Global Information Assurance Certification Paper

IEEE 802.11b Wireless LAN: Security Risks
Version 1.0
Eng Tiong Ow
September 20, 2001

Introduction

The wireless networking standard, the IEEE 802.11b, has recently become more and more popular due to its convenience and falling prices of the hardware. Users have the ability to transfer large files, access the Web and other high bandwidth activities without having the need to attach network cables to ports that are connected to switches or hubs. They have the freedom to roam around anywhere within the range of the wireless network. This paper will discuss the security features implemented in the 802.11b standard and the vulnerabilities discovered.

What is Wireless LAN

An 802.11b Wireless LAN (WLAN) works by using Radio Frequency (RF) to transmit and receive data over the air without the need for cables. It can pass thru walls, ceilings. By using RF, it offers the features of Ethernet without the need to being tied to a cable thus providing freedom and flexibility unmatched by Wired LAN. WLAN are available in 2 basic configurations: Peer to Peer and Client/Server.

In a Peer-to-Peer configuration, multiple PCs or Laptops are equipped with wireless adapter cards and are not connected to any wired networked. It is a simple way to setup a network rapidly when access to a wired infrastructure is not available or needed. Clients talk to each other within the transmission range of each other. In a Client/Server configuration, multiple PCs or Laptops communicate to a wired network hub. This hub is called an access point. An access point can provide coverage from 150 meters indoors to over 500 meters outdoors depending on factors such as obstructions like ceilings and walls to the type of antenna being used. A single access point can support up to hundreds of users. Adding more access points will decrease congestions and provide more coverage.

Challenges for the Network Manager

In the traditional Wired LAN, access is via the connection to an Ethernet port, thus access control to the LAN is governed by the physical access to the LAN ports. In a WLAN environment, the data is transmitted by another medium using RF. Since RF has the ability to penetrate walls and ceilings, any WLAN client can receive it intentionally or unintentionally if it is within range. A client on a different floor, just across the room or outside the building has the ability to passively 'sniff' your network traffic without gaining physical access as long as the person has a WLAN network card that has a promiscuous mode (ability to capture every packet on the segment of the LAN). While the same may happen on a Wired LAN, the person needs to use sensitive listening equipment and it has to be held close to the cable to listen to the electromagnetic waves. For any Network Manager these are serious concerns that have to be considered before introducing Wireless LAN to any organization. The two main issues of access control and privacy have to be addressed. Access control is needed so that data is only transmitted and received by users authorized by the organization. Privacy ensures that those who are authorized to view it only understand any data.

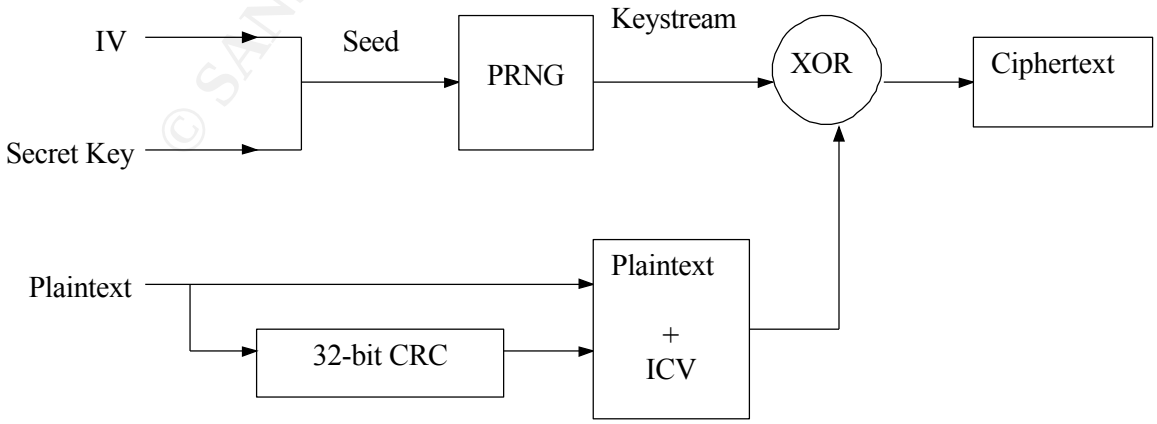
Mechanisms for access control and privacy

IEEE 802.11b group specifies two mechanisms for ensuring both privacy and access control: service set identifiers (SSID) and wired equivalent privacy (WEP). SSID is a setting on the access point that restricts access to approved users using the same network name. Users need to provide the name of the network in their client settings in order to be allowed access to the access point. SSID is used to group users into segments in the network. The idea is that only users who have the SSID name can join the network. The SSID can then act as a shared password for access into the network.

