Seminar Nasional Aplikasi Teknologi Informasi 2006 (SNATI 2006) *ISSN: 1907-5022*
Yogyakarta, 17 Juni 2006

SECURITY IN WIRELESS LAN ATTACKS AND COUNTERMEASURES

Rahmalia Syahputri, Muhammad Said Hasibuan
Teknik Informatika, STMIK Darmajaya
Jln. Za Pagar Alam No 93 A Bandar Lampung
E-mail: lia_juga@yahoo.com, saidmkom@gmail.com

ABSTRACT

Wireless LANs offer many advantages in its utilization. Flexibility, mobility, and can be implemented by individuals or industries, are a little example from that. Since the security standards SSID, WEP and MAC address filtering that implemented in 802.11 known has vulnerabilities, security is become the major weakness of wireless LANs. Masquerading, man-in-the middle attack, and denial of service are examples of attack which can happen in wireless LANs. New security standards are now under development and will be implemented in the new wireless LANs 802.11i, namely TKIP and AES. Booth these new standards are expected to cover the security hole. This report analysing various attacks in wireless LANs which are caused by the vulnerabilities of security features, and the possibility of countermeasures from the attacks.

Keywords: *wireless LANs, security, WEP, MAC address, authentication, attack, TKIP, AES.*

1. Background

Wireless local area networks are LANs which use wireless transmission medium (1). Many of the technologies and standards for wireless LANs were developed in the 1990s, but the major wireless LAN used today is the IEEE 802.11, more commonly known as “Wi-Fi" (Edney et al, 2004).

Today, many individuals, organizations, and companies implement wireless LANs in various locations such as homes and businesses. The primary reason for using LANs is that wireless LANs are very easy to install, as there is no necessary to wire workstations into a specific space. The ease of installation makes wireless LANs inherently flexible, if a workstation must be moved, for instance, it can be done easily without additional wiring, cable drops or reconfiguration of the networks. Another advantage is its portability, for example, if a company moves to a new location, the wireless system is much easier to move as it not necessary to disconnect the wiring system which snakes throughout the building, thus making wireless make more cost efficient. (3).

Although wireless LAN offers many advantages, it does however introduce some security issues. For example, attackers can modify or steal the data through ‘hacking’. This creates a dangerous situation as much of the data sent over the internet contains sensitive information. In this report, the current security issues in wireless LANs and the possibility of countermeasures will be discussed and recommendations made to help overcome these problems.

2. Wireless LANs: A Brief Description

In a wireless LAN, network users use a wireless adapter or wireless Network interface Card (NIC) to connect to the network and communicate with other computers. Wireless LAN also have devices called access points that are stand-alone transceiver that connect wireless clients to a wireless LAN and act as hubs or routers. (McCullough, 2004)

Wireless LANs configurations are divided into two different modes: infrastructure mode and ad hoc mode. The Infrastructure mode (Extended Service Set, ESS) is need an access point to connect all clients to the wireless LANs, Generally access point connected to wired LAN (see figure 1). In ad hoc mode (Independent Basic service Set, IBSS), each client communications directly with other clients within the network, (see figure 2). Ad hoc mode is used to share a file in a short duration time.

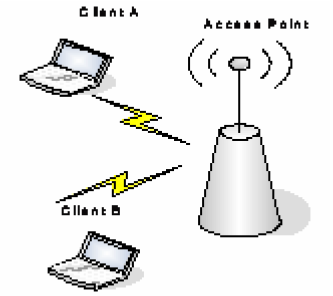

Figure 1. Infrastructure Mode
Source: Your 802.11 Wireless Network has No Clothes (Arbaugh et all, 2001)

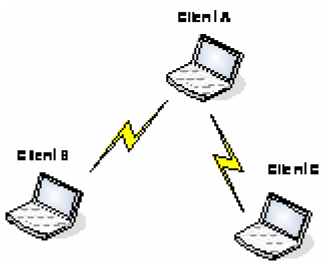

Figure 2. Ad Hoc Mode
Source: Your 802.11 Wireless Network has No Clothes (Arbaugh, et. all, 2001)

802.11 Standards

IEEE has specified wireless LAN standards, some of which are summarized below:

1. *IEEE 802.11b*
   802.11b were developed in 1997 and were the first 802.11x protocols introduced (McCullough, 2004). 802.11b devices operate in the 2.4 GHz radio band, with a maximum capacity of 11 Mbps.
2. *IEEE 802.11a*
   802.11a operates in the 5GHz band with 54 Mbps maximum capacity, almost five times faster than the maximum capacity of 802.11b.
3. *IEEE 802.11g*
   802.11g, or wireless G, is the newest 802.11x physical layer standard, operates in the 2.4 GHz band. The devices for 802.11b and 802.11g can operate on the same wireless network.

