Wireless LAN Security

Today and Tomorrow

By

Sangram Gayal

and

Dr. S. A. Vetha Manickam

Center for Information and Network Security

Pune University

Table of Contents

1. Introduction

Wireless LANs are a boon for organizations that don't have time to setup wired LANs, make networked temporary offices a reality and remove the wire work that goes on in setting LANs. They are reported to reduce setting up costs by 15%. But, with these benefits come the security concerns.

One doesn't need to have physical access to your wires to get into your LANs now. Any attacker, even though sitting in your parking lot, or in your neighboring building, can make a mockery of the security mechanisms of your WLAN.

If you don't care about security, then go ahead; buy those WLAN cards/ Access Points. But, if you do, watch out for the developments on the security front of 802.11.

As this report and many such others tell, contrary to 802.11's claims, WLANs have very little security. An attacker can listen to you, take control of your laptops/desktops and forge him to be you. He can cancel your orders, make changes into your databases, or empty your credit cards.

So, what is the remedy?

Don't trust anybody!!!

Think like an attacker and take proper countermeasures. Have dynamic system administrators. Those attackers won't be lucky every time! The key is, be informed!

2. Wireless LANs

Wireless LANs (WLANs) are quickly gaining popularity due to their ease of installation and higher employee mobility. Together with PDAs and other mobility devices, they go on to improve the quality of life.

2.1 Types of Wireless LANS

The part of success behind the popularity of WLANs is due to the availability of the 802.11 standard from IEEE. The standard specifies operation of WLANs in three ways:

- Infrastructure Mode: Every WLAN workstation (WS) communicates to any machine through an access point (AP). The machine can be in the same WLAN or connected to the outside world through the AP.

- Ad Hoc Network Mode: Every WS talks to another WS directly.

- Mixed Network Mode: Every WS can work in the above two modes simultaneously. This is also called the Extended Basic Service Set (EBSS)

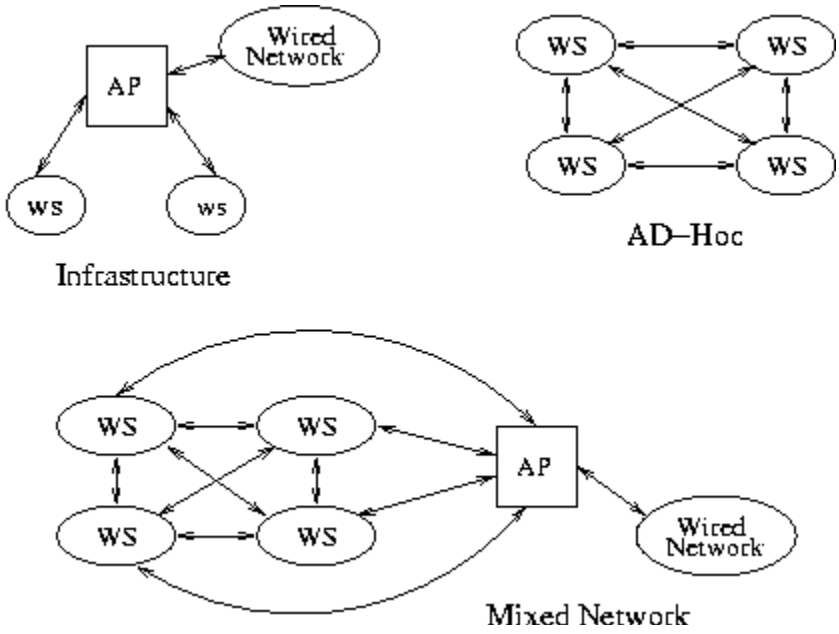

Fig2.1: Types of WLAN

2.2 Protocol Stack

The protocol stack for WLANs was designed such that existing applications can use them with minor modifications. The top three layers of the stack are same as the other networks.

Application Layer
Transport Layer
Network Layer
802.11 MAC/Data-link Layer
802.11 Physical Layer

2.3 The 802.11 Physical Layer

The 802.11 physical layers modulate the data and send it over the air. Three popular standards have emerged since the inception of WLANs, 802.11a, 802.11b, and 802.11g. The comparison between the above standards are given in the following table.