Some manufacturers provided another form of access control via access control lists based on the Ethernet MAC address of the client. The access point will determine the access to the network from a list of authorized MAC addresses.

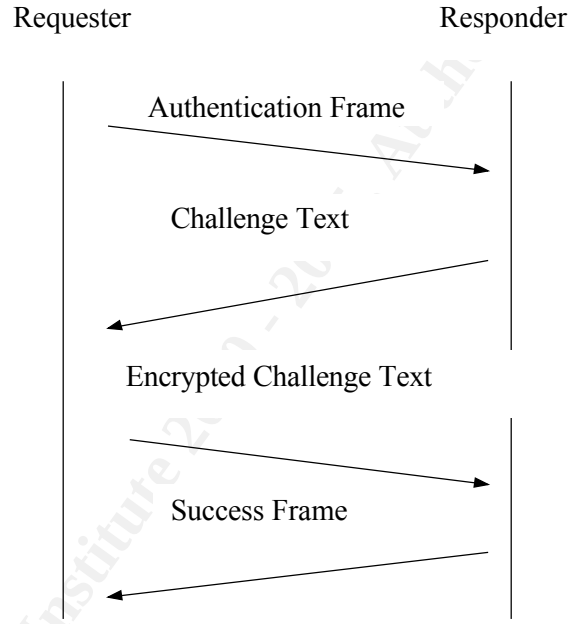
WEP provides two functions. One is to ensure privacy through encryption and the other function is to offer a form of access control. WEP uses a symmetric encryption scheme where a shared key is used for both encryption and decryption. The encryption method used is the RC4 stream cipher system from RSA. A 40 bit shared secret key forms the heart of the system. This key must exist in both the client and access point in order for it to work. Two other additional features were added to augment the system. An Integrity Check Value (ICV) field, which does a 32-bit CRC check on the data frame. The result from the ICV is added to the end of the frame. It is to prevent a hacker from modifying or changing the contents of the packet during transmission. An Initialization Vector (IV) is also added to the shared secret key in each packet to ensure that each packet has a different RC4 key. The IV is a 24-bit field, which produces a 64-bit field when combined with the 40-bit key. This IV is sent in clear text in a WEP data frame and the 802.11b standard states that changing the IV with each packet is an optional feature.

In order to encrypt a WLAN frame, the plaintext data frame goes through the 32-bit CRC check to derive the ICV field, which is concatenated together with the plaintext. The shared secret key is prepended with the per packet IV to produce a seed. It is passed through a pseudo-random number generator (PRNG) to produce a keystream. The keystream, which is equal in length to the data to be encrypted, is exclusive-ored (XOR) with the plaintext frame containing the ICV to generate a ciphertext frame. Finally the IV is prepended to this ciphertext frame as the WEP data frame. To decipher the WEP data frame, the IV that arrived is prepended with the recipient's own secret key and goes thru the PRNG to obtain a key sequence. This key sequence is used to decrypt and obtain the plaintext via exclusive-ored method again. The plaintext's ICV is then check with the ICV generated from the plaintext using 32-bit CRC check to ensure that the packet was not tampered with during transit.



Example of WEP encryption

For the authentication process, IEEE 802.11b specifies two methods for authentication: Open System and Shared key method. The Open System method of authentication is the default method and is essentially a NULL authentication process. Anyone can request authentication and the result need not to be successful. The Shared key method uses the challenge and response method together with the shared key. This is done without the shared key being transmitted in the clear. The station that wishes to be authenticated (*requester*) will send an authentication frame over to the other station (*responder*). The *responder* after receiving the request will then send back a frame that contains the challenge text. This challenge text consists of 128 octets that are generated by the PRNG. The value of this challenge text is unimportant but it is important that it is not a static value. When the *requester* receive this challenge text, it will be copied and undergo encryption by the WEP, and together with the unencrypted challenge text, it is send back to the *responder*. The responder will now attempt to decrypt the contents of the encrypted challenge text. It will check the ICV after which if successful, the responder will compare the decrypted text to the original challenge text. If the match is correct, the authentication is successful, a success frame is send to the *requester*.



