무선 LAN 상에서 안전한 AP인증 메커니즘 설계★

김점구*

요 약

현재 IEEE 802.11표준은 AP와 STA사이의 인증 및 보안 메커니즘이 취약하다고 많이 알려져 있다. 따라서, IEEE는 RSN(Robust Security Network)을 802.11에 대한 보안 아키텍처를 제안했다. RSN은 접근제어와, 인증, 그리고 키 관리 기반으로 IEEE 802.1X 표준을 사용한다. 본 논문에서는 IEEE 802.1X 또는, 802.11이 결합된 몇 가지 모델에 대한 취약점을 제시하고, 세션가로채기 또는 MiM(Man-in the-Middle)공격에 대응 할 수 있는 STA와 AP간의 접근제어, 인증 메커니즘을 설계하였다.

Design of Safe AP Certification Mechanism on Wireless LAN

Jeom Goo Kim*

ABSTRACT

Current IEEE 802.11 standard is very vulnerable that between the AP and STA authentication and security mechanisms is widely known. Therefore, IEEE has proposed security architecture RSN (Robust Security Network) for 802.11. RSN is used the access control, authentication, and key management based on the IEEE 802.1X standard. In this paper, IEEE 802.1X or 802.11 a combination of several models proposed for the vulnerability, and session hijacking or MiM (Man-in the-Middle) attacks to respond, the authentication mechanism Was designed to the access control between the STA and the AP,

Keyword : AP, security, Wireless LAN

접수일(2011년 3월 10일), 수정일(1차: 2011년 3월 23일), 게재확정일(2011년 3월 23일)

★ 이 논문은 2010학년도 남서울대학교 학술연구비 지원에 의하여 연구되었음.

* 남서울대학교 컴퓨터학과

1. INTRODUCTION

Wireless LAN networks (WLANs) as a rapid rate is coming into our lives. Users are connected to the wired network to reduce the time and cost of installation and use of new technology, WLANs are seeking. Airport, or the department turned a lot of people gathering places for the convenience of our customers to provide wireless LAN service. For this purpose, control access to and authenticate access to the IEEE 802.1X standard has been highlighted [1].

Without encryption, IEEE 802.1X, several other processes that many organizations are trying to use. Many organizations because they want to apply the IEEE 802.1X, IEEE 802.11 standard is to have a security problem [2,3,4]. IEEE 802.11 standard Security Working Group is expected to solve these problems. Meanwhile, Robust Security Network (RSN) of the port based network access control today announced the IEEE 802.1X standard. The IEEE 802.1X standard provides strong authentication and access control.

In this paper, using 802.1X authentication in IEEE 802.11 based network access control mechanism and gives an example of an attack, this attack is to design a mechanism that can block.

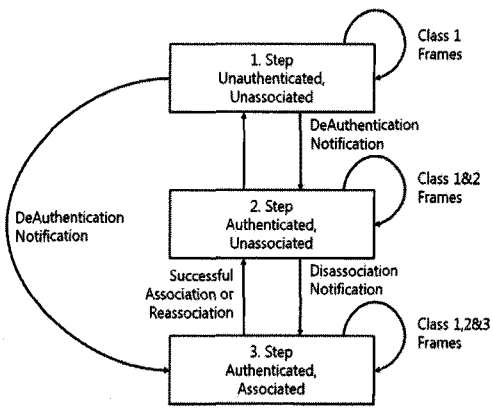
2. Related research

2.1 Default IEEE 802.11 network security mechanism

The IEEE 802.11 standard is made Medium Access Control (MAC) and a public frequency (2.4GHz, 5GHz) to use the physical layer (PHY).

The other client and each client radio to communicate directly within the limit distance that is provided by default Ad-hoc or infrastructure mode. Other structures include the junction Access Point(AP) mode. In this mode, each client point Station(STA) with the objective to transfer the client sends a packet to the AP. This paper deals with security at the junction of the infrastructure mode. For full access to AP and the following three actions are done in the junction and the AP.

1. unauthenticated vi. unassociated
2. authenticated vi. unassociated
3. authenticated vi. associated



(Fig 1) General 802.11 state

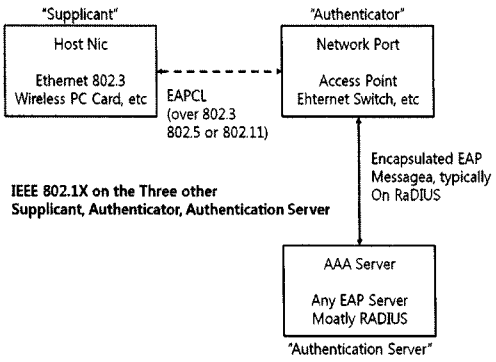
In this section, Robust Security Network (RSN) and IEEE 802.1X standard is described. In the wireless environment, Network access is subject to physical limitations, the security framework should provide a network security certification. Only RSN is limited in the MAC layer is based on IEEE 802.1X an unauthorized network access.

Network connections that are currently used in a particular environment port is provided. In IEEE 802.11 network port in the STA and AP is certified.

