Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Security Mechanism for IEEE 802.11 Wireless Networks

This paper provides an introduction to Wireless Local Area Networks (WLAN), and the methods employed to secure access using the IEEE 802.11 architecture. The vulnerability of IEEE 802.11 technology is disconcerting, although effective security mechanism can be implemented to secure a wireless network. In the future wireless connections will befall a standard on laptops, PDA's and other wireless devices so we need to secure all client and access points to mitigate threats.

Copyright SANS Institute
Author Retains Full Rights

AD

The Security Mechanism for IEEE 802.11 Wireless Networks

Alicia Laing
November 24, 2001
Version 1.2f

Introduction:

This paper explains the introduction to Wireless Local Area Networks (WLAN), and the methods employed to secure access using the IEEE 802.11 architecture.

Overview:

What is Wireless Local Area Network (WLAN) technology? Wireless Networks is a data communication system that uses shared radio waves or infrared light to transmit and receive data without wired cables. Wireless LAN gives great flexibility and freedom to connect to the network or Internet without being physically connected with a cable or modem. With the added functionality of a wireless network, you can replace or extend a wired infrastructure. Data is transmitted or received via air, walls, ceilings, and even cement structures throughout or between buildings. With the absence of wires, wireless networks reduce the network deployment cost and alleviate some hard-wired problems. "Access to the internet and even corporate sites could be made available through public wireless "hot spots"." [1] Traveling to various places where there is a wireless network can provide the user with access to the Internet by using that location's access point.

The Institute of Electrical and Electronics Engineers (IEEE) created the 802.11 standard for wireless LANs to ensure product compatibility and reliability. Wireless LAN's operate at high speeds access, and provide 2.4 GHz band, and data rates up to 11 Mbps. The IEEE 802.11 standard has evolved in the world of Wireless LANs. The 802.11 standard focuses on the bottom two levels of the ISO/OSI model, the physical layer and data link layer. [2] "The 802.11b specification affects only the physical layer, adding higher data rates and more robust connectivity." [4] See figure 1, which depicts the level where 802.11, is located.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

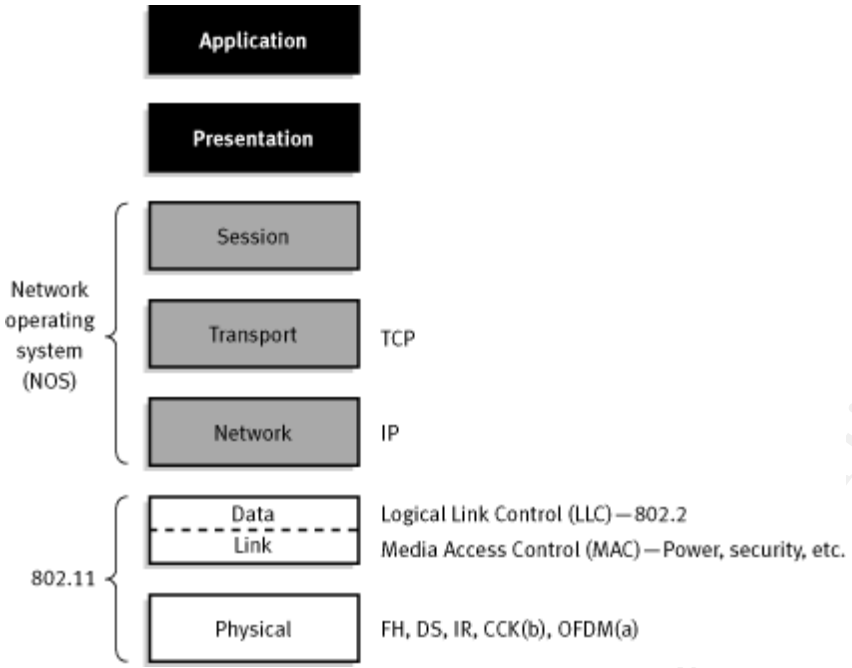

Figure 1

There are two types of transmission that are included in the IEEE 802.11 standard: Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). Spread spectrum enables a stronger signal than a narrowband signal, which is harder for the receiver to detect. Spread spectrum's increased reliability, boost throughput and allows many unrelated products to share the spectrum with minimal interference. FHSS transmission signals hops from one frequency to another at a rate known only to the transmitter and receiver. With DSSS, a redundant "chipping code" is sent with each signal burst and only the transmitter and receiver can decode the chipping sequence. [2] The evolution of the IEEE 802.11b high rate standard, provide for a full Ethernet like data rate of 11 Mbps over DSSS. Because FHSS cannot support such high speeds without violating current FCC regulation, DSSS has become the predominant WLAN standard.