Example of Shared Key Authentication

Weakness of SSID

Earlier in the article, the use of SSID as a means of authentication method was discussed. However it is not difficult to realize that implementing it as a primary security feature is not desirable especially in a large network. The more people who knew the password, the higher the probability that a misuse might occur. The password can be changed from time to time but in a large environment, this could be a mammoth task. Another fact is that most access points out there made by most manufacturers broadcast the SSID in their signals. There are also access points out there using default SSIDs provided by the manufacturers and a list of those default SSIDs is available for download on the Internet. It is also very easy for any

hacker to determine the SSID of a network and gain access to it via software tools.

Wardriving or Wireless LAN Mapping

Wardriving is a term used to describe a hacker armed with a laptop, wireless adapter card and a mode of transportation such as car, bus or subway. The person goes around sniffing for WLANs. Currently there are two tools freely available out on the Internet that can be used to map a WLAN. . These two tools: Netstumbler (http://www.netstumbler.com) and IBM's Wireless Security Auditor (http://www.research.ibm.com/gsal/wsa/) provided a hacker with vital information such as SSID and access point name, signal strength, the vendor of the access points, the firmware version of the access point, the encryption method and the authentication method. From all these information, a hacker would be able to determine which company he had just probed and the value of information that is within the network. Armed with the SSID information, a network that does not have WEP enabled is very vulnerable to an attack from a malicious person. An advantage for the network administrator is that these tools allow him or her to determine if there are rouge access points installed by users inside their network without his or her knowledge. They are numerous WLAN routers available in the market now. It is not difficult for any person in an organization to purchase one and plug it into the Wired LAN. With built in NAT and DHCP services, a little WLAN network could spring up anytime creating a back door into the network.

Weakness of WEP

In February this year, Nikita Borisov and a group of researchers from University of California at Berkeley published the first paper regarding weaknesses in the WEP. The WEP uses the RC4 stream cipher. Stream cipher works by expanding a secret key, in this case the shared secret prepended with the IV, into a long keystream of pseudorandom bits. The weakness of stream cipher is that the two messages must not use the same keystream as this can reveal information about both messages. By XORing two ciphertexts that uses the same keystream, will cause the keystream to cancel out and the result is the XOR of the two plaintext.

C1 = P1 XOR RC4(IV, Keystream)
C2 = P2 XOR RC4(IV, Keystream)
C1 XOR C2 = (P1 XOR RC4(IV, Keystream)) XOR (P2 XOR RC4(IV, Keystream))
= P1 XOR P2

With this XOR information, an attacker can use a statistical attack to recover the plaintexts. But in order for this method to work, two conditions must occur, firstly ciphertexts with keystream that are used more than once are available and secondly partial knowledge of the plaintext. To prevent this, the WEP recommends that the IV that vary from packet to packet. However this IV is included unencrypted in the WEP data frame so that the receiver can know what IV to use for decryption. So in reality, only the shared secret key is truly secret from the attacker.

The WEP standards do not require that IV be changed after every packet. The researchers found that the PCMCIA WLAN cards that they tested reset the IV to 0 each time it's re-initialized, and the IV is incremented by one for each packet. Thus IVs with low value will be generated as keystreams making the attack small in scale. The IV consists of only 24 bits, so there are only about 16 million possible values. A busy access point, which generates 2000-byte size packets at 5 Mbps, will use up the available space in about 14 hours. If an attacker

can have 2^{24} know plaintexts, using the XOR with the same IV can then decrypt all WEP data packets.