The IEEE 802.1X standard signature-based authentication, using smart card authentication methods, including the top-level hierarchy is provided in the framework. This Token Ring,

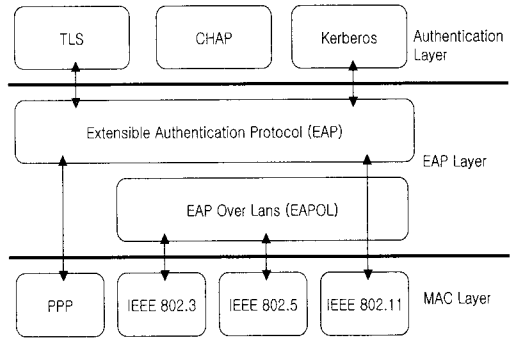
FDDI (IEEE 802.5), IEEE 802.11 and IEEE 802.3 local area network in the complex network technology to provide port based network access control. RSN is effective IEEE 802.1X for wireless LAN network technology.

RSN is provided the security framework in the IEEE 802.1X by the three complex elements to Figure 2 shows the communication settings. There are requester, authenticator or network port, and the authentication server. Requests from the authenticator, the services provided through the port is an object that you want to use. Therefore, a lot of AP for a single network port is assigned, and will be certified through this service. Request via the authenticator, after receiving a complete certification for the service center are certified to the authenticator.



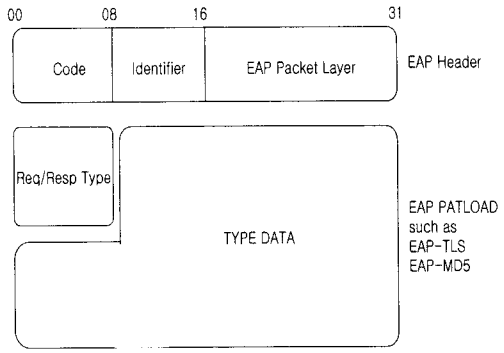
(Fig 2) IEEE 802.1X Set

The IEEE 802.1X standard to allow for a variety of authentication mechanisms, EAP (Extensible Authentication Protocol) was adopted[5]. EAP is a stack structure shown in Figure 3. Check the EAP response communication is done through. Here 4 different types of messages (EAP request, EAP Response, EAP connections, EAP termination) is used. Figure 7: Using the EAP authentication process shows the general.



(Fig 3) EAP STACK Structure

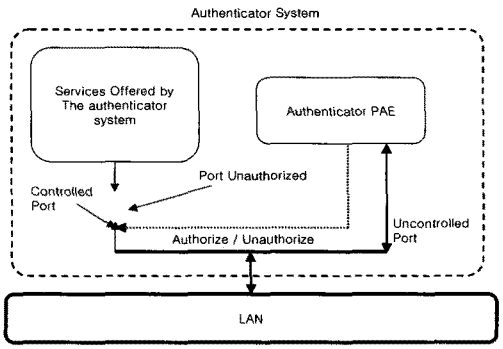
EAP request message to the requester is sent to inform the certification requirements, EAP response message to respond. The other two messages will tell you the results of the requester. Figure 4 is the structure of the EAP packet. This protocol EAP request / response messages with an authentication mechanism which can be encapsulated in. EAP at the network layer than the link layer, the behavior is much more useful. Thus, EAP the central server (RADIUS server, such as EAP) is connected via a message to the authentication process for each network port can be transmitted more flexibly.



(Fig 4) EAP PACKET Structure

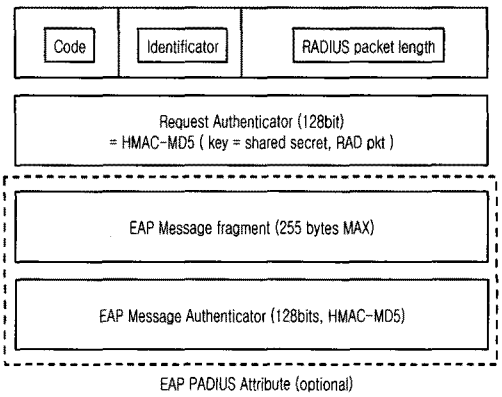
AP are used a dual port models that EAP are established in order to allow traffic before authentication. Figure 5 is dual port concept IEEE 802.1X is introduced in. This authentication system

has two ports not uncontrolled and controlled. Authentication system can be connected to the network has two ports. Uncontrolled port to block all network traffic, only EAP packets to pass.

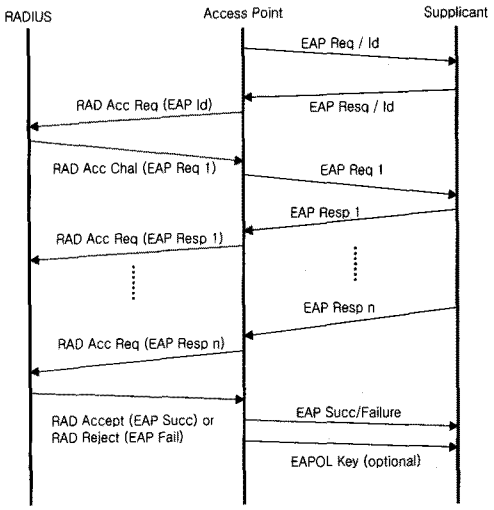


(Fig 5) Uncontrolled and Controlled Ports in Authentication

EAP messages are encapsulated all. EAP Over Lan (EAPOL) protocol to the EAP packets are sent between the authenticator and the pretenders. After encapsulating the first EAP session and log off will be notified. EAPOL-key message is to determine the session key in the top tier. In EAP and EAPOL protocol does not include security.



