Global Information Assurance Certification Paper

Wireless Networking Security:
As part of your Perimeter Defense Strategy

Daniel Owen
GSEC Practical Assignment Version 1.2f
January 23rd, 2002

Table of Contents

Section 1 - Introduction

Wireless LAN technology, as defined by the IEEE (Institute of Electrical and Electronics Engineers) 802.11 standard, has become a key piece in many corporate IT infrastructures. [9] Portable device manufacturers are largely responsible for the fast adoption rate of this immature technology, as they are already providing 802.11 wireless cards as a standard built-in networking device. The portable computing user community is responding to this market trend by adding wireless LAN access onto their physical networks. Once the initial novelty of this exciting new technology wears off, many corporations realize the associated risks of such an uncontrolled medium.

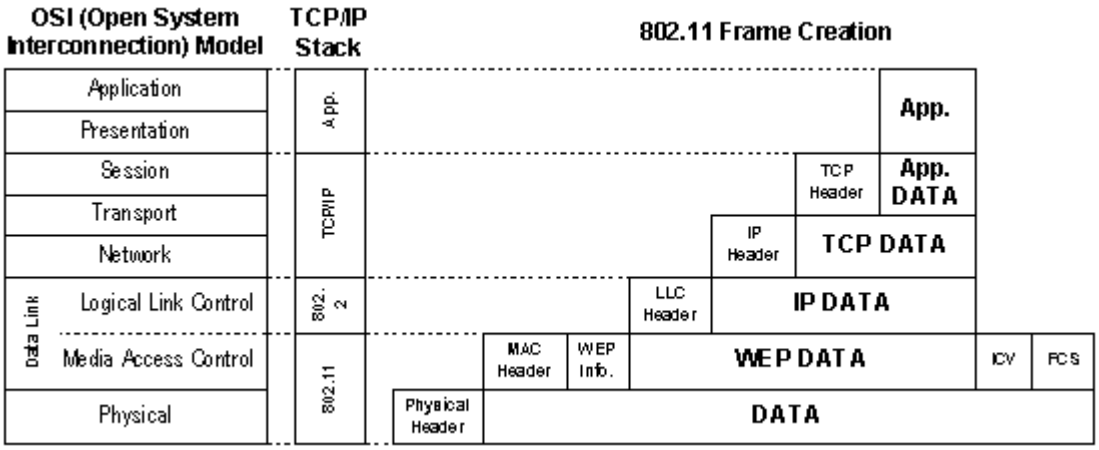
Traditionally, networked devices have always had to be physically connected into a network before gaining access to its resources, which has allowed organizations to physically restrict who is accessing the network. This is not the case when dealing with wireless networking. Due to the inherently open nature of a wireless network and the relative anonymity of wireless connections, wireless networks are becoming a popular backdoor into networks.

The latest adopted version of the IEEE 802.11 standard is 802.11b, which can provide wireless network transfer speeds of up to 11 Mbps. 802.11b wireless devices work on multiple RF (Radio Frequency) channels around the 2.4GHz band. The range of coverage of an 802.11b wireless device depends on the transmission power of the device and the physical topology of where it is located. The effective range of the wireless network may be outside the corporation's physical property which makes it hard, if not practically impossible, to restrict access to the wireless network. This networking exposure has been vividly demonstrated by a technique aptly named 'War Driving', where large numbers of completely unprotected WLANs (Wireless Local Area Networks) can be discovered just by driving through a city center with a wireless enabled laptop. [4]

Unfortunately, as is all too often the case, many address security as an afterthought, forcing those responsible to consider the features of the devices that they have already implemented. Most 802.11 wireless devices have a security protocol called WEP (Wired Equivalent Privacy) implemented in them. This paper explores why using only the WEP protocol to secure your Wireless LAN is far from adequate. It will also endeavor to provide a working solution to the problem of wireless security and options to adapt this solution to meet your requirements.