Parameter	802.11a	802.11b	802.11g
Speed	54 Mbps	11Mbps	54Mbps
Frequency Band	5 GHz	2.4 GHz	2.4 GHz
Modulation	OFDM	DSSS	OFDM
Distance(Indoor)	18 mts	30 mts	30 mts
Distance(Outdoor)	30 mts	120 mts	120 mts
No. of simultaneous networks	12	3	3
Availability	Came after 802.11b available	Widely available in the market	To hit the market by mid 2002
Comments	No interference ; less distance due to high frequencies	Interference from RF sources like cordless phones	Interference, backwards compatible with 802.11b

Table 2.1 Comparison between 802.11 a, b, g

2.4 802.11 MAC layer

The MAC / datalink layer of 802.11(IEEE std., 1) specifies the following features:

1. CRC checksum
2. Fragmentation
3. Auto-Roaming
4. Authentication and Association
5. WEP (Wired Equivalent Security) Protocol

The data-link layer level encryption was intended to perform Wired Equivalent Security, but attackers have proven all these claims false and hollow. In the subsequent sections, we shall consider the loopholes in WEP.

3. Security Features of Wireless LANs

A message traveling by air can be intercepted without physical access to the wiring of an organization. Any person, sitting in the vicinity of a WLAN with a transceiver with a capability to listen/talk, can pose a threat. Unfortunately, the same hardware that is used for WLAN communication can be employed for such attacks. To make the WLANs reliable the following security goals were considered:

- Confidentiality
- Data Integrity
- Access Control

The following security measures are a part of the 802.11 IEEE protocol:

- Authentication
- Association
- Encryption

The need of a client to be mobile brought in the separation of authentication and association processes. Since a client frequently changes AP boundaries, he can be authenticated to various AP at a given point, yet remains associated to his chosen one. Before a client gets associated to other, he must be first authenticated.

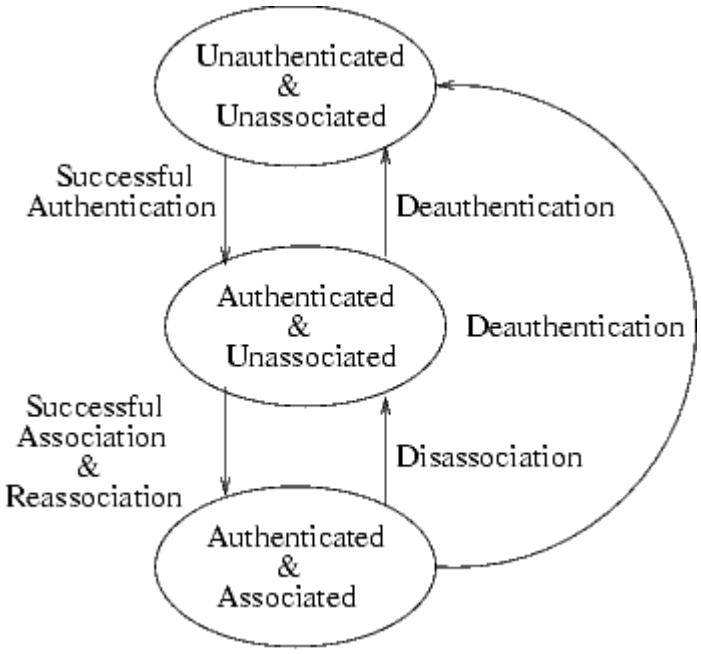

Fig 3.1: Authentication & Association

3.1 Authentication

802.11 specify two authentication mechanisms:

1 Open system authentication
2 Shared key authentication

- **Open system authentication**

A client needs an SSID for successful Association. Any new client that comes in an EBSS area is provided with an SSID. This is equivalent to no security.

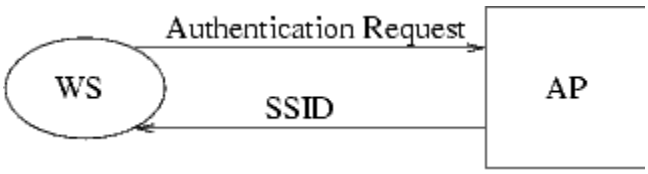

Fig 3.2: Open System Authentication

- **Shared system authentication**

The client cannot authenticate himself if he doesn't have the WEP shared secret key. WEP protocol is used for encryption.

