A SOFWARE SOLUTION FOR DEFENDING AGAINST MAN-IN-THE-MIDDLE ATTACKS ON WLAN

Thuc N.D.[(1)] – Phu N.C.[(1)] – Bao T.N.[(2)] – Hai V.T.[(3)]

[(1)] University of Natural Sciences, VNU HCMC

[(2)] Pedagogical University of HCM City

[(3)] University of Texas at Dallas

Abstract: Wireless local area networks have become more and more popular. They have been installing by businesses of all types. The IEEE 802.11 standards were developed for WLAN. However, sources have shown that the new standards are flawed, allowing attackers to perpetrate attacks. Our works focus on the man-in-middle (MiM) attacks on WLAN. This paper presents a software solution – called AMiMA (Against Man-in-the-Middle Attacks), to defend against this type of attacks. In this solution, the "delayed password disclosure" technique is used for authentication phase, IPSec - VPN technique will be used for data exchange phase.

I. INTRODUCTION

Most wireless local area networks (WLANs) today are built on Wi-Fi technologies, i.e., those based on the IEEE 802.11 wireless standard. Due to security reasons, 802.11 employs the wired equivalent privacy (WEP) protocol [1]. WEP was intended to give the wireless data-link a level of security similar to that of naturally-built in wires and optical links. WEP's goals are to provide access control, data confidentiality and data integrity. It does this by using symmetric key mechanisms. With WEP, all devices must have entered into them by the network administrator with a secret WEP key. This is usually done manually. It is by now well known that WEP is extremely vulnerable and can not be counted on to defend against even casual attackers since there are scripts available online that can defeat WEP in a matter of minutes [2] [3] [4] [5].

While there are many proposed fixes for WEP [6] [7] [8], most of them are not applicable until the next generation of wireless hardware due to their increased computational requirements. In this paper, we present a software solution for WLAN security. Proposed solution meets security goals - access control, data confidentiality and data integrity; and requires limits upgrading of hardware of current systems. In this solution, the "delayed password disclosure" technique [9] is used for authentication phase, IPSec - VPN technique [10] is used for data exchange phase.

The remainder of paper is organized as follows. The next section overviews two techniques that have been used usually for man-in-middle (MiM) attacks on WLAN, thanks to one who learnt weak points of 802.11 that hackers can exploit. Section III then describes proposed solution for wireless security. Proposed solution has to meet security goals - access control, data confidentiality and data integrity and limits upgrading of hardware of current systems. Section IV analyzes the security of proposed solution and alse presents the efficiency of the solution comparing to current used solutions. The security is analyzed on capacity of solution for defending against MiM attacks and its efficiency is compared on criterions of security, speed and hardware using. The paper concludes in Section V.

II. MiM ATTACKS ON WLAN

II.1. Attack on ARP

Attack on ARP (Address Resolution Protocol) is a typical man-in-middle attack. This attack exploits the essential point of ARP that enables hackers can impersonate the computer that user want to communicate. Before the presenting of ARP attack, we recall here about Address Resolution Protocol.

II.1.1. Address Resolution Protocol

ARP is a mechanism that allows mapping IP address to Mac address. At the Data-Link and Physical layers, the computers communicate through MAC address instead of IP address, IP address is used only at logic layer.

For instance, if Computer A wants to know MAC address of Computer B, it sends an ARP packet (that contains request for IP address) in the form of BROADCASTING. When computer B receives this packet, it will match its IP value and IP value receiving from packet. If those values are the same, B will reply a packet which contains MAC address of B to A. A receives replying of B, A then store MAC address of B in ARP table (ARP cache) for using in next communication.

Note that this is not fixed address. Therefore, there are some entries of ARP will be out of date after a period.

Some operating systems allow one replaces entries in ARP cache during using even when they do not send ARP message in advance. This is the key point for ARP attack.

II.1.2. ARP Poison attack

The necessary condition of ARP attack is that the hacker must gain network access and knows information about IP, MAC of some of computers in the network. The scenario for ARP cache infection is as follows:

- Suppose that A and B are two computers that have IP and MAC address as the following:
  A (IP = 10.0.0.2, MAC = AA:AA:AA:AA:AA:AA)
  B (IP = 10.0.0.3, MAC = BB:BB:BB:BB:BB:BB)

  and the computer of the hacker has address

  H (IP = 10.0.0.4, MAC = HH:HH:HH:HH:HH:HH)
- H sends a reply ARP message to A says that IP: 10.0.0.3 has MAC address: HH:HH:HH:HH:HH:HH. At the time, ARP table of A will be IP = 10.0.0.3 – MAC = HH:HH:HH:HH:HH:HH.
- H also sends a reply ARP message to B says that IP: 10.0.0.2 has MAC address: HH:HH:HH:HH:HH:HH. At the time, ARP table of B will be IP = 10.0.0.2 – MAC = HH:HH:HH:HH:HH:HH.

