Design of Secure ARP on MACsec(802.1AE)

Jun-Won Lee1[#1], Seon-Ho Park1[#2], Ki-Ho Gum[*3], and Tai-Myoung Chung1[#4]

[#]*Internet Management Technology Laboratory,*

School of Information and Communication Engineering, Sungkyunkwan University,

300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do 440-746, Republic of Korea

[1]jwlee@imtl.skku.ac.kr

[2]shparkg@imtl.skku.ac.kr

[4]tmchung@ece.skku.ac.kr

[*]*SAMSUNG SDS, 10F, ASEM Tower, 159-1, Samsung 1-dong, Gangnam-gu, Seoul*

135-798, Republic of Korea

[3]kiho.gum@samsung.com

***Abstract*— MACsec provides authenticity and integrity for data frame on data link layer by implementing data encryption. For these advantages, MACsec is highlighted as a solution to protect and transmit data safely from the various security threats in the Wired and Wireless LAN. Until now, MACsec can not guarantee stable ARP management for itself [1]. This paper will propose a design of enhanced ARP to protect IP and MAC address from external threats and the enhanced ARP will encrypt ARP Packet by SAK (Secure Association Key) for the authentication. It will help to keep the address system safe from various security threats on data link layer.**

***Keywords*— ARP, MACsec, MAC flooding, ARP spoofing, MKA**

I. INTRODUCTION

As expanding an opened network environment like a wireless network, the environment of LAN has been exposed to everyone. Organizations have to make adequate security measures to keep important and confidential data from leaking. Various methods are prepared to guarantee the availability of IT infra structure and to prevent disclosure of data. WPA and WPA2 are introduced for protecting wireless network [2] and 802.1X, port-based user authentication [3] has been carried out. Such solutions need high initial investment costs and high operating costs continuously. As compared with high cost, they are insufficient to protect a local network infrastructure from 'DHCP Starvation attack', 'Man-in-The-Middle Attack', 'DoS Attack' [1], 'ARP spoofing' [4] and 'Mac flooding' [5], and assure 'authentication', 'access right', and 'data integrity'. An enhanced protocol, providing authentication, access-control, and data encryption between hosts on data link layer can overcome these problems.

MACsec (IEEE 802.1AE) [9] protocol focuses on the data encryption between the Host-to-Host data communications. However the security measures for ARP and DHCP protocol are excepted from MACsec protocol [7]. Although 'DHCP option 82' [8] can be applied to DHCP vulnerability as a solution, the security threats against ARP are still remained.

In this paper, the enhanced ARP, named Secure ARP will be developed against other data link layer threats such as 'ARP spoofing' [4] and 'MAC flooding' [5]. By using the same cipher module and the same key management protocol (802.1af) [9] with MACsec, it will reduce the resource consumption of system. After adapting this solution, the stable management of ARP Table will be achieved from data link threats like ARP spoofing and MAC flooding.

The rest of this paper is organized as follows. Chapter 2 mentions the vulnerability of data link layer(MAC flooding, ARP spoofing), Chapter 3 explains the MACsec protocol applied to enhanced ARP system, Chapter 4 describes a design of Secure ARP as enhanced ARP solution, and Chapter 5 shows the effects of adapting the Secure ARP.

II. ANALYSIS OF DATA LINK LAYER VULNERABILITY

Most of the attacks on data link layer target the depletion of system resources or the leaks of data. They appear in the type of changing source MAC address of frame. MAC flooding and ARP spoofing are typical types of changing MAC address.

A. MAC flooding

MAC flooding is an ARP cache poisoning attack. In other words, MAC flooding attacks exhaust CPU and Memory of network equipments and hosts by transferring massive frames having a changed source MAC address. Those attacks are occurred by malicious attackers or unintended PC viruses [5]. Attacks of unauthorized user can be mitigated by port-based network access control such as 802.1X [3], and attacks caused by unintended viruses can be controlled by comparing sender's physical MAC with source MAC transfered. Thus the availability of ARP cache in the target can be assured. We can use CAK [6] of MACsec to separate authorized users and unauthorized users [9].