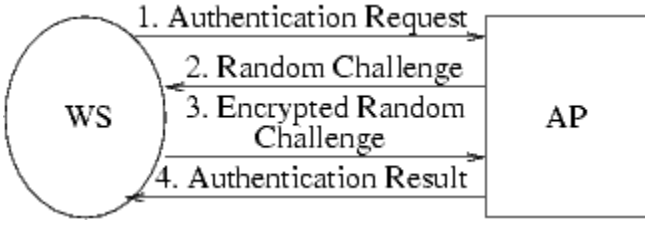

Fig 3.3: Shared key authentication

3.2 Association

An SSID is used to differentiate two networks logically. To successfully associate to a WS, one must have the SSID of the other WS. This was not intended to be a security feature, and in fact SSID is sent in open in the beacon frame of the AP.

3.3 Encryption and Decryption-The WEP Protocol

The WLAN administrator has an option (if the administrator decides to send the packets unencrypted) to make all the communication over the air encrypted, i.e. every frame that is below the Ethernet Header is encrypted using the WEP protocol. The WEP protocol has three components:

- A shared secret key, k (40bit /104 bit): The fact that the secret key is shared helps reduce the load on AP, while simultaneously assuming that whoever is given the secret key is a trusted person. This shared key is never sent over the air.802.11 doesn't discuss the deployment of this key onto Work Stations. It has to be installed manually at each WS/AP. Most APs can handle up to four shared secret keys.

- Initialization vector, IV (24 bit): IV is a per-packet number that is sent in clear over the air. This number is most effective if generated randomly, because it is used as one of the inputs to the RC4 algorithm. 802.11 don't specify generation of IV. Infact, many cards generate IVs in linear fashion, i.e., 1,2,3…

- RC4 algorithm, RC4 (IV, k): This algorithm is used to generate a key stream K, length equal to that of the message to be transmitted by the data-link layer. It takes the IV and k as inputs.

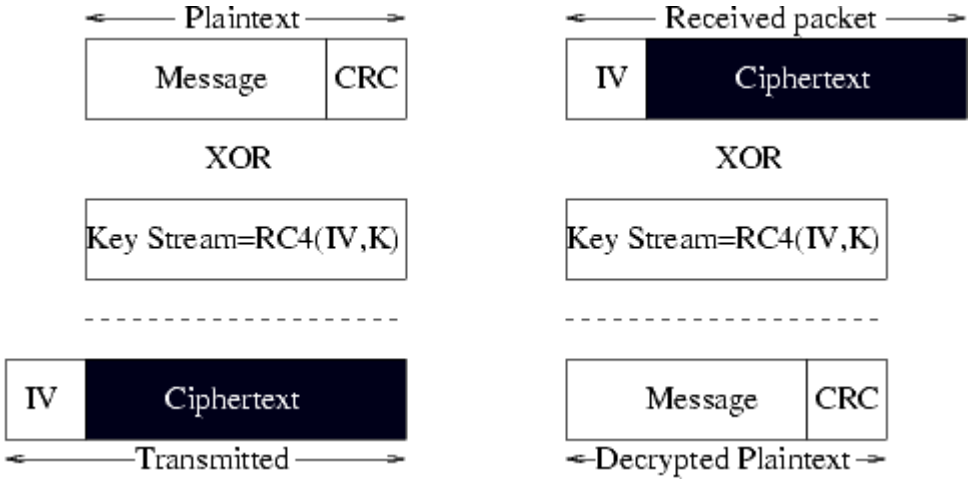

Fig 3.4: Encryption & Decryption on WEP

- Encryption

An IV is chosen on a per-packet basis and is sent along with the Ethernet header.

P = <M,c(M)>
K = RC4(IV,k)

C = P⊕K
where
M : Message to be sent; contains all layers upto the network layer
P : Plaintext
C : Cipher text transmitted over the air

- Decryption

The IV is extracted from the header and is used to find the K.
P'=C⊕K = <M',(c(M))'>

It is checked if
c(M')=(c(M))' and the plaintext, P' is accepted.

4.Known Attacks on WEP

WEP is considered to be very vulnerable to attackers. Any attacker sitting in the parking lot of a building can attack the building's WLAN security. This is unlike the wired case whereby the attacker needs a physical access to the wires. The following known attacks have been employed on WEP.

Type of Attacks

The following known attacks are known to be effective:

- Passive Attacks

  1 Dictionary based attacks
  2 Cracking the WEP key

- Active attacks

  1 Authentication Spoofing
  2 Message Injection
  3 Message Modification
  4 Message Decryption
  5 Man in the Middle Attack

As with other networks, the active attacks are riskier but provide greater powers to the attacker.