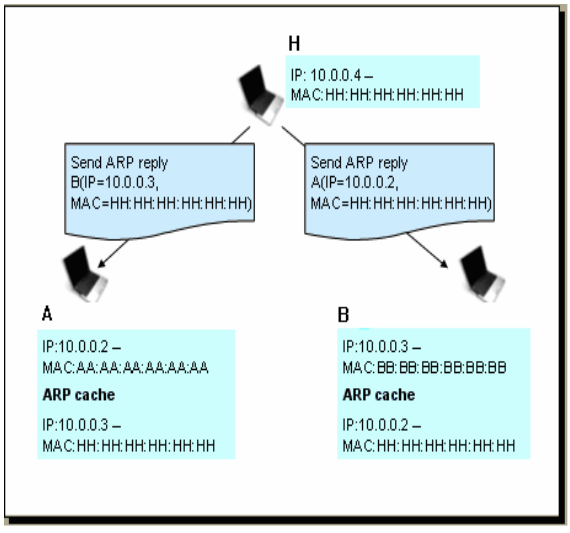

Figure 2.1: ARP cache defection

- When A wants to send a message to B, because MAC address of B in ARP table of A is HH:HH:HH:HH:HH:HH, A will send to H instead of B. H receives this message, processes it and sends to B.
- If B sends a message to A, process of attack is the same.
- Hence, H acts as a main-in-middle to receive and transmit messages between A and B. H can change messages before transmitting them to destination machine.

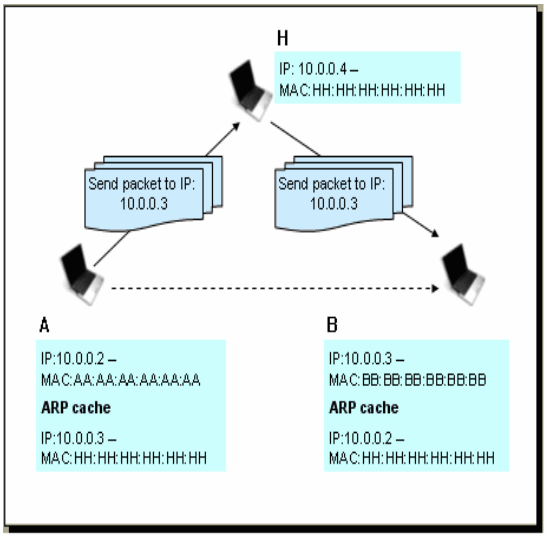

Figure 2.2: Attack on machine that is defected ARP cache

II.2. IP Spoofing

IP Spoofing relies on characteristics of WEP: WEP only protects data on the WLAN environment, i.e. WEP encrypts packets before transmitting and decrypts packets after the Access Point (AP) transmits data into Wired-LAN. Therefore, during the AP to Wired-LAN, the content of packets is in plaintext state, the attacker tries to redirect the IP destination of packets to the address that she can control and then she can easily read the content of packets.

Condition for the IP Spoofing to be success is that the hacker must modify the IP destination to which the packet is sent, and therefore that IP destination must be a computer which she can control.

Because RC4 use XOR keystream and plaintext, we can know position of IP in cipher. Let C(IP) is

cipher value of IP, P(IP) is plaintext value of IP. We have,

$$C(IP) = keystream(IP) \oplus P(IP)$$

And we knew C(IP) and P(IP), so

$$keystream(IP) = C(IP) \oplus P(IP),$$

this is defined in [4].

Then, the hacker replaces IP by another IP that she can control and packets would be transmitted to. This will be performed as follows:

$$Cnew(IP) = keystream(IP) + (new\ IP)$$

Because we had C(IP) and Cnew(IP), following [4], we can define number of changed bits when Cnew(IP) was changed to update ICV field of 802.1X data frame.

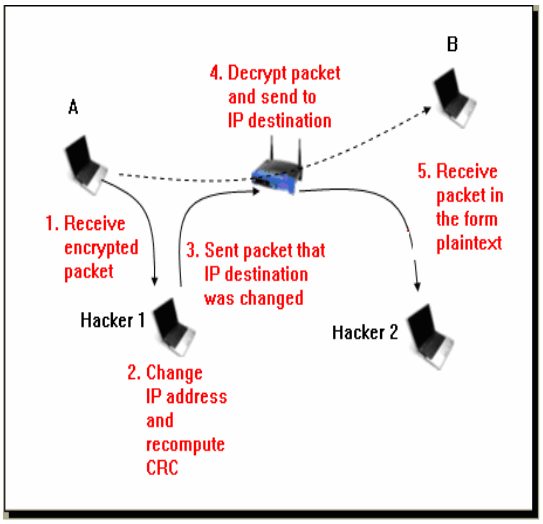

Figure 2.3: Attack by IP Spoofing

III. AMiMA – A SOLUTION FOR WLAN SECURITY

Although the 802.1X wireless standard specifies both the authentication services and encryption protocols, sources have demonstrated that they are severely flawed, leaving wireless communications open to several types of attacks [2] [3] [4] [5]. We have implemented a software solution for defending against man-in-middle attacks, called AMiMA.