(Fig 6) 802.1X authentication is used for General RADIUS Packet Structure



(Fig 7) Between EAP and RADIUS 802.1X Certification procedures

Authentication server and authentication, the RADIUS (Remote Authentication Dial-In User Service) protocol is used[6]. Figure 6 shows a typical RADIUS packet. RADIUS protocol between AP and RADIUS server authentication of each packet, and has a checking mechanism. Figure 7 shows a complete 802.1X authentication session.

3. Design of transmission mechanisms for secure data transmission

In this chapter the standard IEEE 802.11 and 802.1X attacks be prevented by modifying the method is presented.

3.1 Authentication and robustness of each packet

For each packet authentication and data management at the level of vulnerability for the IEEE 802.11 frame, the key distributor of the

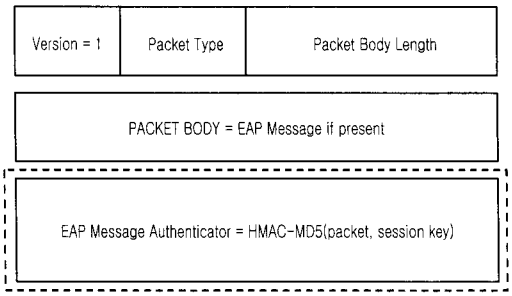
protocol has many security problems. Managed to steal the frame by using a vulnerability in the authentication is session hijacking.

Simple packet authentication to prevent attacks and should ensure the integrity of the data frame.

Should ensure that the integrity of the data frame currently in IEEE management frames do not have any plans for the protection.

3.2 EAPOL message protection and assurance

802.1X message authentication is vulnerable to a MiM attack. RADIUS EAP-Authenticator, as provided in the message is completed. EAP-Authenticator, EAP-Success message is added, such as a pseudo. The point is, such as EAP-TLS session key is made from top-level authentication protocol. EAP-Success message is removed, EAP layer are inserted EAPOL-key for completed sign. Figure 8 shows the pseudo the following message is added EAPOL packets.



(fig 8) EAPOL Packet Added Intention Messages

3.3 Point to point authentication model

This section contains two RSN framework represents an important element. As a result of this, many more point to point can be used to authenticate. The benefits of this framework that can be applied in Ad-hoc wireless scenarios.

3.3.1 Symmetric authentication (Symmetric authentication)

Between the requester and the AP can not be trusted element is determined. Therefore, the symmetric (in relation), IEEE 802.1X authentication should be included in the model. Now the authentication request is very similar to the state server and dual port mode is included. RADIUS server for the AP and the STA should be matched by similar conditions as possible. Only if different, STA and the RADIUS server is to communicate through the AP.

3.3.2-phase authentication (Scalable authentication)

To have greater mobility, RADIUS server, the steps that AP is a need to control. Each AP is not easy for users of the current management environment is shared. Steps must be certified by the AP theory.

4. Conclusions and future research

Clearly set forth in the wireless environment, security is very important. Transfer device is being shared by a range of physical security

As a result, strong access control and authentication is required, and the organization became necessary to protect the information. However, the existing wireless LAN standards include access control and authentication, session hijacking, and which was due to the MiM attack. However, AP and the RADIUS protocol for the connection between the secure session is designed. In this paper, we present a modified protocol designed with a more powerful security features are expected to complete the protocol.

Reference

[1] IEEE. Standards for local and metropolitan area networks: Standard for port based network access control. IEEE Draft P802.1X/D11, March 2009

[2] W.A. Arbaugh, N. Shankar, and J. Wang. Your 802.11 Network has no Clothes. In Proceedings of the First IEEE International Conference on Wireless LAN's and Home Networks, December 2009.

[3] N. Borisov, I. Goldberg, and D. Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. In proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, pp180-188 2009

[4] S. Fluhrer, I. Martin, and A.Shamir. Weakness in the key scheduling algorithm of rc4. Eighth Annual Workshop on Selected Areas in Cryptography, Agust 2009.

[5] L. Blunk and J. Vollbreeht, Ppp extensible authentication protocol (cap). RFC 2284. March 2008.

[6] C. Rigney and et. al. Remote authentication dial in user service(radius). RFC 2138, April 2007

[저 자 소 개]

김점구 (Jeom Goo Kim)
광운대학교 전자계산학과(이학사)
광운대학교 전자계산학과(이학석사)
한남대학교 컴퓨터공학과(공학박사)
(주)제성프로젝트 연구원
(주)시사컴퓨토피아 인터넷사업 본부장
2011년~현재 남서울대학교
컴퓨터학과 교수
IT융합연구소장
email : jgoo@nsu.ac.kr