Passive Attacks	Active attacks
No risk involved	Riskier
No need to be the part of networks, because the WLAN cards support monitor mode, whereby one can listen to the communication without being a part of the network	The attacker has to first get into the network, before doing damages
The attacker can only listen to whatever is going on. He can not fiddle with the network	The attacker can interrupt, hijack and control the network at his will

Table 4.1. Passive vs. Active attacks

Decryption Dictionaries

The attacker passively sniffs every packet of the victim. He keeps storing the ciphertext along with the corresponding IV. Whenever the same IV repeats, he has two ciphertexts for the corresponding IV. As shown in the figure he has $C_{31,0}$ and $C_{31,1}$ for K_{31}

$C_{31,1} \oplus C_{31,0} = P_{31,1} \oplus P_{31,0}$

Using classical techniques it is possible to find a and b from a ⊕ b. Thus the attacker can get the knowledge of $P_{31,0}$,$P_{31,1}$ and K_{31} provided he has patience and resources to do it.

IV	Ciphertext
IV0	C0, 1
....	....
IV31	C0,31
....	....
IVN	C0,N

Table 4.2. A Decryption Dictionary

3.3 Cracking the WEP key (The working of Airsnort)

This passive attack is used to find the secret key, k. The attack is based on the premise that some weak IVs exist (Fluhrer et. al., 2), i.e. they reveal information of a byte x of k. The following facts/assumptions are used:

- The first byte of plaintext is known, it happens to be 0xAA for ARP and IP packets. We thus know the first byte K1 of the key stream K.
- K1 is enough to find the byte x of k.
- All the bytes of k prior to x have been deciphered correctly.
- The probability of finding byte x of k correctly is more than 0.05.

We illustrate here, with an example, the working of the attack:

1. We take a packet and keep its IV.
2. There can be two cases (Function classify of crack.c of Airsnort, 5)
    - If it is not a weak IV we dump it.
    - If it is a weak IV, we find that it helps us in finding 6th byte of k
3. We calculate the value of 6th byte (Function key Guess of it RC4.c of Airsnort, 5). We find out that this weak IV w.r.t 6th byte of k calculates k_6 to 0x67. We keep this Value of k_6 in a table (because the calculated value 0x67 may be wrong).

4 Such a table keeps filling. After sufficient entries, we find that the calculated value 0x67 of k_6 is correct because it occurred the maximum times.

5 After finding all the bytes of k, we make a try on all the packets, used above, by

decrypting them and checking whether indeed, CRC(M) is consistent for all of them.(This step is same as the decryption method described earlier)

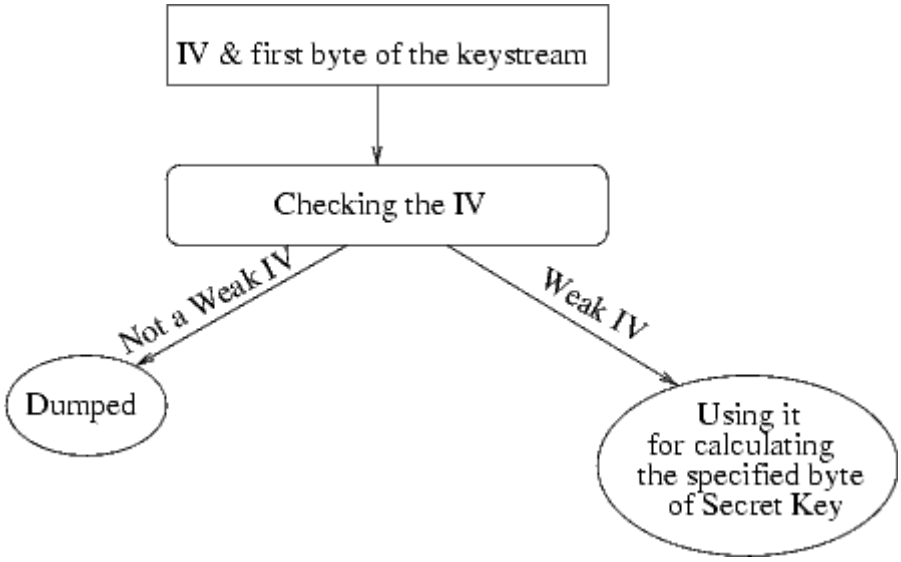

Fig 4.1: Working of Airsnort

Byte No. of k	Value	Value	Value	Value	Value	Value
....	....	....	....	....	....	....
6	0x67	0xab	0x37	0x67	0x67	0x20
....	....	....	....	....	....	....