B. ARP spoofing

If ARP reply is changed by attacker, the host which requests the target MAC address can not know whether the address replied is original or not. Thus the data can be transferred to an unintended address and attacker sniffs the data and redirects it to original destination [4]. ARP table is

978-1-4244-8812-4/10/$26.00 ©2010 IEEE

composed of ARP packets transferred from hosts. However it's very hard to divide malicious ARP packets from transmitted or received packets by using the present ARP system. Though static ARP keeps the ARP table static and prevents ARP table changing from ARP packets transmitted, changes of hosts due to guests, users, new employee, etc need frequent updates on the ARP table and many efforts to manage the stable ARP table. If there is an authentication process for ARP table update, ARP security can be assured without the static ARP management. In addition to authentication, it should include preparations for hosts not to participate in authentication.

III. MACsec Protocol Overview

A. 802.1af - MACsec Key agreement protocol

802.1af(MACsec Key agreement protocol) is created by modifying 802.1X for the purpose of providing a secret key between stations that have encrypted communication [9]. This protocol supply a key named CAK, and CAK is used to generate a SAK for MACsec communication. PAE of Fig. 1 is module supplies EAP service in MACsec [9]. PAE can perform a Supplicant or an Authenticator for sharing CAK. The Key sharing is carried out through uncontrolled port. CA leader is an authenticator and a station that has the role of communicating with authentication server. CA leader broadcasts EAP request to the other PAEs(Supplicant) periodically, and all stations in a single CA, can share a same CAK.

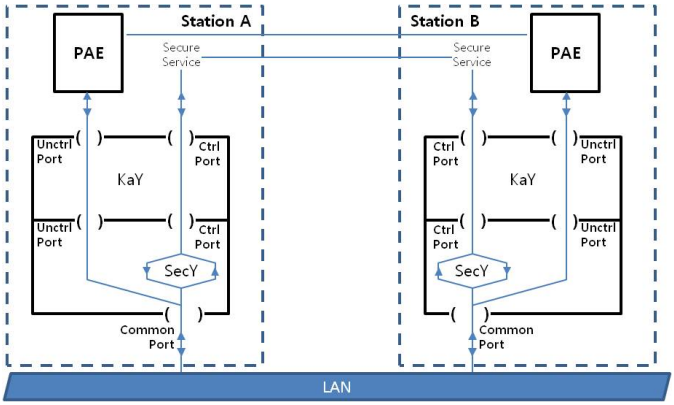

Fig. 1. 802.1af Process Flow

A CAK transferred to the stations in a single CA makes ICK and KEK by AES-ECB. KEK is a Key Encrypting Key and derived from the CAK as equation (1). KEK encrypts SAK with AES Key Wrap, and ICK(ICV-Key) derived from the CAK as equation (2) is used to authenticate message [10].

$$KEK=AES\text{-}ECB(CAK, 0x0) \quad (1)$$
$$ICK=AES\text{-}ECB(CAK,0x1) \quad (2)$$

The distributed SAK [9] encrypts user data with SecTAG values and the order of distributed SAKs is arranged by AN(Association Number).

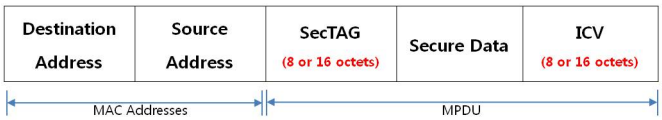

Fig. 2. MACsec Frame

MACsec provides data confidentiality and integrity between stations in the same CA. The key used in encrypting data is generated by 802.1af protocol [9]. In a SA, each station transfer secure data encrypted with a SAK as Fig. 2. MACsec Frame is divided into MAC address and MPDU(MACsec Protocol Data Unit). Default Cipher Suite(GCM-AES-128) [11] encrypts user data(MSDU) and makes generate ICV(Integrity Check Value) with SecTAG, MSDU, and ICK. The SecTAG field in front of the secure data has important information for encryption and authentication. The station receiving frames checks MPDU and ICV with SecTAG and SAK. In case of transmitting data, 'transmit multiplexer' puts together frames from uncontrolled port and controlled port and transmit combined frames through common port. In case of receiving data, receive de-multiplexer separates and transmit to uncontrolled port and cipher suite module. The cipher suite module carries out encryption, decryption, and validation check in transmitting and receiving process [9].