WLANS can be configured using two topological ways: Peer-to-Peer or Adhoc mode and Client/Server or infrastructure networking. Peer-to-Peer topology consists of two or more PC's equipped with wireless network interface cards but with no connection to a wired network. Wireless devices have no access point connection, and each device communicate with each other directly. See figure 2.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

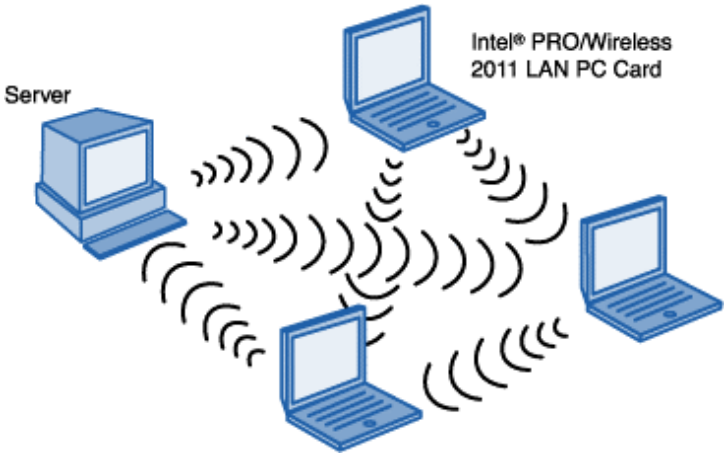

Figure 2

Client/Server wireless technology extends an existing wired LAN to wireless devices by adding an access point. The access point is a bridge between a wired LAN and a wireless LAN and is the central controller for the wireless network. Through an Ethernet cable that is connected to a wired backbone, antenna's mounted on the access point allows devices to communicate with each other. Multiple PC's link to the access point that acts as a bridge to the resources that connects to the wired network. All network traffic from the wireless stations on the network goes through an access point to reach it's destination in either a wired or a wireless LAN or WAN.
See figure 3.

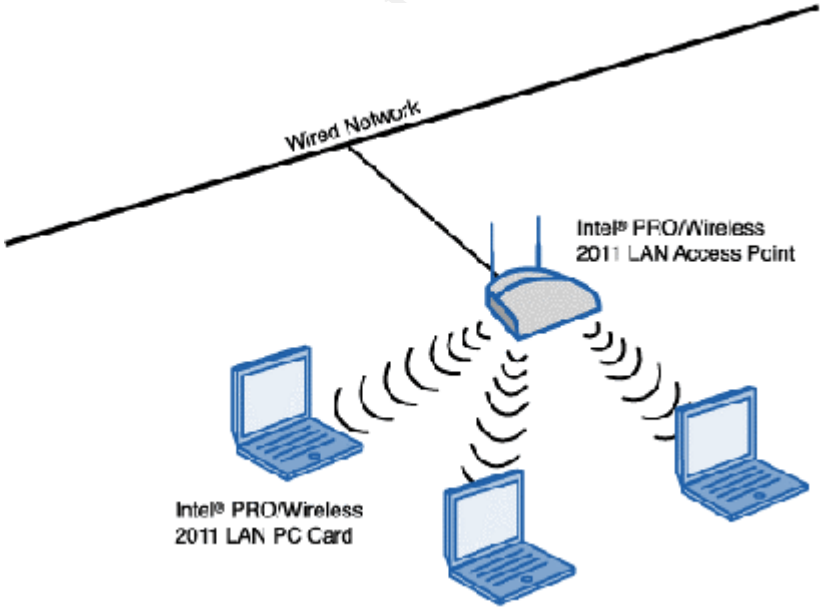

Figure 3

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Wireless LAN Obstacles

As the popularity of wireless LAN increases, security, roaming and configuration has become a great challenge. Data can be subject to eaves dropping via radio frequency if its not encrypted. Similar to a wired network, wireless networks must have reliability and security features when connecting to a wired LAN. Wireless traffic is transmitted in the clear over a shared medium. Since the data is traveling through the air or radio waves, the network is now accessible both inside and, outside of the building. The proper security procedures must be implemented to prevent potential data theft.

The basic methods to secure access to an Access Point that is built on IEEE 802.11 networks are:

- Configure IEEE 802.11 access points with a service set identifier (SSID)
- Wired Equivalent Privacy (WEP) algorithm
- MAC Address filtering
- Setup Virtual Private Networking (VPN) across radio frequency LAN

Deploying all four of these access control methods provide a more robust solution for the IEEE 802.11 architecture.

SSID

SSID is an identification value programmed in the access point or group of access points to identify which subnet you exist on. This segmentation of the wireless network in multiple networks is a form of an authentication check. If a wireless station does not know the value, access is denied to the associated access point. When a client computer is connected to the access point, the SSID acts as a simple password thus providing a measure of security.