Table 4.3. Working of Airsnort

The actual number of packets needed to crack the WEP key was not checked by us ,but reports say that it can be done in a matter of a few hours for 40-bit secret key and a matter of days for 104-bit secret key.

Message Modification

This active attack is used to change a particular part of the message M that is known to the attacker, along with its position in the packet. This field can be an email ID, HTML form.

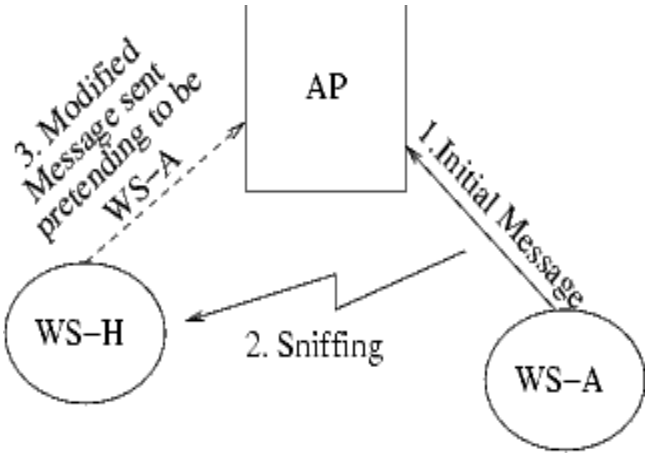

Fig 4.2: Message Modification

The attacker doesn't need to have the knowledge of key stream K or the secret key k for the attack. The attack is based on the fact that CRC(M) is an unkeyed function of M

Message Injection

The attack assumes that the attacker has a pair of K, IV. This pair can be reused over and over again without arousing suspicions, because there is no mechanism to check continuous repetition of IVs. Again the fact that CRC (M) is an unkeyed function of M.

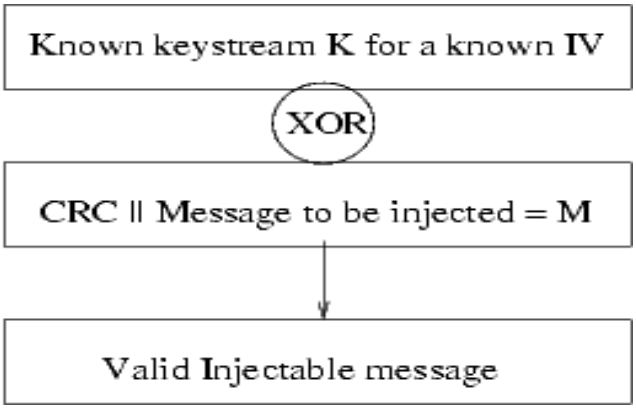

Fig 4.3: Message Injection

Authentication Spoofing

This attack is another form of Message Injection. By sniffing the shared key authentication process, the attacker knows a pair of Plaintext (Random Challenge) and Cipher text (Challenge Response) and the corresponding IV. Thus he knows the required <IV, K> pair. This pair can be used for authentication purposes.

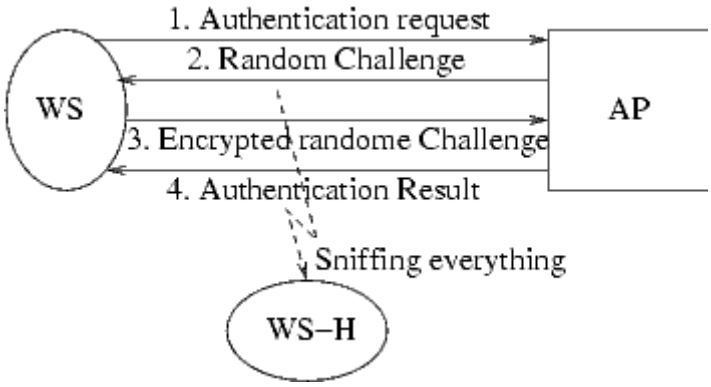

Fig 4.4: Authentication Spoofing

Message Decryption

There are two methods of decrypting the message by active attacks.