This table below shows comparisons between IEEE 802.11b, 802.11g, and 802.11a

Table 1. Comparison Of Wireless Lan Standard

Characteristic	***802.11b***	***802.11g***	***802.11a***
Spectrum type	2.4 GHz	2.4 GHz	5.2 GHz
Spectrum congestion	High	High	Low
Radio type	DSSS [1]	OFDM[2]	OFDM[2]
Performance	11 Mbps	54 Mbps	54 Mbps
Maximum throughput	6 Mbps	22 Mbps	30 – 35 Mbps
Cost	Low	Low	Moderate
Non-overlapping channels	3	3	12
Coverage	100 meters	100 meters	50 meters

[1] Direct sequence spread spectrum (DSSS)
[2] Orthogonal frequency-division multiplexing
Source: Deploying secure Wireless Networks, Intel Information Technology, *White Paper*, May 2003

3. Masquerading

The attacker hijacks or pretends to be a legitimate device to establish a connection and then takes over the connection by masquerading as that station, the first thing to do is sniff network traffic and wait for someone to authenticate the access point and capture the authentication data (see figure 3 and 4).

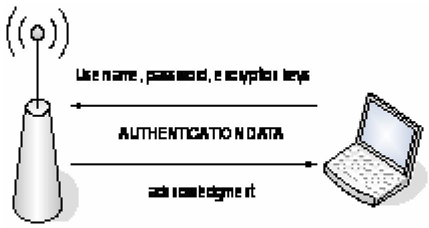

Figure 3. Authenticating With An Access Point

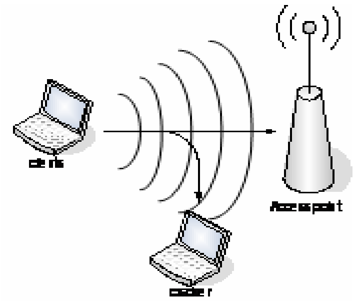

Figure 4. Sniffing Network Traffic
Source: Caution! Wireless Networking: Preventing a Data Disaster (McCullough--- 2004)

The attacker inserts a command that forces the target server (or access point) to re-establish the connection and then hijacks the session by authenticating with the sequence and acknowledgement numbers that has been sniffed (see figure 5 and 6).

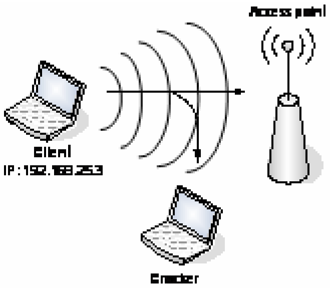

Figure 5. Sniffing A Valid Ip Address And Intercept That User's Authentication Data

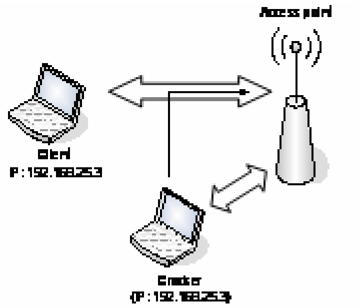

Figure 6. Session Hijacking
Source: Caution! Wireless Networking: Preventing a Data Disaster (McCullough--- 2004)

An attacker can imitate the access point and send a legitimate client a disassociate frame and disassociate frame which will disconnects the client from the wireless LAN. If this situation happens, the attacker can spoof the client's MAC address and take over the user's session. The session remains open because AP did not send the disassociation message, but the attacker did. The original user is still connected and authenticated, as long as the AP is concerned, see figure 7 and 8.