III.1. WLAN with AMiMA

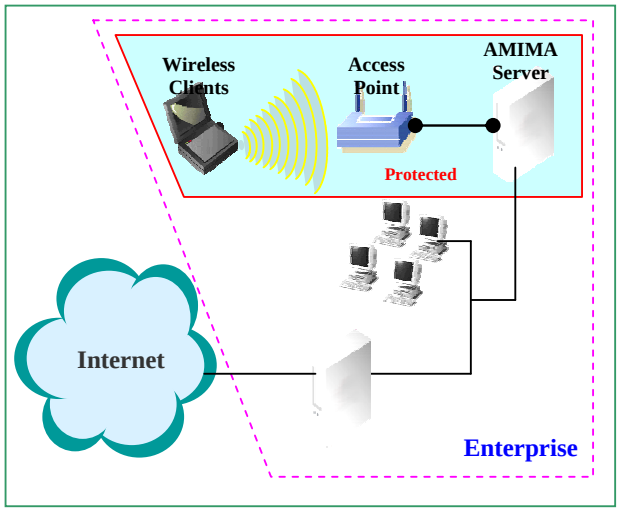

Figure 3.1: a WLAN model.

The organization of a typical WLAN is shown in Figure 3.1. The network includes personal computers, host computers and other devices that are connected to each other through cable; wireless computers or devices are joined into this wired-LAN through access points (APs).

In our model (Figure 3.2), WLAN will include wireless computers and devices that are joined into a wired-LAN through APs and AMiMA server. This creates a three-party system:

- **Supplicant**. User who wants to join the network.
- **Authenticator**. AP which controls access.
- **Authentication server**. AMiMA which makes authorization decisions.

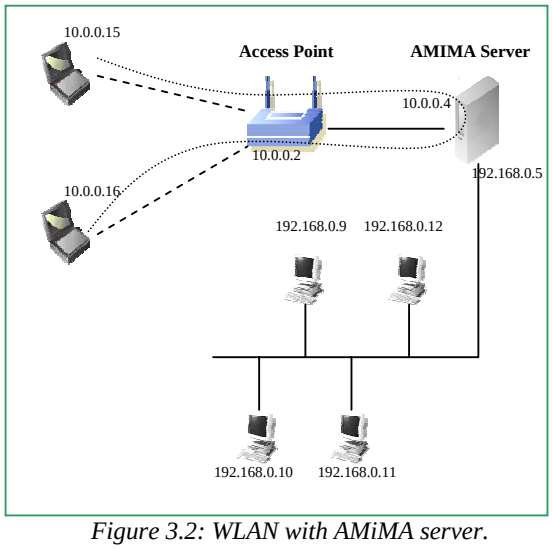

Figure 3.2: WLAN with AMiMA server.

AMiMA server provides basic services as follows:

- It plays as a RADIUS server which makes authorization decisions and exchanges session key to wireless devices based on EAP (Figure 3.3(a)).
- It plays as a VPN gateway which prevents casual eavesdropping (Figure 3.3(b)).

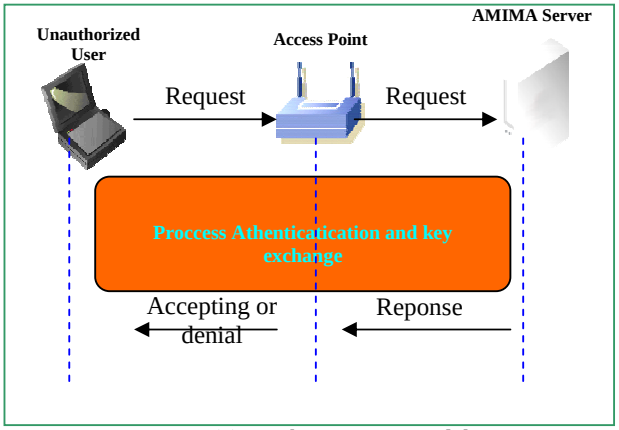

Figure 3.3(a): Authentication model.