1. IP Redirection
2. Reaction Attack

- **IP Redirection**

This attack is an extension to message modification. The attacker modifies the destination IP in the IP header of the packet. By doing this, the attacker sends a packet from WEP encrypted zone to *No WEP Zone*, where he holds a machine.

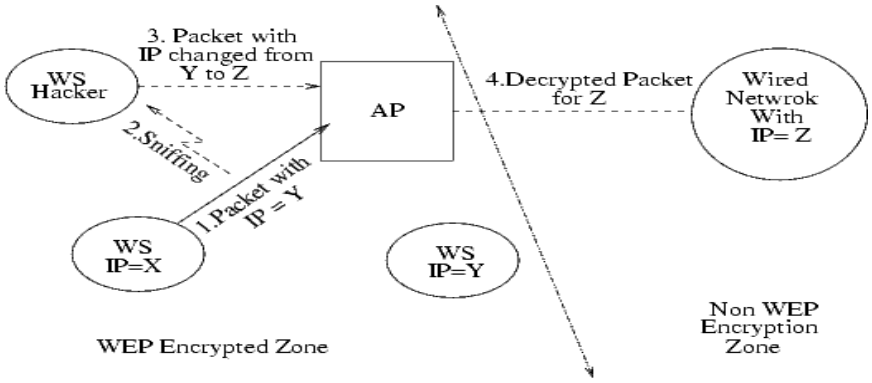

Fig 4.5: IP Redirection

To do this he has to make changes in the IP Header Checksum. In most cases the initial IP Checksum is not known although the attacker is assumed to have the initial destination IP address. So the attacker keeps sending packets with various values of checksum till he gets the packet across to his machine in *No WEP Zone*.

We did a simulation of this attack. The number of packets required, as a function of initial and final destination IPs, before getting a hit is open for interpretation.

- **Reaction Attack**

This attack only works for TCP Packets.

If TCP checksum is valid w.r.t. to the checksum, an ack is sent, otherwise the packet is dropped silently. This attack is based on the receiver's willingness to decrypt arbitrary cipher text and feed them to another component of the system that leaks a tiny bit of information about it's inputs. The attack is rightly called reaction attack as it works by monitoring the recipient's reaction to our forgeries.

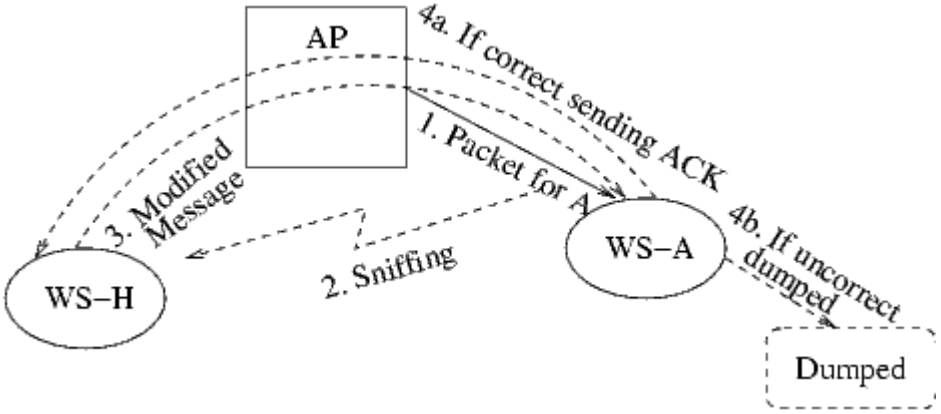

Fig 4.6: Reaction Attack

We have coded a simulation that verifies the property of TCP checksum that if bits P_i and P_{i+16} are complements of each other then putting complemented values into each, P_i and P_{i+16} doesn't affect the TCP checksum. Thus, the attack works in following fashion:

1. Take complements of C_i and C_{i+16}.

2. Make appropriate changes in the CRC checksum (this is not to be confused with the IP or TCP checksums) of message, CRC (M), and send the packet to the recipient.

3. There are two cases:
    1. ACK received: P_i and P_{i+16}} were complements of each other.
    2. No ACK: P_i and P_{i+16} were same.

We didn't test the actual effectiveness of this attack.