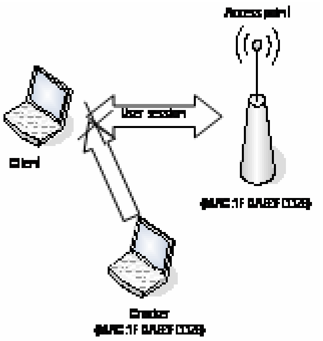

Figure 7. Attacker Spoofing Mac Address

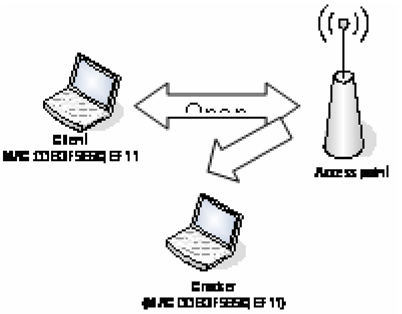

Figure 8. Exploiting A Race Condition
Source: Caution! Wireless Networking: Preventing a Data Disaster (McCullough--- 2004)

This type of attack exploits a race condition. In this situation, the attacker forces the legitimate user to disconnect and then races to take over the user's session, and if the attacker can spoof the client's MAC address before the client gain authenticates, then the attacker can hijack the session and take over until the session time out.

Man-in-the-middle Attack (Modification)

Because the management frame lack any integrity protection, establishing a man in the middle with IEEE 802.11 based networks is easy (Edney et al, 2004). Man in the middle attacks are possible because there are no integrity guarantees provided at the link layer (layer 2) and MAC address is easily copied.

To create a man in the middle attack, the process is almost identical to a masquerading attack, first the attacker will issue a deauthentication message to the client after the client already has connected to an AP. This thing will make the client associate with that AP and look for another AP or reassociate with the old AP. At the same time, the attacker will build an illegal AP with same ESSID and MAC address as the legal AP. The client will associate with the illegal AP because the target is denied service with the legal AP by attacker's deauthentication messages.

The difference between man-in-the middle attack and a masquerading attack is the former type attack will not shut down communication between client and an AP after target associates with illegal AP, but will stand in the middle between client and AP to take control, see figure 9.

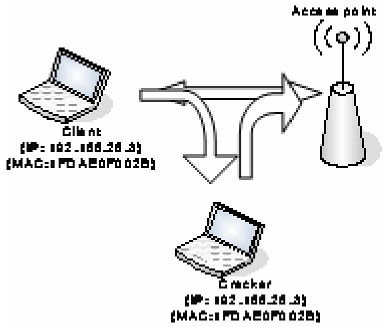

Figure 9. Man-In-The-Middle Attack
Source: Caution! Wireless Networking: Preventing a Data Disaster (McCullough--- 2004)

Denial of Service (DoS)

This type of attack can deny not only client but also attacker itself from connection. There are two types of denial of service. First is denial of service in Radio Frequency (RF) and the second is in layer 2 (MAC layer).

In RF attack, the attacker uses a wireless transmitter to broadcast interference on the same frequency channel used by AP, drowning it out and creating so much radio frequency noise. This would mean that wireless LANs devices in the area can't operate.

In layer 2 denial of service attacker has several choices. First, when the attacker can see the AP when that AP association with the station. attacker simply forges a disassociation or deauthentication frame and sends it either the AP or client. The AP or the client will think that the station wants to leave or the AP no longer can service the client), grants the request and closes the association. Disassociation or deauthentication frame permits the attacker to use the broadcast MAC address as the target.

The second choice is the attacker sends a forged association-request message with the target MAC address to an AP on the same wired LAN. The AP that receives the association request approves and sends out a layer 2 update frame to the wired LAN. The router or switch begins forwarding traffic to the AP that sent the layer 2 update, and the actual station no longer receives any traffic.

Another method of denial of service is denying service to a group. Attacker gives thousands of tasks network traffic to AP, preventing legitimate users from connecting to the network. The AP will reboot or no longer permits new stations to associate. In the other word, both attacker and client blocked out by AP, see figure 9.

Countermeasures

There are several security solutions to protect wireless LAN from attack, some of describe as follow:

- *Temporal Key Integrity Protocol (TKIP)*

TKIP exist for one reason that is to allow WEP system to be up graded to be secure (Edney, et, all, 2004). TKIP just upgrades WEP system but does not change it all, this is means TKIP will be implemented in the hardware that already uses WEP (RC4 algorithm), TKIP addressed to solve several problems in WEP, where the weaknesses of WEP are already mention in section labelled wired equivalent privacy.