SSID security alone is very weak because the value is known by all network cards and access points, and is easily accessibly through air and radio waves, since no encryption is provided. The access point is configured to broadcast its SSID. When enabled, any client without SSID is able to receive it and have access to the access point. Users are also able to configure their own client systems with the appropriate SSID, because they are widely known and easily shared. [3]

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

WEP Algorithm

WEP security protocol is intended to protect against eavesdropping and physical security attributes, which is equivalent to security of a wired network. WEP is the encryption standard specified by IEEE802.11 architecture. WEP encrypts a data frame and its content to protect authorized users on a WLAN. WEP uses a 40-bit secret key for authentication and encryption, and other IEEE 802.11 allows 104-bit secret key encryption. "The encryption key is concatenated with a 24-bit "initialization vector," resulting in a 64- or 128- bit key." [3] When encryption is enabled, the access point issues an encrypted challenge packet to any client attempting to connect to the access point. Then the client uses it's key to encrypt the correct response in order to authenticate it-self and gain network access. [4] The client computer and the access point use the same key to encrypt and decrypt data. All WEP key on a wireless LAN must be managed manually, because there are no key management protocols specified for distribution. WEP security protocols can only be implemented on a client/server wireless LAN with an access point, it cannot be utilize on a Peer-to-Peer.

WEP encryption has weaknesses, which are vulnerable to attacks. WEP keys are static for encryption and authentication, making WEP susceptible to password replay attacks, traffic injection, and statistical attacks. Changing the WEP key regularly will reduce the security risk of unwanted visitors. Hackers would exploit the weakness by intercepting traffic, flipping bits and injecting modified packets into the network. Researchers at the University of California Berkeley; discovered security flaws in WEP. These include misapplication of cryptographic primitives, that it permits eavesdropping and tampering with wireless transmission. There are three main security goals of the WEP protocol: confidentiality, access control and data integrity. There analysis is beyond the scope of this paper; access the link to get more detailed information http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf. The researchers argued and proved in a paper that none of these three security goals were achieved. The Advanced encryption standard (AES) might be a replacement encryption for WEP. On a client/server network you need to deploy WEP with SSID for segmentation of the network.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

MAC Address Filtering

Client computers are viewed by a unique MAC address of its IEEE 802.11 network card. To secure an access point using MAC address filtering, each access point must have a list of authorized client MAC address in its access control list. MAC address filtering is time consuming because the list of client MAC address must be manually inputted in each access point. Since the MAC address list must be kept up-to-date it's better suited for a smaller network. In a small network the security solution can be 128-bit WEP in conjunction with MAC address filtering and SSID.

VPN

High security networks must incorporate a VPN solution with a wireless access. VPN solution is an alternative to the three access control as discussed earlier. VPN provides a secure and dedicated channel over an un-trusted network - in cases of the Internet and wireless solutions. With a VPN solution it consists of a VPN server and a VLAN between the access point and the VPN server. The VPN server, which acts as a gateway to the private network, provides authentication and full encryption over the wireless network. IEEE 802.11 wireless access can be established via a secure VPN connection using various tunneling protocols.

VPN is mainly deployed to provide remote users with a secure connection to the network by way of the Internet. VPN is a logical solution for wireless networks because it provides access control where-by no unauthorized routes to the outside Internet exists from the wireless network. This protects the network from unauthorized users using costly Internet bandwidth. Deploying VPN technology on an enterprise network has its advantages of low administration for the client and the access point, and authentication has to be established before traffic to the internal network is acknowledged.

Security Trends For WLAN

In a wireless network an enterprise need to deploy several layers of defense across the network to prevent threats. A good wireless network design should consist of firewalls,

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

intrusion detection systems and segmentation of the network. My proposed solution is to put the access point in it's own DMZ, insuring that everything goes through the firewall. VPN technology should be incorporated from the client straight to the access point. The client computers should be equipped with a personal firewall or an intrusion detection system. The intrusion detection system should be between the access point and the firewall to deny any unauthorized connection. To reduce the unauthorized access to system and other resources, change the administrative password that is preset on the access point, change the default SSID value and disable SSID broadcasting and enable encryption and avoid installing access point near external walls or windows where signals might be intercepted.

Conclusion

The vulnerability of IEEE 802.11 technology is disconcerting, although effective security mechanism can be implemented to secure a wireless network. In the future wireless connections will befall a standard on laptops, PDA's and other wireless devices so we need to secure all client and access point to mitigate threats.

References:

1) Fout, Tom. "Wireless LAN Technologies and Windows XP." July 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/evaluate/wrlsxp.asp
2) Intel Corporation. "IEEE 802.11b High Rate Wireless Local Area Networks." June 2000. URL: http://www.intel.com/network/documents/pdf/wireless_lan.pdf
3) Dell Corporation. "802.11 Wireless Security in Business Networks." September 2001. URL: http://www.dell.com/us/en/biz/topics/vectors_2001-wireless_security.htm
4) 3COM Corporation. " What is 802.11 & 802.11B?" April 2001. URL: http://www.pulsewan.com/data101/802_11_b_basics.htm
5) Borisov, Nikita, Goldberg, Ian, Wagner, David; "Intercepting Mobile Communications: The Insecurity of 802.11." August 2001. URL: http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

6) Meredith, Gail. "Securing the Wireless LAN." July 2001. URL: http://www.cisco.com/warp/public/784/packet/jul01/p74-cover.html
7) Geier, Jim. "Wireless LANs, Second Edition." Indianapolis, Indiana: SAMS, July 2001

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**