Man in the Middle Attack

This is a standard attack employed on all sorts of networks. In WLANs, the attack works in the following fashion:

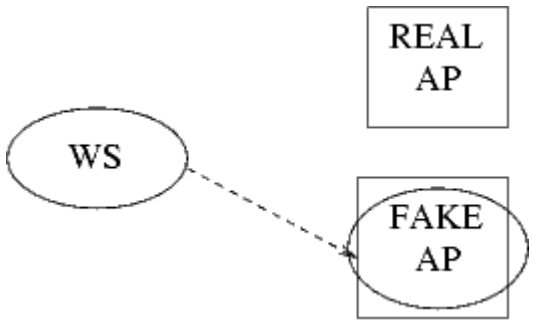

Fig 4.7: Man in the Middle

Steps in Man in Middle attack:

1. The attacker sets up a fake AP near to existing AP using a WS to masquerade network logons.
2. The user connects, in error, to the fake AP, and enters username and password.
3. The intruder collects data and informs user of incorrect password, then sleeps for five minutes, and successfully logs on to the real AP.

Tools available for attacking WLANs

These are few of the tools that are available for attacking the WLANs:

1. Airsnort (Linux) - cracks the WEP key.
2. WEPCrack (Linux) - cracks the WEP key.
3. NetStumbler (Windows) - finds the network parameters like, SSID, Channels, MAC Addresses, Type of Encryption used, Vendor of the card, tells the default secret key of the vendor can be used with a GPS for locating APs.
4. Kismet (Linux) - a WLAN sniffer
5. Thc-Wardrive (Linux) - for war driving
6. dsniff (Linux) - counterpart of NetStumbler
7. dstumbler (FreeBSD) - counterpart of NetStumbler

Summary of 802.11 vulnerabilities

The following 802.11 vulnerabilities come out on the basis of the known attacks

- SSID is required for associating a WS to an AP, and it is in the beacon frame. So, anyone can get it easily.
- IV size is very small.
- Many vendors increase the IVs in a linear fashion(0,1,2,3..)
- An IV that has occurred before is bound to occur after 2^{24} times, and infact after 5000 packets due to birthday paradox. This infact make the dictionary attack possible, because this translates to keeping a data of 2^{24}* 1500 = 16 GB.
- The strength of stream ciphers is based on the fact that a same seed never repeats, while the contrary has been described in the above point.
- Despite knowing that a secret key should be changed frequently, no known mechanisms have come for good key management.
- Only four secret keys are generally used in a network simultaneously, that too, most people don't change them from the default key provided by the vendor.
- CRC(M) is an unkeyed function of M, message.
- In the next chapter, we have recommended ACLs, but even MAC address spoofing can fool them.

5. Countermeasures

If there are vulnerabilities, then there are their countermeasures also, which cannot overcome them fully but can protect to a great extent.

Here are few countermeasures, which can help a lot in retaining security of WLAN.

- Do not trust WLAN and work under the coverage of a VPN (Virtual Private Networks).
- Maintain a good key management system, which changes the key before the sufficient no of packets required for cracking the key are transmitted.
- Increasing the bit length of IV and secret key is also a partial solution.
- Use of strong algorithm like AES
- Making the checksum of the message a keyed function, using algorithms like HMAC: keyed Hashing.
- **Configuring AP for allowing only few MAC addresses, which are there in his Access Control Lists (ACLs).**
- **Define the ACL depending upon Signal strength.**
- One must take care of the physical security also. You should take care that no unauthorized person gets access of your laptop or any Work Station, which is in the network because he can just copy the secret key.
- Enable RADIUS or Kerberos authentication for workstation to Access Point.
- Enable IPSec or Application level encryption for secure data communications

5.1 Fake Access points or Honey Pots.

Honey pots are devices placed on the periphery of a network for luring attackers to compromise them. By making attackers send their energy and resources on honey pots, effectively the real network is protected. Wireless honeypots consist of devices that transmit fake beacon frames. These devices emulate hundreds of fake access points, this results that the attacker is confused and tries to connect to any one of the fake access points. The attacker activity can be logged and studied. This also protects the network from attackers by hiding the network behind a mask.

5.2 Wireless Network Auditing

Wireless network auditing is an important part of WLAN security policy. The network needs to be regularly audited for **rouge hardware.** In this method the network is scanned and mapped for all access points and WLAN nodes. Then this is compared with previous network map. Commonly available network mapping tools like **netstumbler** and **wavelan-tool** can be used to do this.

Specialized tools such as Airsnort can be used for WEP cracking and auditing the network for weak keys, key reuse and WEP security settings. These methods include the same tests as those carried out by hackers for breaking into the network.