To obtain plaintexts, the researchers provided several methods. The first method involves the attacker listen passively on the wireless traffic. When two IVs are reused (called collision), the attacker will XOR the two packets to obtain XOR of the two plaintexts. The attacker still need to know at least one plaintext of two, once this is know, all other messages that uses this keystream can be obtainable. An attacker can send a packet, with a plaintext known to him, over the Internet to the access point. The access will encrypt the packet before transmitting it over the air for the attacker to intercept it. The researchers also discovered that some access points transmit broadcast messages in plaintext and encrypted form when access control is disabled. An attacker simply transmits a broadcast message, which is accepted since access control is disabled, and the access point will in turn retransmit in encrypted form. But the easiest method is to get hold of the packets used in the WEP authentication process as both plain and encrypted challenge are send back to the access point.

Now the hacker just simply stores this keystream in a table using the IV as the index. The size of this table is the most 24 GB and hard disk of this capacity is cheaply and easily available in the market. So the next time the attacker receives a packet with the same IV and assuming the secret key is still the same. He can look up the table to obtain the keystream, XOR is against the packet to decrypt the plaintext. And since most WLAN clients re-initialized their IV to 0, this reduces the dictionary size, as the range of IVs will be small. It does not matter if 40 bit or 104 bit shared secret key are used as the attack centers on the IV collision.

The researchers also found fault in the ICV adopted by WEP, it was designed to provide integrity to the data transmitted. The 32-bit CRC used for the ICV can be used to detect random error but not against malicious errors. Being linear function, 32-bit CRC when used with RC4, which is linear too, allows an attacker to modify the packet due to weakness in them. Once an attacker obtains the plaintext for one encrypted message, he possesses the ability to construct correct encrypted packets. To achieve this, he creates a new message, determines the ICV and then uses it to XOR with the encrypted packet to produce new cipher text. When the recipient decodes the packet, it will not notice that the message has been changed as the ICV is valid. Another possible method is to adjust the ICV itself in order to hide the changed plaintext.

It is noted that in the WEP authentication process, the *requester* sends both the plaintext and ciphertext of the challenge frame to the *responder*. The attacker can derive the keystream from this knowledge and attempts to get himself authenticated. The attacker will get a challenge text from the access point and armed with this keystream, an XOR with the challenge text will produce the necessary encrypted text and the access point will allow entry when it receives it. This attack works as the access point allows the reuse of IVs.

Together with all these techniques to modify and inject packets mention above, the hacker could use it to decrypt packets. Since he does not know the shared secret key, he will make use of the access point, which has the ability to decrypt packets

and then forward it to the attacker. First, the enemy gains access by tricking the authentication process. He then takes the packet to be decrypted and changes its destination IP address to the one that he controls. He then sends it to the access point that will decrypt it and then forward it to the altered destination IP. Even if the access point is not connected to the Internet, an attacker can still decrypt the packets. However this method only works on the TCP traffic. This is because the attacker needs to make use of the TCP checksum to determine if the TCP packet is accepted or rejected. A ciphertext is captured and then a few bits in the ciphertext are flipped and the ICV is adjusted such that the WEP portion is correct. The new packet is then transmitted to the access point. If there is a TCP acknowledge packet, it shows that the modified packet is accepted and passed the TCP checksum. By selectively choosing the bits to flip, the attacker can slowly learn most of the plaintext.

Weaknesses In Key Schedule Algorithm in RC4

Scott Fluhrer, Itsik Mantin and Adi Shamir publish a paper in August this year that provided the most devastating attack ever on the WEP. In the paper, the trio discovered that by using only the first word of the keystream, they could obtain information of the shared secret key. A search is conducted to find IVs that causes the keystream to leak out information regarding the key. The authors termed this condition as *resolved* condition. Each of these *resolved* packets only leaks out information for one key byte and that key byte must be guessed correctly so that the next packet can offer information of the next key byte. To speed up the attack only certain IVs, which are weak, are searched for. When guessing the key byte, the resolved packet provides a 5% chance of getting it correct. But since there is a large amount of resolved packets traveling the network, the chances are greater. Adam Stubblefield, an intern at AT&T Labs, was the first person to implement this attack. He noted that an extra 802.2 header is added in IP traffic, this make the attack easier as every IP packet has the same first plaintext byte. In order for the attack to be successful, during the early phase of the attack, the first few key byes must be guessed correctly. Stubblefield utilized two methods to achieve this. The first way is to target *resolved* packets to narrow down the possible combination of key bytes. These keys are then check if its correct by checking if the ICV from the decrypted packets. The second method centers on the way WEP keys are distributed. A user most probably has to enter an easy to remember key into the configuration software. An easy to remember key should contain ASCII characters, by checking if the key bytes matches an ASCII character such as letter or symbol etc. the chances of guessing the correct key byte increases. The Borisov attack will not yield the secret key easily but this attack makes it possible .In a flooded traffic environment this makes the attack easier and most importantly it is passive in nature. It scales linearly so regardless if it is 40-bit or 104-bit, it makes not much of a difference in terms of difficulty. Soon after the Fluhrer and Stubblefield papers are released, two *script kiddies* tools came out on the Internet, Wepcrack and Airsnort.