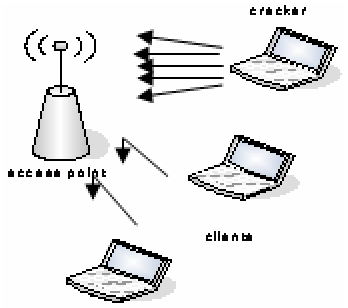

Figure 9. A Denial Of Service Attack
Source: Caution! Wireless Networking: Preventing a Data Disaster (McCullough, 2004)

- *Message Integrity*

When attackers can easily modify a message, it means the system implemented is weak. Message Integrity Code (MIC) is a combination of all bytes in the messages to produce check value. MIC is computed by a special nonreversible process and secret key combination, it can make an attacker will not easy to recompute the MIC which is send along the message, only legal receiver can recompute and check the result. In other word, MIC can be used to detect tempering message.

However, to implement a straight MIC is difficult. Generally, the microprocessor inside the MAC chip in the most Wi-Fi card does not have any fast multiplication. To solve this problem, TKIP uses method called Michael.

Unfortunately, Michael is open to brute force attack. The concept of countermeasures can be used to solve this problem. The idea is when an attacker is detected, countermeasures will shut down all networks, therefore preventing the attacker repeated attempts.

4. Selection and Use

It is considered in IV that already implemented in WEP face several weaknesses, TKIP introduces several new rules in the way using the IV to increase security, such as increasing size of IV, secondary role in IV, and IV is constructed to avoid weak keys.

The IV length is considered to short, by adding 32 bits extra in the original 24 bits will give 56 bits. From 56 bits of new IV, only 48 bits will used, the rest of the bit will used to avoid weak keys. With this new size attacker would need thousand of year to completely break the IV space. WEP also facing had no protection to against replay attack. By using TKIP Sequence Counter (TSC) mechanism, TKIP try to avoid that attack.

Per-Packet Key Mixing

In the Wired Equivalent Privacy, key is used for everything. Per-packet key mixing derive a specific key for each and every packet. It also avoids if two clients are connected to the same AP to decrypt traffic each other. (Edney et al, 2004)

Vulnerabilities of TKIP

In TKIP, even the weak key vulnerability has been immigrated by key-mixing approach, the fundamental weakness in the first bytes of the RC4 key stream is still there and can also be the weakness of TKIP. (Edney et al, 2004).

Advanced Encryption Standard (AES)

AES is a block chipper and works using mathematical and logical operations based on Rijndael algorithm. The method combines a key and 128 bit block of data (unencrypted) to create a block of different data (encrypted) (Edney et al, 2004**).**

In 802.11i also known as Robust Network Security (RSN), the security protocol build in AES is called Counter Mode-Cipher Block Chaining MAC Protocol (CCMP). CCMP defines a set of rules that use the AES block chipper to enable the encryption and protection of IEEE 802.11 frames of data at the MPDU level (Edney, 2004).

How CCMP works in RSN

CCMP algorithm will process MAC Protocol Data Unit (MPDU) to generate a new encrypted MPDU. However, CCMP not only encrypt MPDU, and also add extra fields to make it 16 bytes longer than original MPDU encrypted. MIC will protect The MAC header and CCMP header, because both of these headers are not encrypted and will be grouped together to form authentication data.

The CCMP has two purposes. First, to provide the 48-bit packet number with replay protection. Second, it tells the receiver which group key has been used.

Summary

Since the explosion of utilizing wireless LAN in companies, industries, and by individuals, security has now become a real issue, even wireless LAN provides security features, such as Service Set Identifier (SSID), Wired Equivalency Privacy (WEP), MAC address filtering, but each of the standards have weaknesses.

SSID is vulnerable because it is sent periodically using beacon by an AP. Attackers will easy sniff it and gain entry to the AP. MAC address filtering also has weaknesses, because MAC address is sent in plaintext and everybody can see it , it would mean MAC address can copied relatively easy by attackers.

The other standard is WEP and it is considered not strong enough to protect wireless LAN from attack. For instance, 24 bit Integrity Value (IV) length is realized too short and attacker can break it.

Authentication is the major problem in security, if one attacker can break it; the data sent trough wireless LAN is insecure. There are several attacks identifiable attack in wireless LAN, such as masquerading, man-in-the middle attack, and denial of service (DoS).

In the masquerading, the attacker pretends to be an AP to hijack the client and take over the session. There are similarities between masquerading and man-in-the middle attack process, the difference is that man in the middle does not shut down communication between client and AP. The attacker positions itself between client and AP. This means that all communication between both devices will pass the attacker first. Denial of Service attack is divided into two types, denial in radio frequency (RF) and in the MAC layer. This type of attack can deny not only client but also the attacker from AP.

Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) are two security standards which will be implemented in 802.11i in the future. TKIP will cover weaknesses in WEP. For instance, TKIP will add to the length of IV from 24 bits into 48 bits. AES, CCMP is built to enable the encryption and protection of IEEE 802.11 frames of data at the MPDU level.

5. Conclusion

In conclusion, wireless LANs is relatively easy to attack if wireless LANs users do not implement new securities standard and rely only on security features which now used in most wireless LANs .

Because of lack of SSID, MAC addresses filtering and WEP in wireless LANS, a number of attacks can be found, for instance, masquerading, man-in-the middle attack, and denial of service.

Migration to a new standards such as TKIP and AES are good choices, attacker will find it more difficult to break these standards.

6. Recommendations

Based on the discussion in the section labelled fact and discussion. Into order to avoid wireless LAN from attacks, wireless LANs users can not just depend on the security features now implemented in most Wi-Fi. Several securities can obviously be attacked and all the information becomes insecure, there are several recommendations for wireless LANs users to make wireless LANs secure:

1. If the wireless LANs device only uses SSID and MAC address filtering to protect the security, the users can implement WEP algorithm. Even WEP has several known vulnerabilities, but it is still better than disabling this standard.
2. When the device has already implement WEP algorithm, to increase security it can add TKIP**.**
3. For the strongest and long terms securities, users should change to the new devise thus allowing implementation of AES.

References

Arbaugh et al. (30th March 2001) *Your 802.11 Wireless Network has No Clothes*, Department of Computer Science, University of Maryland. http://www.cs.umd.edu/~waa/wireless.pdf, Accessed: December 16, 2005

Bhagyavati et al. (September 2004) *Wireless Security Techniques: An Overview*, Columbus State University, Telcordia Technologies, Inc. Accessed: December 12, 2005

Edney, Jon et al. (2004) *Real 802.11 Security Wi-Fi Protected Access and 802.11*, Boston, Addison-Wesley.

Intel Information Technology White Paper. May 2003, *Deploying Secure Wireless Networks: Intel's Strategies to Minimize WLAN Risk*. Intel Corp., http://developer.intel.com/design/network, Accessed: December 12, 2005

Intel Information Technology White Paper. February 2003, *Intel Building Blocks for Wireless LAN Security*. Intel Corp., http://developer.intel.com/design/network, Accessed: December 12, 2005

KING, Jason S. (22nd October 2001) *An IEEE 802.11 Wireless LAN Security White Paper*. U.S Department of Energy, Lawrence Livermore National Laboratory. University California. www.llnl.gov/asci/discom/ucl-id 147478.pdf Accessed: December 12, 2005

Kizza, Joseph Migga. (2005) *Computer Network Security*, United States of America. Springer Science+Bussines Media.

McCullough, Jack. (2004) *Caution! Wireless Networking: Preventing a Data Disaster*, Indianapolis, Wiley Publishing

Mehta, Princy C. April 2001)*Wired Equivalent Privacy Vulnerability.*, LevelOne Security Essential Track. As Part of GIAC Practical Repository. SANS Institute.www.giac.otg/certified_ptofessionals/practicals/gsec/0624.php, Accessed: December 12, 20065

Park, Joon S et al.(July 2003) S*ecurity Challenges and Countermeasures in WLANs*, School of Information Studies, Syracuse University.http://wirelessgrids.net/docs/CCCT03_Park_T387UH.pdf, Accessed: December 14, 2005

Park, Joon S et al. October 2003. *WLAN Security: Current and Future*, Syracuse University. IEEE Computer Society. ieeexplore.ieee.org/iel5/4236/27614/01232519.pdf, Accessed : December 14, 2005

Wells, Sam. December 2002. *802.11 WLAN Security – Choose Wisely!*, Bechtel Telecommunications Technical Journal. www.bechteltelecoms.com/docs/bttj_v1/Article11.pdf, Accessed: December 16, 2006

Wi-Fi Alliance. 6th February 2003. *Enterprise Solution for Wireless LAN*. www.wi-fi.net/OpenSection/pdf/Whitepaper_Wi-Fi_Enterprise2-6-03.pdf. Accessed: December 18, 2006.