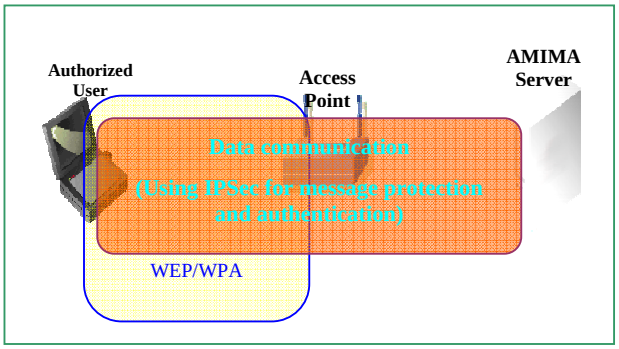

Figure 3.3 (b): Message protecting model.

III.2. Mechanism for WLAN protection

WLAN is protected by two layers: 802.1X and IPSec.

- AP will be configured so that it can use AMiMA server for authentication process based on EAP and WEP key using for data encryption of 802.1X.
- Wireless client will be installed a AMiMA client software and be configured two system parameters: one for AP (SSID, WEP key, type of authentication…) and the other for AMiMA server (AMiMA server address, encryption key, encryption algorithm…).
- Server will be installed AMiMA server software which provides authentication services and protections of data that are transmitted between wireless client and wired-LAN.

III.3. Processes of AMiMA system

First, when an unauthorized wireless client wants to join into network, it needs to send a request to AP.

When AP knows that the client is an unauthorized one, it sends this request to AMiMA server. Then the wireless client and AMiMA server will operate the authentication together. After this authentication process, AMiMA server will inform the result of process to AP.

If the process fails, AP will close the communication port and the wireless client is rejected. If the process is succeed, key exchange process will also be operated. Now, wireless client has the access right to the system and is ready to transmit data.

The process to transmit data from wireless client to LAN is operated as follows:

- Data are packed throught layers of TCP/IP.
- At the IP layer, packets will be encrypted by IPSec mechanism and will be passed to AMiMA server.
- Encrypted packets will be passed into 802.1X layer and be encrypted again by WEP to form frames. These will be transmitted to AP.
- AP receives these frames, decrypts them using WEP to recover the packets which were encrypted by AMiMA server.
- AP sends these packets to AMiMA server.
- AMiMA server receives these packets which were encrypted through IPSec, decrypts them and sends to destination address.

The process to transmit data from AMiMA server to wireless client is operated similarly: AMiMA uses IPSec to encrypt the packets and sends them to AP. AP uses WEP to encrypt these packets again and sends to wireless client. Wireless client receives these frames, uses WEP to decrypt and uses IPSec to decrypt again to recover data.

III.3. Authentication service

The system authorizes based on a RADIUS server (here it is AMiMA server) and exchanges authorized messages based on EAP.

RADIUS server provides each user an account which includes at least two entries: username and password.

Password will be transformed to a message digest by a one-way hash function H (in our system, we use SHA function). This message digest is secret.

Process of authentication is shown in Figure 3.4:

- **Step 1**. The username value is transformed to message digest by a hash function H. Station sends H(username) to authentication server in the form of EAPoL-Packet.
- **Step 2**. Authentication server (AS) sends a certificate to the station to confirm that it recognized the station. The certificate is created as follows:
  - AS looks for the password corresponding to H(username) in the account database of system.
  - AS then creates a mask corresponding to this password by:
    - Generating a matrix of 2xn, where n is the bit length of password.
    - If the first bit of the password is zero, the first row of the first column is selected; if it is one, the second row is selected. Similarly, the second bit of the password is represented in the second column, and so on.
    - Selecting a sequence of random that adds up to the value zero and writes in positions that correspond to the password of supplicant. AS then selects the other sequence of random – Ks – that add up to a number other than zero and writes in the other position of the mask. Now we have a certificate in the plaintext form - Certificate.
  - AS encrypts this Certificate by AES using key that is just the password of user: C_certificate = AES(Certificate)[password].
  - AS sends C_certificate to station.

Note that even if Certificate is sent in the form of plaintext, it is still very difficult for the eavesdropper to extract a correct sequence that adds up to the value zero corresponding with the password of user. Note also that there exist m (m > 0) sequences that add up to the value zero in the mask of Certificate. Therefore the eavesdropper must try m.2^n cases to find a correct password, while this operation is linearly for the legal user.

- **Step 3**. Station verifies the received C_certificate.
  - Station decrypts C_certificate using its password:

    Certificate = AES^{-1}(C_certificate)[password].
  - Station reads only the digits which were written in positions that correspond to the password and adds these together.
  - If the total is zero, supplicant reads in other positions of the sequence Ks.
  - Then Ks is encrypted:

    C_{Ks} = AES(Ks)[password].
  - Finally supplicant sends this C_{Ks} to AS.
- **Step 4**. AS verifies the received C_{Ks}.
  - AS decrypts this received C_{Ks}:

    Ks' = AES(Ks)[password].
  - If Ks' ≡ Ks then a session key for data exchange will be established based on the given function f.
  - AS informs the result of authentication to AP. Based on this result, AP makes a decision of permitting or refusing the right of the client to access into system.