Section 2 - Vulnerabilities

Figure 1 – 802.11 Frame referenced against the OSI Model



** Original diagram created from information contained within referenced document [14].*

Visibility

Wireless (802.11) traffic can be sniffed. That is to say it is possible to collect all the data that travels over a wireless network. If this data is unencrypted (see Figure 1), it can be easily reassembled and read presenting a variety of issues depending on the wireless network. If the network is intentionally left open for public access, such as wireless internet access, your customers must be informed that there is no guarantee of privacy when using the service, so as not to open yourself up to unnecessary liability. Likewise, if the wireless LAN is intended for access to a corporate network, the information gathered could be subsequently used to impersonate a legitimate user or device to perform a network intrusion. To make matters worse, while an attacker is sniffing traffic they can remain completely undetected.

Authentication

WEP specifies the use of pre-shared keys as the means of authenticating a device. WEP does not however, specify how this key should be distributed or even the frequency that it should be changed. This has resulted in most manufacturers implementing no means of key distribution and in turn forcing their customers to manually configure each device with matching keys. The result of this is that most deployments of WEP use a manually configured key that rarely, or never, changes.

The SSID (Service Set Identifier) identifies the 802.11 devices that belong to a Basic Service Set (BSS). A BSS is analogous to a LAN (Local Area Network) in wired terms. Although some WLAN cards require that you manually configure the SSID, this is not meant to be a layer of security; rather it is meant as a method of identifying which Service Set you wish to communicate within when multiple Service Sets are in range. Even when using WEP encryption the SSID is still fully visible. Some manufacturers even allow there

wireless WLAN cards to poll for the SSID and self configure.

It is also possible to restrict access by MAC (Media Access Control) address on many APs (Access Points) by means of an ACL (Access Control List). Although all standards compliant network cards (including WLAN cards) should have a unique MAC address, software does exist that will allow this address to be 'spoofed'.

On a wireless network spoofing an IP address is easily done. Unlike Internet connected machines, which have routing issues to overcome, the IP addresses of wireless devices can be manually changed to whatever an intruder desires. On some networks, those that have a DHCP (Dynamic Host Configuration Protocol) or BOOTP server, the intruder may even be provided a valid IP address dynamically.

Encryption

Wired Equivalent Privacy (WEP) is the encryption protocol provided by the 802.11 standard. WEP delivers what its namesake suggests, privacy to the level that one could expect from a wired public network. IEEE 802.11 wireless, and the WEP protocol, are implemented at the lowest layers (Physical and Data Link Layer [Media Access Control] Layers) of the OSI model which means that it is independent of, and transparent to, higher-level protocols (such as TCP/IP). Operating at this layer provides 802.11 traffic an equivalent level of privacy when on a public network that one could expect without having a higher-level encryption protocol (e.g. SSL or IPSEC Encryption) protecting their traffic.

WEP as defined by the 802.11 standard has some design flaws that can allow for decryption of cipher text (encrypted plain text) by an attacker. WEP uses the RC4 encryption algorithm with either a 64bit or 128bit 'unique' per-frame key. The reason WEP is crackable is not because of any weakness in RC4 algorithm itself or even the key length, but rather the way the algorithm is implemented. [13]

The per-frame key is a combination of a pre-shared key (40bit or 104bit) and a pseudo random 24bit Initialization Vector (IV). The per-frame key is run through the RC4 encryption algorithm to produce the keystream.

WEP encryption and decryption is done using the same keystream at both the sending and receiving ends using a simple XOR (Exclusive OR) operation. This means that encryption is ***'keystream' XOR 'plaintext' equals 'cipher text'*** and that the reverse, decryption, is ***'cipher text' XOR 'keystream' equals 'plain text'***. One problem though is ***'cipher text' XOR 'plain text' equals 'keystream'*** is also true. This means that the keystream for any given cipher text can be found if some of the plain text is already known.

The combination of the pre-shared key and the random IV is intended to avoid duplicate keystreams from being used. Unfortunately, because the pre-shared key changes infrequently, the IV is the main means of insuring the uniqueness of the keystream.

The 802.11 standard does not define how the IV should be randomized and therefore have left this decision up to the hardware vendors. Because the IV is 24 bits long it can have over 16 million (2^{24}) possible values. If a vendor implements an inferior randomizing algorithm the effective IV length shrinks due to the increased likelihood of a duplicate IV being created. Sixteen million possible values may seem substantial, but when a new IV is required for every frame, the probability of a duplicate keystream becomes a valid concern.