Ways to safeguard your WEP network

To safeguard a WLAN, it is recommended that the default SSID be changed, a check on the Netstumbler's website database reveals numerous access points using the default value supplied by the manufacturer. The SSID and the access point name should not reflect your company's main name, division, products, brand name or any information that allows a

hacker to determine which company he or she found. Turn off the broadcast of SSID in your access point. Although using MAC addresses as a security measure is an excellent idea, there is scalability problems as the number of address that can be stored by an access point is limited. Most PCMCIA WLAN cards have their MAC address printed on the card itself, a malicious user can simply copy the address and spoof it. MAC addresses are also broadcast in the clear so an attacker just simply 'sniffs' it. This job is made even easier when most WLAN cards allow their MAC address to be change in software.

Vendors were already implementing ways to improve the security of WEP before the Fluhrer paper came out. A major weakness is the use of a shared secret key. There is no proper key management procedure spelt out in the 802.11b specification. A group of vendors is proposing to use the IEEE 802.1x standard for authentication and key distribution. Cisco has implemented it in its Aironet series of cards and Microsoft has added the feature to its latest OS, WinXP. The 802.1x was designed for all IEEE 802 LANs. It role is to provide a level of authentication such that the network can establish the identify of the end-user that its trying to connect to it. Any stolen wireless cards no longer poses a threat as the network now authenticates the user not the hardware. When the user (called supplicant) wishes to use the service of the network, he will connect to the switch or access point in our case (called authenticator) and a RADIUS server (called an authentication server) at the other end will receive the request and issue a challenge. If the supplicant could provide a correct response, it is allowed access. In the Cisco model, the supplicant and authentication server will change roles and attempt mutual communication. The advantage of using this method of authentication is that the risk of authenticating to a rouge access point is minimized. As the user knows that it is authenticating with a known access point. It also allows access control via the assigning of VLAN membership from the outcome of the authentication. In the Cisco implementation of 802.1x, after authentication, the authentication server and the supplicant will determine a WEP key for the session. This gives each client a unique WEP for every session. Although, this unique per session WEP key makes the Fluhrer attack more difficult. Once an attacker has gathered sufficient packets from a user who remains connected for a long duration. This unique per user per session WEP key is vulnerable to airsnort or webcrack attack. What Cisco recommends is to set a timeout for each user. The timeout should be fast enough such that there is no chance for an attacker to compromise the WEP key. Factors for determining the timeout include: numbers of users per access point, the packet size and the packet rate. While the Cisco solution may look attractive in solving WEP's problems, the disadvantage is that the entire inventory of access points and wireless cards has to be changed to Cisco products.

Another technology proposed by the company NextComm, Inc. (http://www.nextcomm.com) uses an IC chip that uses MD5 hash to generate the keystream and a key distribution system to change keys rapidly. Called Key Hopping, this distribution system can change keys as fast as every three seconds to prevent hackers from gathering enough packets for analysis. However this system requires the access points and client cards to use the IC chip in order to enjoy the benefits.

The most interesting solution comes from Interlink Networks' (http://www.interlinknetworks.com) Wireless Access Manager. Available as

software, it implements the EAP and LEAP protocol used in the 802.1x standard. Using a RADIUS-based solution, it provides the WLAN with the same security features found in the Cisco Aironet series described earlier. Companies with existing access points and wireless cards need not upgrade or change them to new ones as long as the access points are RADIUS compliant.

