range is acceptable and whether it concerns a certificate of other trusted CAs.

b) When all of the above is fine, the server decrypts the encrypted random number by using the client's public key and encrypts it with its own secret key. It also encrypts a randomly generated session key using the public key in the client's certificate and sends these two data blocks as well as a challenge back to the client.

c) The VPN client decrypts the session key with its own private key, and then checks the validity of the server's certificate and decrypts the answered random number using the server's public key. Since the server's certificate is valid and the challenge sent from the client to the server has been returned encrypted with the server's secret key, the client can be sure, that the server is in the possession of the secret key belonging to the server's certificate and since the CA has signed the connection between this key and the server's user ID, the client can be sure that this partner is the really server it's looking for. If mutual authentication is required, the client sends back the challenge of the server encrypted with its own secret key. And the server will confirm the client's identity.

In the following communication, the sender always send data encrypted with the receiver's secret key, which can be decrypted only by the receiver. Thus, a secure virtual tunnel is set up.

IEEE 802.1X is an IEEE standard that enables authentication and key management for IEEE 802 Local Area Networks, including Ethernet, Token Ring, FDDI, and WLAN.

This port-based network access control has the effect of creating two distinct kinds of points to access the authenticator system. Before authentication, the supplicant can only access the uncontrolled ports of the authenticator so that it can apply for authentication. All other controlled ports will be disabled until the authentication succeeds.

802.1x provides protection against client-to-client attacks, which VPN can not provide. In addition, it needs the support of the access point. Till now only a part of the access point can support 802.1x. But it's no doubt that most access points may be upgraded in the future by firmware to support 802.1x.

4 Security Solution for WLAN

The security methods discussed in this paper can be implemented independently or in certain combinations to provide a much higher security level for the WLAN.

a) In a short term, i.e. while 802.1x is not fully supported by all access points of the local WLAN, a useful security policy for WLAN can be like:

Closed Network + WEP + Firewall + RADIUS MAC Address Filter

This model can fully provide the advantage of the WLAN as well as prevent the normal unauthenticated access to the WLAN. However, it can not prevent the intended attack.

In the mean while, all sensitive data should be kept behind the VPN server and transfer inside the VPN tunnel. The suggest model to use is:

Closed Network + WEP + Firewall + RADIUS MAC Address Filter + VPN

Using VPN, the attacker may crack WEP encryption and the MAC address filter. However, he can only access the WLAN, but will not be able to access the sensitive data in the corporate network. The sensitive data encrypted in the VPN tunnel are safe enough during the transfer in the WLAN.

b) In a long term, i.e. when all access points support 802.1x, we can use the following security policy:

Closed Network + WEP + Firewall + IEEE 802.1x or

Closed Network + WEP + Firewall + IEEE 802.1x + VPN

Here we can use 802.1x to replace the RADIUS service since the access points can provide either RADIUS or 802.1x function. The VPN here only acts as a supplementary protection mechanism for the sensitive data.

5 Conclusion

For all security mechanisms that were studied, VPN provides point-to-point security. However, it can neither protect multicast communication nor prevent client-to-client attacks. 802.1x is new and still not fully supported by all operation systems and wireless equipments. According to the security policy, base on the need of different users, different security mechanisms should be combined.

6 Reference

Books:

Certified Wireless Network Administrator™ (CWNA™) Study Guide
by Planet3 Wireless
Publisher: McGraw-Hill; 2nd edition (February 18, 2003)

Wireless Security: Models, Threats, and Solutions
by Randall k. Nichols, Panos C. Lekkas
Publisher: McGraw-Hill; 1st edition(December 13, 2001)

Websites:

[1] The IEEE 802.11 Wireless LAN Standard
http://standards.ieee.org/getieee802/download/802.11-1999.pdf

[2] The Wireless LAN Association
http://www.wlana.org/learn/security.htm

[3] The Wi-Fi Alliance
http://www.wi-fi.org

[4] Unofficial 802.11 security web page
http://www.drizzle.com/~aboba/IEEE/

[5] Homepage of AirSnort
http://airsnort.shmoo.com/

[6] Remote Authentication Dial In User Service (RADIUS) (memo)
http://www.ietf.org/rfc/rfc2865.txt

[7] RADIUS Accounting (memo)
http://www.ietf.org/rfc/rfc2866.txt

[8] Homepage of FreeRadius
http://www.freeradius.org/

[9] Homepage of FreeS/WAN
http://www.freeswan.org/

[10] Virtual Private Network Consortium
http://www.vpnc.org/

[11] 802.1x Standard.pdf
http://www.vayner.net/Docs/802.1/802.1X-2001.pdf