The IV is included as a plain text field in every frame transmitted so that the receiver can combine it with the pre-shared key and generate the correct keystream for decryption. This also means an attacker can catalog all frames captured by their IV. Any two frames that have the same IV will be using the same keystream, unless the pre-shared key was changed between the times when the two frames were collected.

If the attacker has some means of knowing or accurately guessing some part of a WEP encrypted packet the use of the ***'cipher text' XOR 'plain text'*** equation can provide the keystream for a given IV. The next time this IV shows up in the data collection that packet can be decrypted, without having to know the under lying pre-shared key.

What cipher text may already be known to an attacker, or able to be guessed, depends on your particular scenario. Although large amounts of known data is the fastest way of determining as many keystreams as possible, the information may be as innocuous as known fields in a protocol header or a DNS name query.

Although the attack described above provides a simple method of decrypting WEP traffic, with more advanced cryptanalysis the actual WEP pre-shared key can be discovered. A proof of concept tool has been created that can discover a WEP key after as little as 1,000,000 encrypted frames [12] and some tools have been made publicly available that can discover a WEP key once only 100MB to 1GB of encrypted traffic has been collected. [5] [11]

Section 3 - Solution

Overview

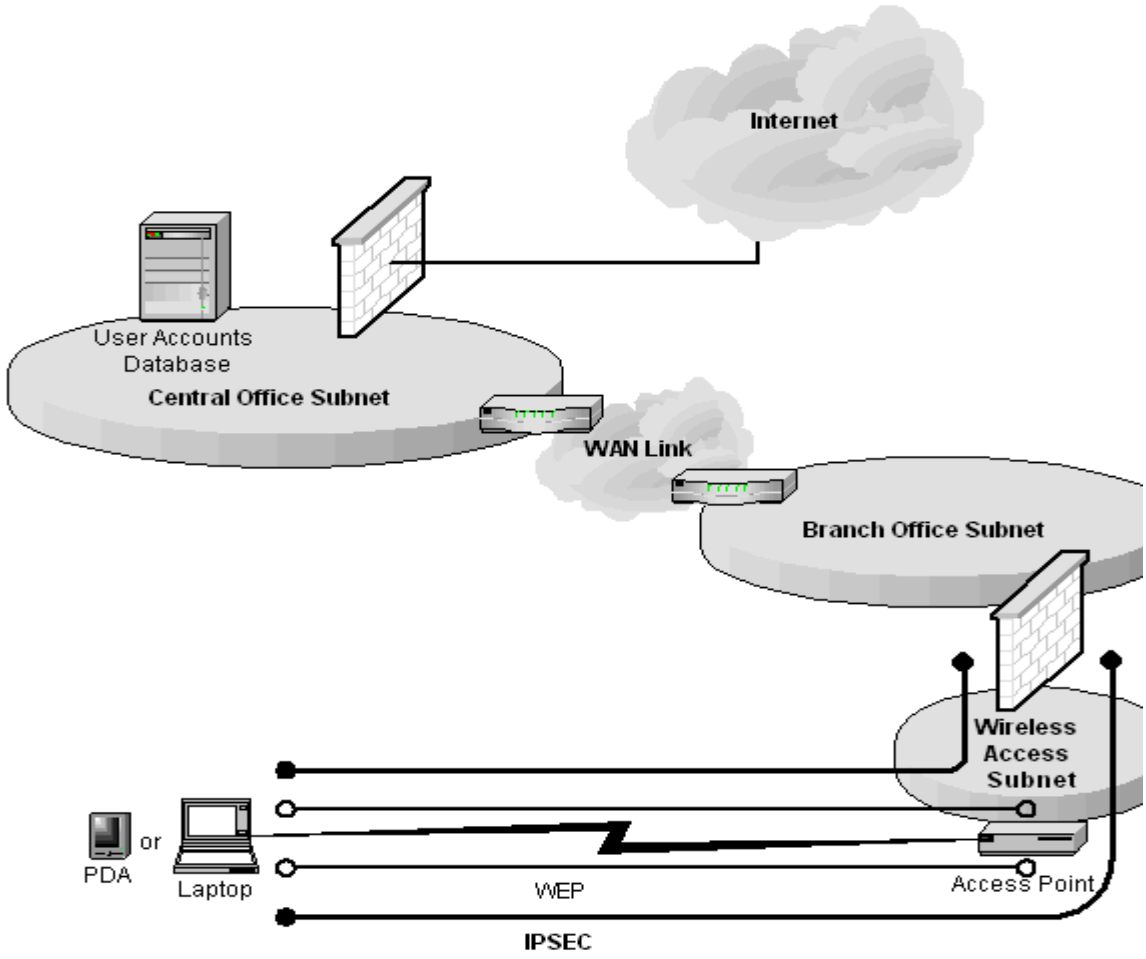
The very real probability of a wireless-based intrusion into a corporate network requires that multiple layers of security be used so that a compromise at one layer does not result in a complete exposure of the internal network. The point of this solution is to make wireless connections into your network abide by your corporations perimeter defense strategy and in turn make the weaknesses of WEP inconsequential.