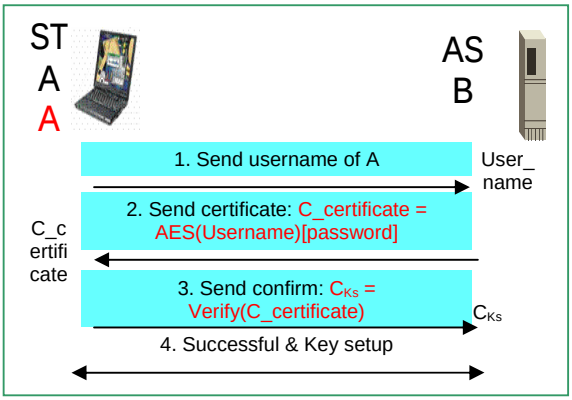

Figure 3.4: Mutual authentication between station and authentication server.

III.4. Casual eavesdropp prevention

As we present above, the proposed model uses IPSec technique to encrypt and to transmit message: origin message will be encrypted at IP layer, then be passed to 802.1X layer and be encrypted again (using WEP or WPA, depends on the support of devices). Therefore, the system can be installed as software without upgrading the hardware.

The input of encryption process is the packet of IP layer in TCP/IP model – called Payload. The encryption and decryption process are operated as follows:

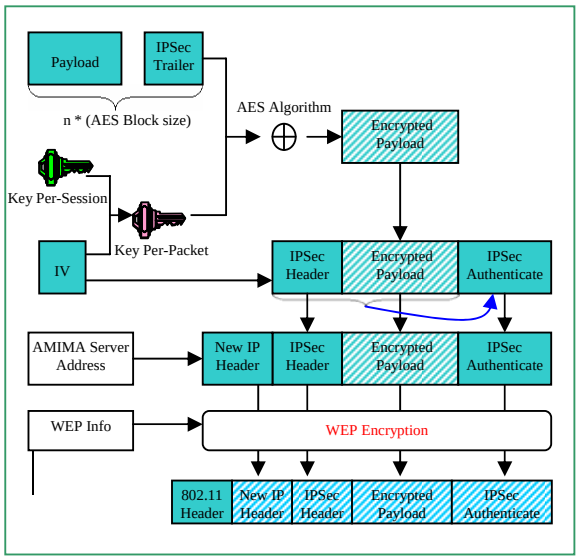

Figure 3.5: Message encryption.

III.4.1. Message encryption

Step 1: Inserting IPSec Trailer and creating encryption key for payload.

- Payload will be added IPSec Trailer at the back so that size of result – N, is a multiple of size bock – n, corresponding to the chosen encryption algorithm: N = mn, m > 0.
- System generates a random initialization vector (IV).
- Encryption key of IPSec for payload (Key Per-Packet) will be the combination of IV and Key Per-Session.

Step 2: Encrypting payload (IPSec Trailer has been added)

- Splitting Payload into m blocks.
- Using AES to encrypt these blocks.

Step 3: Inserting IPSec Header and IPSec Authenticate

- Inserting IPSec Header into the head of encrypted payload block.
- Creating MAC value of the payload that was inserted IPSec Header, using HMAC algorithm. This MAC value will use for payload integrity.
- Inserting MAC value into IPSec Authenticate and adding result into back of payload.

Step 4: Inserting new IP Header.

- Inserting a new IP Header into the head of packet so that the new IP destination is just the AMiMA server address.

Step 5: Passing packet to Physical layer for the 802.1X to encrypt again to form frames.

Step 6: Transmitting these frames to AP through radio wave.

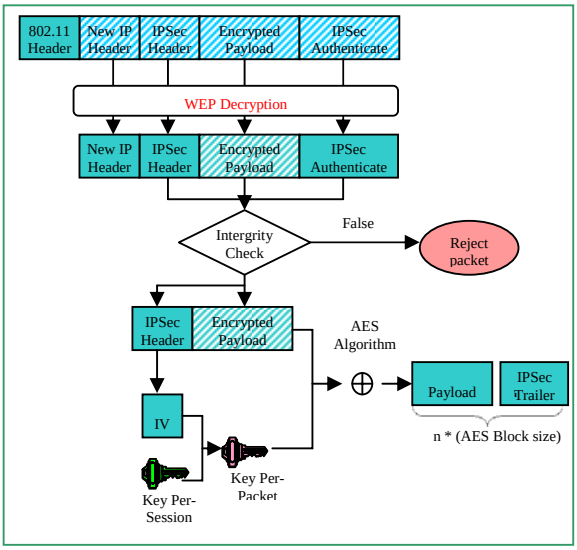

Figure 3.6: Message decryption.