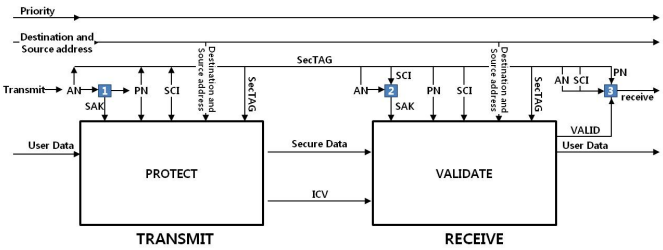

Fig. 3. MACsec Operation (Transmit & Receive)

When the MACsec transfer user data as Fig. 3, 'function 1' provides SAK and PN fit for AN. When the 'function 2' of Fig. 3 receives AN and SCI, the SAK is selected. If AN, SCI, and PN accord with the values decrypted in the SecTAG field, 'Function 3' will finally decide to receive frames. In other words, the combination of Function 2 and 3 can check integrity and authenticate normal hosts.

IV. Design of Secure ARP

A. The Direction of Design

Authentication for normal host, integrity check for ARP packet, and admission for reliable hosts are essential functions in the enhanced ARP. However the original ARP is limited to support these functions. We will arrange additional fields by assigning new protocol type for Secure ARP, and design a module to check and control Secure ARP packets and original ARP packets.

B. Design of ARP Packet for MACsec

By using a different protocol type with MACsec protocol, Secure ARP can focus on supplying authentication and access control besides data encryption between hosts. In Secure ARP, we used '0x0807'(temporary number) as ehter type number in place of '0x0806'. ARP SecTAG including ether type'0x0807', APDU(ARP Protocol Data Unit), and ACV(ARP Check Value) are located on the Secure ARP frame, shown as Fig. 4. ARP SecTAG contains values for encrypting and decrypting original ARP packet, and all values except for PN(Packet Number) and SCI(Secure Channel Identifier) are fixed. APDU is an encrypted data of ASDU(ARP Service Data Unit, Fig. 5) with SecTAG and SAK by using GCM cipher suite.

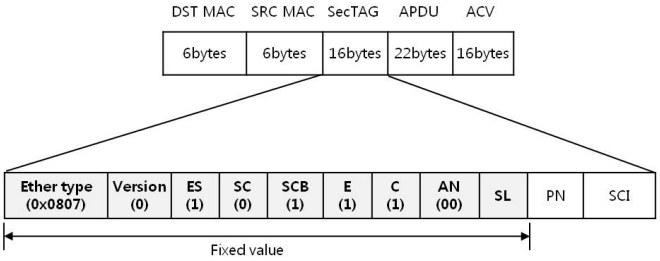

Fig. 4. Secure ARP Frame

As with ICV providing integrity and authenticity, ACV(ARP Check Value) can perform the same function for As a HMAC of APDU, ACV can check authenticity and integrity of ARP information. The Secure ARP will keep a focus on IPv4 that has many issues related ARP attack. The 6byte fields including hardware type, protocol address type, and address size are deleted to minimize Secure ARP frame size. When applying SecTAG and ACV, the size of Secure ARP frame is increased from 40byte to 66byte.

Operation (OPER) (16bit)
Sender hardware address (SHA) (first 48 bits)
Sender protocol address (SPA) (first 32 bits)
Target hardware address (THA) (first 48 bits)
Target protocol address (TPA) (first 32 bits)

Fig. 5. ASDU(ARP Service Data Unit)

C. Enhanced ARP Process Flow

Because Secure ARP can not share the cipher suite of MACsec having different ether type,'0x88E5', it needs a logically separate path. ARP Filter is inserted to distinguish Secure ARP packets and to block anomaly ARP packets into and from uncontrolled port as Fig. 6.

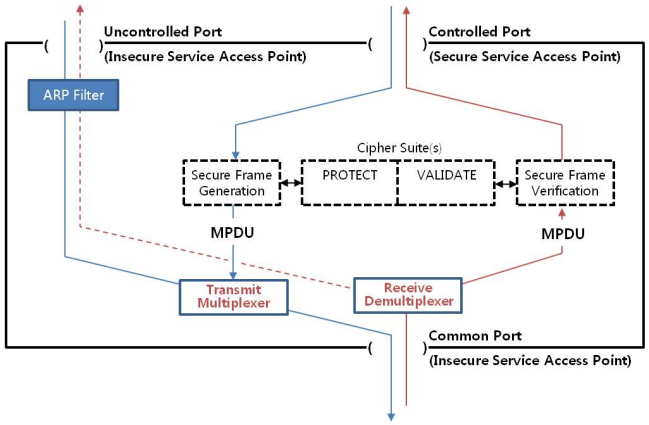

Fig. 6. Secure ARP Architecture on MACsec

ARP Filter changes the shape of outgoing ARP packets for Secure ARP requirements and inspects the ingoing ARP or Secure ARP packets.