6. Future of Wireless LAN Security

6.1 Advanced encryption Standard (AES)

Advanced Encryption Standard is gaining acceptance as appropriate replacement for RC4 algorithm in WEP. AES uses the Rijandale Algorithm and supports the following key lengths

- 128 bit
- 192 bit
- 256 bit

AES is considered to be un-crackable by most Cryptographers. NIST has chosen AES for Federal Information Processing Standard (FIPS). In order to improve wireless LAN security the 802.11i is considering inclusion of AES in WEPv2.

6.1 Temporal Key Integrity Protocol (TKIP)

The temporal key integrity protocol (TKIP), initially referred to as WEP2, is an interim solution that fixes the key reuse problem of WEP, that is, periodically using the same key to encrypt data. The TKIP process begins with a 128-bit "temporal key" shared among clients and access points. TKIP combines the temporal key with the client's MAC address and then adds a relatively large 16-octet initialization vector to produce the key that will encrypt the data. This procedure ensures that each station uses different key streams to encrypt the data. TKIP also prevents the passive snooping attack by hashing the IV.

TKIP uses RC4 to perform the encryption, which is the same as WEP. A major difference from WEP, however, is that TKIP changes temporal keys every 10,000 packets. This provides a dynamic distribution method that significantly enhances the security of the network.

An advantage of using TKIP is that companies having existing WEP-based access points and radio NICs can upgrade to TKIP through relatively simple firmware patches. In addition, WEP-only equipment will still interoperate with TKIP-enabled devices using WEP. TKIP is a temporary solution, and most experts believe that stronger encryption is still needed

6.2 802.1X and Extensible Authentication Protocol

Combined with an authentication protocol, such as EAP-TLS, LEAP, or EAP-TTLS, IEEE 802.1X provides port-based access control and mutual authentication between clients and access points via an authentication server. The use of digital certificates makes this process very effective. 802.1X also provides a method for distributing encryption keys dynamically to wireless LAN devices, which solves the key reuse problem found in the current version of 802.11.

Initial 802.1X communications begins with an unauthenticated supplicant (i.e., client device) attempting to connect with an authenticator (i.e., 802.11 access point). The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (e.g., RADIUS). Once authenticated, the access point opens the client's port for other types of traffic.

7. Conclusion

Wireless LAN security has a long way to go. Current Implementation of WEP has proved to be flawed. Further initiatives to come up with a standard that is robust and provides adequate security are urgently needed. The 802.1x and EAP are just mid points in a long journey. Till new security standard for WLAN comes up third party and proprietary methods need to be implemented.

8.

References

1. L.M.S.C. OF THE IEEE COMPUTER SOCIETY. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ANSI/IEEE std. 802.11, 1999 edition.

2. Fluhrer, Mantin, Shamir. Weakness in the key-scheduling algorithm of RC4.

3. Stubblefield, Ioannidis, Rubin. Using the Fluhrer, Mantin and Shamir attack to break WEP.

4. Borisov, Goldberg, Wagner. Intercepting Mobile communications: The Insecurity of 802.11 - Draft.

5. http://airsnort.shmoo.com

About the Authors

Dr. S. A. Vetha Manickam, Head of Technology

S. A. Vetha Manickam holds a PhD degree in Scientific Computing and Numerical Analysis from Indian Institute of Technology, Bombay. He has a Masters in Applied Mathematics from Anna University, Chennai, where his dissertation was in "Object Oriented Methodologies". He was a Fellow of National Board for Higher Mathematics (NBHM), Department of Atomic Energy (DAE), India during the doctoral and post doctoral degree. Dr. Manickam has extensive experience in implementing e Security for organizations and defining the Information Risk Management Policies. He has been doing secure code auditing for many banking applications. He has also been involved in development of cryptographic algorithms and PKI products for authentication, confidentiality, integrity and Digital Signature. He is also involved in cryptanalysis for mobile and Wireless LAN encryption algorithms. He has spearheaded development teams in iKey integration, desktop security development, vulnerability scanner development and incorporation of Digital Signature for the Enterprise solutions.

Sangram S. Gayal, Information Security Consultant

Sangram S. Gayal is Bachelor of Engineering in Electronics and Telecommunications from Government College of Engineering, Aurangabad. He currently is an Information Security Consultant with Network Security Solutions India Ltd. and Associate researcher at Center for Information and Network Security, University of Pune. He currently is researching on wireless LAN vulnerabilities and countermeasures.