III.4.2. Message decryption

Message decryption includes two phases: one is processed by AP and the other by AMiMA server.

Step 1: After receiving frames, AP decrypts them to packets which are packed by IPSec.

Step 2: AP sends this packet to AMiMA server.

Step 3:

- AMiMA server computes MAC value – MAC' – of IPSec Header and Payload using the given hash function h.
- If MAC' != MAC, where MAC is the MAC value that is in IPSec Authenticate then this packet is rejected.

Step 4: Decrypting packet

- Taking IV value from IPSec Header.
- Combining IV with Key Per-Session to form Key Per-Packet.
- Decrypting packet using AES algorithm to get payload with IPSec Trailer.
- Removing IPSec Trailer to achieve origin payload.

Step 5: Transmiting payload to destination machine.

- AMiMA will determine the address to which the payload belongs. If this address belongs to WLAN, AMiMA server will use IPSec to re-pack the packet and transmit to AP. In constrast, if this belongs to enterprise network, AMiMA server will pass this payload to Physical layer to transmit to a computer of enterprise network.

III.5. User account protecting

The system defines a master key (which is setup when installing the system or is given in advance) which will be used to encrypt information in the account file. This key is transparent to users and will be the master key of production even if the network admin does not know this key.

The list of accounts will be hold in the form index of file. Figure 3.7 shows the structure of this files.

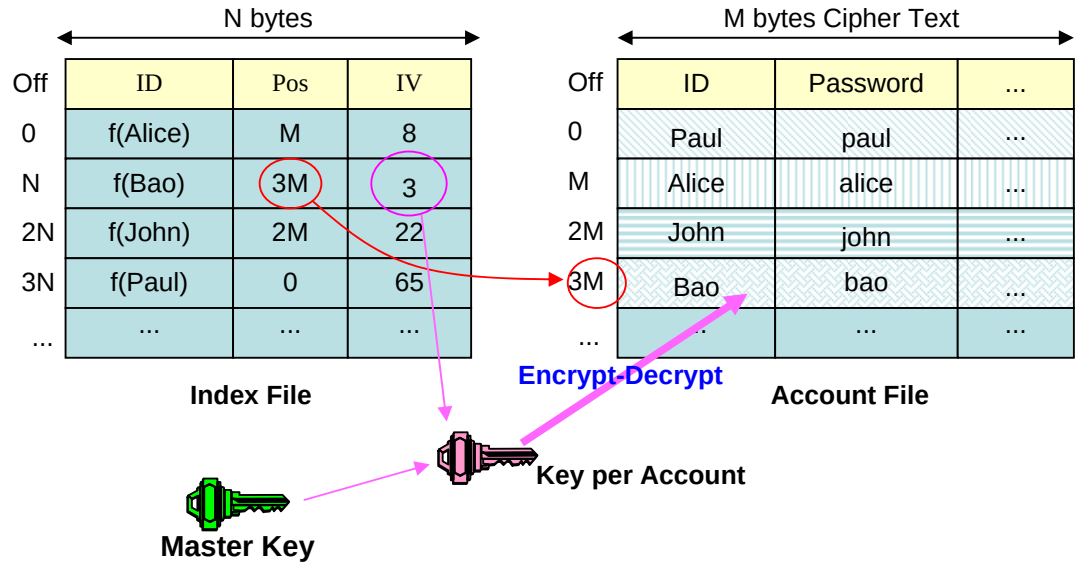

Figure 3.7: the file structure for user account protecting.

Account information is hold in two binary files:

- **Account file**: holds the list of real user accounts
- **Index file**: holds information of corresponding accounts

These files are managed by the system, their structures are private and are not public to the users.

III.5.1. Index file

Index file is a set of fixed size records. Each record holds information of corresponding account in the account file and includes:

- **Id.,** which is the identification of user and the value of hash function of username: h(username).
- **Pos**., which is the position of corresponding account in the account file.
- **IV**., which is a random integer value and will be combined with Master Key to form the encryption-decryption key of the corresponding account.

This file is sorted by the ID field.

III.5.2. Account file

Account file is a set of fixed size records. Each record holds information of concrete account. Each record is a cipher text which was encrypted by AES using the combination of master key and corresponding IV in the index file.

The structure of record is as follows:

- **Id**., which is the identification of account and is just the username.
- **Password**., which is the user password that will be used in the authentication phase.
- …

Note: Information of each account in account file is encrypted by different keys. These keys are the combination of master key and corresponding IV in the index file. In order to decrypt a specific account, it must have all of the master key, the index file and the account file.

IV. SECURITY AND PERFORMANCE ANALYSES

In this section, we will analyze AMiMA's ability of defending against man-in-middle attacks on WLAN. We focus on the attacks which were presented in section II. The performance of the system will be presented by compareing AMiMA with other solutions.