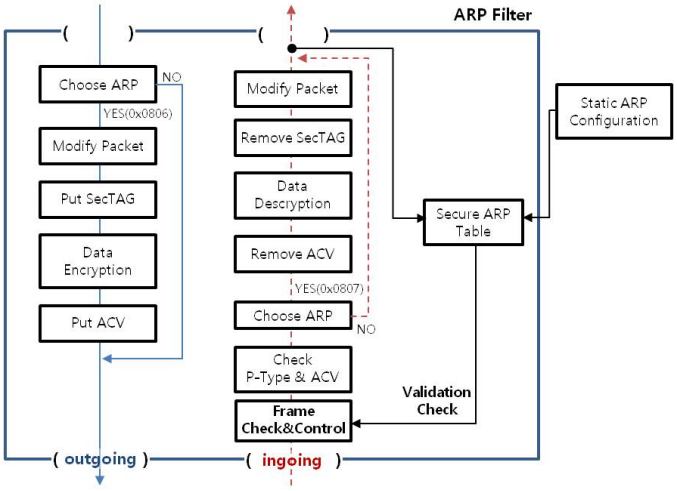

Fig. 7. ARP Filter Architecture

Fig. 7 illustrates the more detail description of ARP Filter. In case of outgoing traffic, the ARP Filter chooses ARP packet and transfers the other packets to 'Transmit Multiplexer'. After sorting packets, ARP Filter changes the header and the data unit of ARP as Fig. 4 and attaches ACV at the end of APDU. The processes for ingoing traffic are reverse, but 'Check P-Type & ACV', and 'Frame Check & Control' are added in front of 'Choose ARP' module. 'Check P-Type & ACV' module determines whether to receive a orginal ARP(0x806 protocol). If it allows general ARP packets, additional plans for security should be established. Setting a static ARP on gateway and redirecting the information to the subnet can be another method to keep the ARP Table stable.

Fig. 8 illustrates the flow that a Secure ARP Host(Host A) request a MAC address of non Secure ARP Host(Host B). When Host A request a MAC address of Host B, the Host B, not a Secure ARP Host can not reply with the Secure ARP request. However, the gateway has the information of the Host

B in advance and can broadcast the ARP information to the Host A by Secure ARP. In addition, the ARP database of gateway is maintained as a separate server or as itself. Fig. 9 illustrates the flow that a non Secure ARP Host(Host B) request a MAC address of Secure ARP Host(Host A). The Host A eliminates the ARP request of non Secure ARP Host B in the ARP Filter to prevent attack. To improve these problems, the gateway provides the ARP reply with reference to Secure ARP table of itself. If the Host B is an unauthorized user, the ARP replies provided by the gateway must be limited.