Corporations normally have some sort of perimeter defense strategy, though the features vary greatly. For some, the strategy may be as simple a NAT (Network Address Translation) router for Internet connections, but for the most part perimeter defense strategies go far beyond this. The following list outlines some of the most common areas that a comprehensive strategy would include:

- Firewall port filtering (at all points of entry)
- Encrypted connections (for remote access)
- Double authentication (for remote access)
- Multi-layer zones (for publicly accessible servers)
- Network Intrusion Detection (either/both side/s of firewalls)

The wireless access solution (see Figure 2) includes most of these features while allowing for the remaining as required. It should be deployed with components and technologies that are compatible, or at least compliant, with your corporation's existing perimeter defense strategy. An important feature of this design is that it is standards based and modular, which will allow it to adapt to future technologies without having to be completely redesigned.

Figure 2 – Wireless Access Solution Diagram



** Original diagram*

Elements of the solution:

- IEEE 802.11b
  - WEP Enabled
  - WEP Key 104 bit
  - MAC ACL Enabled

- IPSec (Tunnel Mode)
  - Network Based Authentication
  - ESP using 3DES

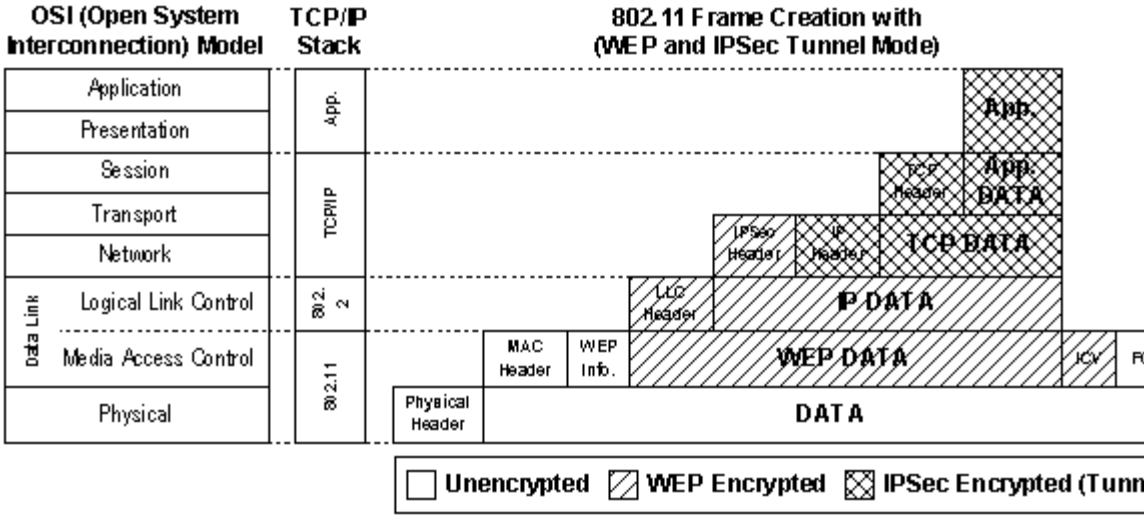
- Proxy Firewall
  - IPSec Tunnel End Point
  - Deny All except:
    - IPSec tunneled traffic
    - BOOTP (DHCP)