Besides relying on the WEP for confidentiality, users should use other available encryption methods. SSH should be use instead of using telnet when connecting to remote hosts. Tunneling features available in SSH can be utilized for providing secure connections to your applications that are connected to a remote server. An example is the POP mail, instead of connecting directly over to the POP server. Configure your SSH client to create a secure tunnel from the machine to the port on the remote server side. Configure your mail reader to the local port that connects to this tunnel. When installing SSH, do take the effort to install SSH version 2 to avoid vulnerabilities found in the earlier one. There are quiet a few SSH software available on the Internet for free such as OPENSSH. This should help make implementing SSH an attractive option. PGP should also be used to ensure that your emails are confidential.

A VPN can be used to act as a gateway between the WLAN and the network. It can supplement the WEP's function of authentication and encryption. When VPN clients need to access the network, it will connect to a VPN server. The server will authenticate the client. If successful, the VPN server will provide the client with an IP and an encryption key. All communications are done through this IP. Every packet that passes through this secure tunnel between the client and server will be encrypted. An attacker cannot simply hijack an IP to gain access, as he does not possess the encryption key. The VPN server will simply reject all connections from the attacker. VPN solutions are available in hardware boxes or software that are installed in computers. The advantages of employing a hardware solution are speed in encrypting and decrypting packets. Another advantage of implementing VPN is that employees who wish to access the organization's network from ISPs can connect by a VPN.

Place all access points outside a firewall. All connections to the web servers inside the organization's network should go through SSL. This is to prevent any information from being sent or receive in the clear text. It is advisable to use SSL 3.0 only as the 2.0 version suffers from the man in the middle attack.

Do a periodic wireless scan of your network to pick up rouge access points that may have pop up unnoticed. This is especially dangerous when someone setups a wireless network inside the firewall. Add or amend your security policy to prevent users from setting up their own wireless network without permission.

Summary

While there are serious vulnerabilities when using WLANs. Taking certain precautions to safeguard the confidentiality and integrity of your data can make your WLAN as safe as the wired equivalent. Although these precautions may cost more effort and money, they are necessary if you have an existing WLAN or intend to implement one. The 802.11 Tgi group is working on new ways to replace WEP with schemes such as replacing the RC4 with AES and adding sequence numbers to

packets to prevent replay attacks. Until such schemes are finalized and available as the 802.11i standard, there will be no complete fix for these existing vulnerabilities.

References

ANSI/IEEE "Std 802.11 1999 Edition" 20 September 2001 P: 59-69 URL: http://a957.g.akamai.net/7/957/3680/v0001/standards.ieee.org/reading/ieee/std/lanman/802.11-1999.pdf

Nikita Borisov, Ian Goldberg, David Wagner "Intercepting Mobile Communications: The Insecurity of 802.11" 20 September 2001 URL: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

Scott Fluhrer, Itsik Mantin, Adi Shamir "Weakness in the Key Scheduling Algorithm of RC4" 20 September 2001 URL: http://www.eyetap.org/~rguerra/toronto2001/rc4_ksaproc.pdf

Adam Stubblefield, John Ioannidis, Aviel D. Rubin "Using the Fluhrer, Martin, and Shamir Attack to Break WEP" Revision 2. 21 August 2001 URL: http://www.cs.rice.edu/~astubble/wep_attack.pdf

William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan "Your 802.11 Wireless Network has No Clothes" 30 March 2001 URL: http://www.cs.umd.edu/~waa/wireless.pdf

Sultan Weatherspoon "Overview of IEEE 802.11b Security" 2000 URL: http://developer.intel.com/technology/itj/q22000/articles/art_5.htm

Cisco "Cisco Aironet 350 Series Wireless LAN Security" 20 September 2001 URL: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm

Intel "IEEE 802.11b High Rate Wireless Local Area Networks" 20 September 2001 URL: http://channel.intel.com/business/ibmp/files/sb-networking-100100-sbc-01.pdf

Tom Zeller "Security Still Up in the Air" 5 February 2001 URL: http://www.networkcomputing.com/1203/1203ws1.html