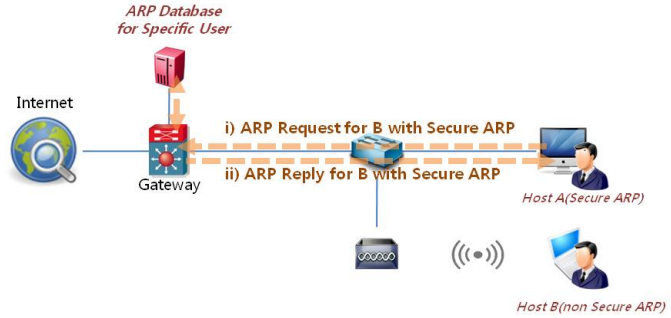

Fig. 8. ARP Request / Reply for non Secure ARP User

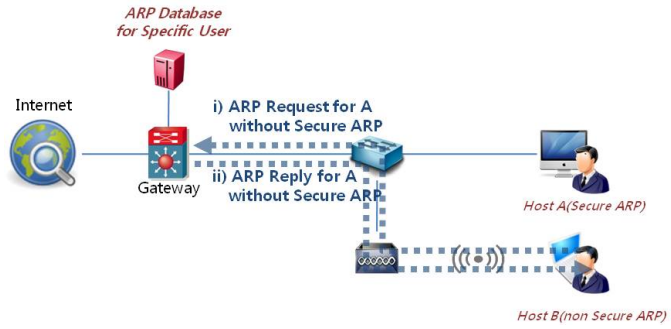

Fig. 9. ARP Request / Reply for Secure ARP User

V. The Effects of Adapting Secure ARP

A. Guarantee of availability

The 'Receive de-multiplexer' delivers frames not encrypted by MACsec to uncontrolled port as Fig. 6. The resources of machines are consumed in ARP filter, due to encryption and decryption process of Secure ARP, and checking and handling non secure ARP packet. Nevertheless, Secure ARP can keep the availability from the exhaustion of CPU and Memory, when incoming sudden attacks.

B. MAC flooding

When a MAC flooding occurs, huge packets flow in a network switch. In recent years, the most of switches have a function to limit inflow with threshold. Because gateway (e.g., Router) concentrated with more huge packets, it needs an ability to separate invalid packet. 'Frame Check & Control' module shown as Fig. 7 checks source MAC address of frame using the Secure ARP Table. The Secure ARP table is updated by Secure ARP packets and static ARP configuration. If the source MAC address is not updated on the Secure ARP table, ARP filter discards the invalid frames. The availability of CPU and Memory can be protected in a similar fashion. Fig. 10 illustrates the process that Secure ARP ensures the services from the MAC Flooding.

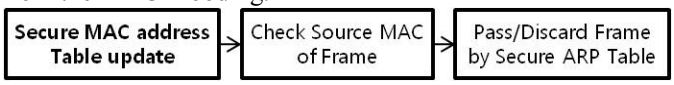

Fig. 10. Inspection of MAC flooding

C. ARP spoofing

ARP Spoofing attack is used to sniff data by broadcasting ARP reply packet to the hosts. Attackers change origin source MAC address with their MAC address. In Secure ARP system, ARP spoofing appears in two types as the use of Secure ARP. First, the reply packet in original ARP type is discarded in the phage of 'Frame Check & Control' as shown Fig. 7. Second, the reply packet in Secure ARP type is discarded in the phage of 'Check P-Type & ACV'. If Secure ARP reply packet has normal P-Type and normal ACV value, it is very hard to separate the anomaly packets. In order to avoid exposing the SecY information to unauthorized hosts, careful management is required.

VI. Conclusion

Secure ARP model presented in this paper is focused on the ARP of IPv4 that has security issues. The most considerable change is to add the authentication process to an existing ARP packet, so that the access of unauthorized host is controlled from the start of ARP update. For authenticating Secure ARP hosts, GCM-AES-128 and SecY are applied same with MACsec. Beside MACsec, Secure ARP can be extended for the ARP of IPv4 with changing the key management method and the cipher-suite. So, it can help to keep the local network safe from the attacks occurring by unauthorized users or viruses.

References

[1] Altunbasak, H., Krasser, S., Owen, H., Grimminger, J., Huth, H., Sokol, J.: Securing Layer 2 in Local Area Networks. Networking-ICN 2005 (2005) 699–706

[2] Selim, G., El Badawy, H., Salam, M.: New protocol design for wireless networks security. In: The 8th International Conference Advanced Communication Technology, 2006. ICACT 2006. (2006) 4

[3] Mishra, A., Arbaugh, W.: An initial security analysis of the IEEE 802.1 X standard. (2002)

[4] Whalen, S.: An introduction to arp spoofing. Node99 [Online Document], April (2001)

[5] Spangler, R.: Packet Sniffing on Layer 2 Switched Local Area Networks. Packetwatch Research (2003)

[6] Romanow, A.: Media Access Control (MAC) Security. IEEE 802.1 AE (2006)

[7] Jerschow, Y., Lochert, C., Scheuermann, B., Mauve, M.: CLL: A Cryptographic Link Layer for Local Area Networks. Security and Cryptography for Networks (2008) 21–38

[8] Coley, K.: Recommended Operation for Switches Running Relay Agent and Option 82. In: EtherNet/IP Implementor Workshops. (2004)

[9] Ohba, Y.: 802.1af overview. In: IEEE 802.21 MEDIA INDEPENDENT HANDOVER. (2008)

[10] Weis, B.: Security considerations and proposal for MACsec key establishment. (2006) 18

[11] McGrew, D., Viega, J.: The Galois/Counter mode of operation (GCM). (2004)