- Change factory default
  - Administrative ID
  - Administrative Password
  - WEP key
  - SSID (to a name that does not identify your corporation)
  - Disable response to ESS beacons

- WEP key management
  - Change WEP keys frequently
  - Distribute keys within the SSL tunnel prior to a scheduled change

Analysis

Figure 3 - 802.11 WEP\IPSec (Tunnel) Encrypted Frame referenced against the OSI Model



** Original diagram created from information contained within referenced documents [2] and [14].*

Having encryption occurring at both Layer 2 (Data Link) and Layer 3 (Network) of the OSI Model makes WEP more resistant to a decryption attack. Due to the fact most data within the WEP encrypted data chunk is now also encrypted with IPSec, there is very little left for the attacker to base their attack against. This does note make it impervious to attack though, as the LLC Header, and the IPSec Header still remain single encrypted.

The solution, though robust, still leaves some information completely 'out in the open'. The attacker will still be able to find out the: MAC address, SSID, IV, Key ID, and FCS. There is no way of encrypting this information as it is being exposed at the Physical and Media Access Control layers.

Due to the encryption strength provided by the interaction of the WEP (RC4) and IPSec

(DES3), the information provided by the SSID, IV and Key ID are of little use to attacker. The FCS (Frame Check Sequence) is just a one-way CRC (Cyclic Redundancy Check) of the payload of the Media Access Control packet and is used to establish the integrity of the frame after it has been transmitted.

Of the unencrypted data, the source MAC address is the most unfortunate exposure as it informs the attacker of a valid MAC address that can be subsequently spoofed. For this reason the MAC address should be considered supplemental to other methods of authentication.

In this design, authentication occurs for both the device and the user. The device is authenticated by means of the WEP Key, which although crackable, can be somewhat trusted as the key is being changed frequently and distributed securely. Before the device is allowed to communicate through the firewall the user of the device must also be authenticated to the central accounts database.

The firewall not only prevents unauthorized entry into the network but also blocks broadcast\multicast traffic that may provide details about the corporation's internal network. In turn, the IPSec tunnel on its way into the network does not give away any details of the internal network; it encrypts then replaces the IP Header that contains the destination IP address with it's own header that has the IP address of the tunnel end point which is the firewall.

Disabling an Access Point's response to ESS beacons does not prevent people from viewing the SSID, but does reduce the chances that your WLAN will be discovered in the first place. Popular wireless network discovery applications depend on these beacons to locate networks. [1]

Adaptation

The first part of adapting this solution is to choose how you will enable WEP. If your organization has already made an investment in wireless products your implementation choices may have been laid out for you already. In such a case you would need to take a highest common denominator approach when deciding what level of WEP (64bit or 128bit) you can afford to implement.

Another important choice is how to implement key distribution. The solution proposes that the keys be distributed via SSL prior to their scheduled change date. This would require individuals to reconfigure their own keys. In some organizations this would not be practical, and another secure method would need to be found. The most secure method is having one individual responsible for changing the key on each device, but this has the probable outcome of infrequent key changes. Some manufacturers have incorporated methods of key disruption into their products, but because IEEE 802.11 does not define how this is to be done, these solutions are proprietary. This is set to change in the near future with a supplementary standard that is presently in draft (IEEE 802.1x).

The next step is to decide what type of firewall fits your needs. This critical piece places a layer of abstraction between your wireless network segment and your corporation's internal network. This is what really makes this solution part of your perimeter defenses. When choosing the firewall, ask yourself the following:

- What products are already protecting my Internet gateway? Are they appropriate for this Wireless gateway?
- How many locations (separate network segments) is this solution going to be used in? If many, what is the incremental cost, and can all of the gateways be managed centrally?
- Does the product support the remote user authentication method mandated by my corporation's remote access policy?
- Is the implementation of this authentication method compatible with my central accounts database/s?
- Will the firewall allow me to implement encrypted traffic tunnels with the types of wireless devices that we will be using?