IV.1. ARP attack

As we already knew, the necessary condition of the ARP attack is that the hacker must gain the right to access WLAN . There are three possibilities:

- In the first possibility, hacker does not have any information. Because the system has been upgraded with the authentication service, the attack on this service is impossible. In principle, only the case when the username and password of the user is uncovered, then the hacker can use this legal information to access network, otherwise he must crack AES to get the session key.
- The second possibility is that the hacker has learned information about username of the victim (the hacker can be the internal user of the network). Because the hacker does not have password, she can not get this password and session key from the Certificate because of fail-safety of AES and the complexity of the Certificate. In the process of message receiving, hacker can only receive IP packets in the cipher form of AES through IPSec layer and the integrity of message is ensured by the safe HMAC algorithm. Therefore, even if the hacker has taken the message, she can not understand and also can not modify the content of message. Hence, the data confidentiality and data integrity are still secure.
- The worst case happens when hacker has discovered both the username and password of the victim. In this case, only when the hacker attacks just during the time that user and system are communicating, then the hacker can takes session key; otherwise she is unable to perform the ARP attack method because the message was encrypted by AES using this session key. Hence, even in this worst case, the system is still secure with the probability of 50 percent based on using of different session key for each session.

IV.2. IP spoofing attack

IP spoofing attack bases on exploiting of the weak points of RC4 and CRC. In this attack method, the hacker has learned positions and values source and the destination IP. From there, she changes destination address so that packets will be forward to a computer that she has taken control. When the message passed through the AP into WLAN, it is decrypted and the hacker will be able to understand this plaintext.

Using AMiMA, the real source and destination address were packed and encrypted through IPSec layer, therefore, the only address that the hacker can manipulate is the address to AMiMA server (a VPN gateway). If the hacker attacks using IP spoofing as presented in section II, there are two possibilities:

- The hacker replaces destination IP of WEP with the address of a computer that is external of WLAN (it may be a computer in LAN or on Internet). In this case, the message has only one way to AMiMA server. When the packet comes AMiMA, because the destination address is not matching, AMiMA will refuse this legal message. Hence, the hacker will be unable to receive the expected message.
- In the case that the hacker routes packet to a computer on WLAN that she can control (in this case, this computer has the access right). Through AP, packet will be forwarded to the hacker's computer, but she still receives the message which was encrypted at IP layer using IPSec technique. In order to take advantage of the message, the hacker must have the session key, but this is impossible. Hence, the system is still protected.

IV.3. Performance analyses

The compare bases on the following criterions:

- Security
  - Access control
  - Confidentiality
  - Integrity
- Speed
- Hardware using

IV.3.1. AMiMA and WEP

	AMIMA	WEP	AMiMA > WEP
Authentication	Using a new protocol based on EAP for mutual authentication.	Using 4 ways Handshake.	Safer
Confidentiality	Message is encrypted by 2 layers: RC4 of WEP and AES at IPSec.	Massage is only encrypted by RC4 of WEP.	Safer
Integrity	Using HMAC of IPSec to protect packet and CRC of WEP to protect frame.	Using CRC of WEP to protect frame.	Safer
Key for data encryption	Each session, using a different key to encrypt data.	Using only one key for all sessions.	Safer
Speed	Encryption at IP and MAC layers.	Encryption at MAC layer.	Slower
Hardware	Using devices compatible with WEP and a computer for AMiMA server.	Using devices compatible with WEP.	Need a computer for AMiMA server.

Table 4.1: Compare between AMIMA and WEP

IV.3.2. AMiMA and WPA

	AMIMA	WPA	AMiMA > WPA
Authentication	Using a new protocol based on EAP for mutual authentication.	Using 802.1X for authentication.	Equivalent
Confidentiality	Message is encrypted at 2 layers: RC4 of WEP and AES of IPSec.	Message is encrypted by AES.	Safer
Integrity	Using HMAC of IPSec to protect packet and CRC of WEP to protect frame.	Using MIC to protect frame.	Equivalent
Key for data encryption	Each session, using a different key to encrypt data.	In each session, using a different key to encrypt data.	Equivalent
Speed	Encryption at IP and MAC layers.	Encryption at MAC layer.	Slower
Hardware	Using devices compatible with WEP and a computer for AMiMA server.	Only using devices which supports WPA.	AMiMA needs only a computer to be the server and there is no change of current hardware, meanwhile WPA needs.

Table 4.2: Compare between AMIMA and WPA

IV.3.3. AMiMA and WEP+VPN

	AMIMA	WEP+VPN	AMiMA > WEP+VPN
Authentication	Using a new protocol based on EAP for mutual authentication.	Through 2 access controls: AP and VPN server.	Safer and more effective
Confidentiality	Message is encrypted by 2 layers: RC4 of WEP and AES at IPSec.	Message is encrypted at 2 layers: RC4 of WEP and the	Equivalent

		encryption algorithm of VPN	
Integrity	Using HMAC of IPSec to protect packet and CRC of WEP to protect frame.	Message is protected at 2 layers: WEP and VPN.	Equivalent
Key for data encryption	In each session, using a different key to encrypt data.	In each session, using a different key to encrypt data.	Equivalent
Speed	Encryption at IP and MAC layers.	Encryption at IP and MAC layers.	Equivalent
Hardware	Using devices which are compatible with WEP and a computer for AMiMA server.	Using devices which are compatible with WEP and a computer for VPN server.	Equivalent

Table 4.3: Compare between AMIMA and WEP+VPN

IV.3.4. Summary

	WEP	**WPA**	**WEP+VPN**	**AMIMA**
Authentication	Not safe	Safe	Safe	Safe
Confidentiality	Not safe	Safe	Safe	Safe
Integrity	Not safe	Safe	Safe	Safe
Key for data encryption	Using only one key for all of session.	In each session, using a different key to encrypt data.	In each session, using a different key to encrypt data.	In each session, using a different key to encrypt data.
Speed	Fastest	Fast	Slow	Slow
Hardware	Immutable	Changes of hardware configurations.	Add a computer to be VPN server.	Add a computer to be AMiMA server.

Table 4.4: Summary of compare results between solutions.

V. CONCLUSION

We presents a software solution for defending against main-in-middle attacks on WLAN – AMiMA. AMiMA is developed based only on current hardware while strengthening the capacity of access control and confidentiality using IPSec technique. The system is developed as software, therefore, it is easily to install into current devices without upgrading of the hardware.

AMiMA is intended to enforce three main security goals for WLAN: access control which is based on EAP and mutual authentication technique, confidentiality and integrity through two layers: WEP and IPSec.

For access control, AMiMA does not use the 4-ways handshake of WEP, but instead using a new method based on EAP. All the messages in the communication are encrypted using AES and the mutual authentication. When the password is not disclosed, eavesdropper is unable to get the password as well as sthe ession-key even if he can captures the EAP-packet.

Confidentiality and integrity were solved at once in AMiMA. Messages are protected by two layers: current WEP layer and IPSec. Therefore, although WEP is unsecure, even if the hacker can passes WEP layer, he is unable to go furthur because the messages are still protected by IPSec layer. Because the IPSec is implemented in software, we can select one among the advanced cryptography algorithms. Hence, AMiMA meets two demands for WLAN: confidentiality and integrity.

The problem of account protection is also considered through the organization of index and account files. The structure and content of these files are secret therefore the management of keys is secure, flexible and easy to maintain. We can use system like Active Directory of MS Windows for this purpose.

Acknowledgments

The works is carried out in part at the Department of Electr. Eng. and Information Sciences, Ruhr-University Bochum, Germany, under the financial sponsor of the KAAD. We would like to thank Dr.

Heinrich Geiger of KAAD, Prof. Christof Paar and Prof Jorg Schwenk of Ruhr-University Bochum for their valuable help.

References

[1] B. O'Hara and Al Petrick. The IEEE 802.11 Handbook. *IEEE Press, 1999*.

[2] Nancy Cam-Winget, Russ Housley, David Wagner and Jesse Walker. Security Flaws in 802.11 Data Link Protocols. *Communication of the ACM, May 2003/Vol. 46, No. 5*.

[3] Russ Housley and William Arbaugh.Security Problems in 802.11- based Networks. *Communication of the ACM, May 2003/Vol. 46, No. 5*.

[4] Borisov, N. Goldberg, I. And Wagner, D. Intercepting Mobile Communications: The Insecurity of 802.11. *Proceeding of the 11th Annual International Conference on Mobile Computing and Network, p.180, July 16-21, 2001*.

[5] J. Leyden. Tool Dumbs Down Wireless Hacking. *www.theregister.co.uk, August 2001*.

[6] T. Dismukes. Wireless Security Blackpaper. *www.arstechnica.com*.

[7] T. Karygiannis and L. Owens. Wireless Network Security: 802.11, Bleutooth and Handheld Devices. *NIST Special Publication 800-48, DRAFT, 24 July 2002*.

[8] J. Walker. 802.11 Key Management Series: Part I and Part II. *Available online.*

[9] M. Jakobsson, S. Wetzl and B. Yener. Stealth Attacks. *http://www.informatics.indiana.edu/markus/stealth-attacks.htm, 2005*.

[10] Sheila Frankel, Karen Kent, Ryan Lewkowski, Angela D. Orebaugh, Ronald W. Ritchey and Steven R. Sharma. Guide to Ipsec VPNs. *NIST Special Publication 800-48, DRAFT, January 2005*.