The last major decision you will need to make in adapting this solution to your environment is whether IPSec is viable in your infrastructure. The secondary method of encryption does not have to be IPSec for this solution to work, but the trade-offs have to be understood before a different technology is selected. If SSL (Secure Socket Layers) was chosen, for example, the creation of a tunnel between the firewall and the connecting client would not be possible, therefore exposing the real destination address within the IP header. SSL operates at a higher layer in the TCP/IP stack and therefore exposes more information to the layers below. SSL is primarily implemented as a web protocol, which means it may restrict what types of applications your corporation can enable over your wireless network.

Section 4 - Conclusion

IEEE 802.11 truly is a useful technology and as portable devices continue to become more popular in the work place, so will wireless networking. Although the security issues that this technology currently faces are sure to change, there will certainly be many more to come before this technology has fully matured. Due to the severe network exposures that wireless devices can create it is imperative that corporate network security specialists understand wireless networking.

Appendix A -References

[1] Bowman, Barb. "Securing SOHO Wireless Residential LANS" 3 Dec. 2001. URL:http://www.microsoft.com/windowsxp/expertzone/columns/bowman/december03.asp (23 Jan. 2002)

[2] Doraswamy, Naganand & Harkins, Dan. "IPSec Architecture" Chapter 4 of IPSec – The New Security Standard for the Internet, Intranets and Virtual Private Networks. 1999. URL:http://www.microsoft.com/technet/security/network/ipsecarc.asp (23 Jan. 2002)

[3] Doraswamy, Naganand & Harkins, Dan. "IPSec Implementation" Chapter 9 of IPSec – The New Security Standard for the Internet, Intranets and Virtual Private Networks. 1999. URL:http://www.microsoft.com/technet/security/network/ipsecimp.asp (23 Jan. 2002)

[4] Emigh, Jacqueline. "Driveby Hacking on the GO" 4 Jan. 2002. URL:http://itmanagement.earthweb.com/secu/article/0,,11953_949081,00.html (23 Jan. 2002)

[5] Jeremy & Blake. "AirSnort Homepage" URL:http://airsnort.sourceforge.net/ (23 Jan. 2002)

[6] LAN MAN Standards Committee of the IEEE Computer Society. "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" ANSI/IEEE Std 802.11, 1999 Edition. 1 Feb. 2000. URL:http://standards.ieee.org/reading/ieee/std/lanman/802.11-1999.pdf (23 Jan. 2002)

[7] LAN MAN Standards Committee of the IEEE Computer Society. "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Higher-Speed Physical Layer Extension in the 2.4 GHz Band " IEEE Std 802.11b-1999. 18 Sept. 2001. URL:http://standards.ieee.org/reading/ieee/std/lanman/802.11b-1999.pdf (23 Jan. 2002)

[8] Newsham, Tim "Cracking WEP Keys" 13 June 2001. URL:http://www.lava.net/~newsham/wlan/WEP_password_cracker.ppt (23 Jan. 2002)

[9] Nicolett, Mark "Gartner Predicts 2002: What's Ahead for IT Infrastucture" 9 Jan. 2002. URL:http://www4.gartner.com/DisplayDocument?doc_cd=103717 (23 Jan. 2002)

[10] Microsoft Corporation. "Traffic That Can--and Cannot—Be Secured by IPSec" Q253169. 17 Apr. 2000. URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;q253169 (23 Jan. 2002)

[11] Rager, Anton T. "WEPCrack – An 802.11 key breaker" URL:http://wepcrack.sourceforge.net/ (23 Jan. 2002)

[12] Stubblefield. Adam & Ioannidis, John & Rubin, Aviel D. “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP” Revision 2. 21. Aug. 2001
URL:http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf (23 Jan. 2002)

[13] Walker, Jesse R. “Unsafe at any key size; An analysis of the WEP encapsulation” Doc.: IEEE 802.11-00/362. 27 Oct. 2000.
URL:http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip (23 Jan. 2002)

[14] WildPackets, Inc. “WildPackets’ Guide to Wireless LAN Analysis”
URL:http://www.wildpackets.com/elements/Wireless_LAN_Analysis.pdf (23 Jan. 2002)