AP와 RADIUS서버 보안 및 취약점 분석

김현호* · 장원태**· 조정복** · 이훈재**

* **동서대학교

AP and RADIUS server security and vulnerability analysis.

Hyun Ho Kim* · WonTae Jang** · Jung Bok Jo** · Hoon Jae Lee**

* **Dongseo University

E-mail : feei_@naver.com, {jwtway, jobok, hjlee}@dongseo.ac.kr

요 약

현재 무선 네트워크를 이용할 수 있는 기기(스마트폰, 태블릿PC, 노트북)이 많이 출시하고 있다. 그리고 무선 네트워크 사용자 증가에 따라 무선 AP도 증가 하고 있다. 지금 무선 네트워크 서비스는 전국적으로 이용할 수 있으며, 개인이 AP를 구축하여 이용하는 사용자 수도 늘어나고 있다. 이렇게 개인이나 통신사에서 제공하는 무선 네트워크를 사용하는 이유는 구축비용이 저렴하고 속도가 빠르다는 것이다. 그러나 무선 네트워크발전은 급속히 증가하고 있지만, 무선보안에 대해서는 그만큼 따라가지 못하고 있다. 현재 무선보안은 개방형 네트워크를 많이 사용하고 있고, 암호를 알고 있는 사람은 누구나 접속할 수 있다는 문제점이 있다. 본 논문에서는 AP와 RADIUS서버를 이용하여 사용자 인증시스템을 구축해보고 문제점을 분석해 본다.

ABSTRACT

These days wireless network devices (smartphones, tablet PC, laptop) are being utilized more frequently. In line with the increasing number of users of a wireless network, the usage of wireless access points is also increasing. Nowadays as nationwide wireless network services being made available, wireless networks are increasingly being used due to the lower costs of building faster and affordable private or carrier networks. However wireless security is not keeping up with this development. Many use open networks where anyone can join, meanwhile for those using wireless security protocols there is the problem of managing the password. In this paper, we analyze the problems of trying to build a user authentication system using an access point and the RADIUS server.

키워드

AAA Server, RADIUS, Wireless Scurity, Wireless Lan

Ⅰ. 서 론

최근 무선 네트워크가 많이 발전해서 무선단말기인 스마트폰, 노트북, 태블릿PC와 같은 스마트기기사용자가 급속히 늘어나고 있다. 그와 동시에 무선 네트워크 서비스도 같이 늘어나고 있으며, 현재 학교, 카페, 병원과 같은 건물에서 무선 랜 존과 개인이 무선공유기를 설치하여 무선 랜 존을 만들어 사용하는 경우도 매우 많아졌다. 이처럼 무선 랜 서비스가 급속히 증가하는 반면 무선보안은 너무 취약점을 많이 가지고 있다는 것이 문제점이 됐다. 본 논문에서는 이러한 무선보안에 대해 직접 실험해 보고 문제점을 파악하여 기존보다 좀 더 강화된 보안방법을 알아본다. II장에서는 802.11인증 방식 중 WEP 인증 방식과 WPA/WPA2 인증 방식 및 인증요청과정, RADIUS 서버 특징 III장은 무선라우터의 보안종류 및 보안수준, 무선라우터와 RADIUS서버의 문제점을 알아보고 IV장에서 PacketTracer5.3.3로 현재 많이 사용하고 있는 무선 네트워크를 구축해보고 문제점을 분석해서 마지막으로 V장에서 결론을 맺는다.

Ⅱ. 관련연구

본 장에서는 802.11의 인증방식 중 WEB 인증 방식, WPA/WPA2 인증방식 대한 설명, 연결과정과 RADIUS서버 특징에 대해 알아본다.

1. WEB 인증 방식

WEB 인증방식은 Open System Authentication 방식과 Shared Key Authentication 방식이 있다. Open system Authentication 방식은 단순한 데이터 프레임 암호화만 사용하고 인증은 없다. 이 방식은 인증과정이 없기 때문에 인증서가 필요 없는 시스템이다. 그러므로 사용자는 WEB Key만 있으면 인증 받을 수 있다. 이렇게 Client는 AP에 연결 요청을 하게 되면 다음과 같은 인증과정을 거친다.

1. Client가 AP에게 인증을 요청한다.
2. AP는 인증 응답과 자신의 인증 방식과 암호화 방법을 전송한다.
3. 상태와 정보 초기값을 AP에게 전송
4. AP는 clear-text challenge를 전송하고 client와 정보를 기억
5. client는 수신받은 challenge text를 설정된 WEP Key를 이용해 암호화 후 인증 요청 메시지를 전송함
6. AP는 수신한 데이터를 복호화 하여 자신이 보낸 clear-text와 비교 확인 하여 client의 인증여부를 판단함.
7. 인증 완료 후 데이터를 WEP Key를 사용하여 암호화 후 데이터 통신함

2. WPA/WPA2 인증 방식

WPA는 WEP의 취약점을 보안하기 위해 개발된 프로토콜이다. WPA와 WPA2의 다른점은 WPA는 TKIP 암호화 방식을 사용하고 WPA2는 PSK, AES 암호화 방식을 사용하는 것이다.

2.1 WPA의 특징

- WPA 방식으로 공인된 암호화 방식인 TKIP(Temporal Key Integrity Protocol) 암호화 알고리즘과 AES(Advanced Encryption Standard)이 개발됨.
- 2계층의 페이로드를 암호화
- 메시지가 임의로 변경되는 것을 막음

2.2 WPA2의 특징

- TKIP보다 강력한 AES(CCMP)를 사용[1].

3. RADIUS서버

RADIUS서버는 NAS(Network Access Server)와 인증 서버사이의 인증(Authentication), 서비스 허가(Authorization), 과금(Accounting)에 관한 정보전달을 위한 프로토콜로써, 유선 환경에서 로밍 PPP(Point to Point Protocol) 사용자를 인증하기 위한 AAA(Authentication, Authorization, Accounting) 프레임워크로 제안되었다. RADIUS 서버는 사용자가 연결을 요청하면 인증을 해주고 인증 받은 사용자에게는 허가된 서비스를 제공한다. RADIUS 서버는 4가지의 특징이 있다.

- Client/Server 모델 : NAS는 RADIUS 서버의 클라이언트로 동작하고, 사용자의 정보를 RADIUS 서버에게 전달한다. RADIUS 서버는 사용자 연결 요청을 받으면 사용자를 인증하고 서비스에 필요한 환경 정보를 반환한다.
- Network Security : NAS와 RADIUS 서버 사이의 인증은 미리 약속된 shared secret를 통해서 이루어지고 사용자 패스워드는 암호화된다.
- 유연한 인증 구조 : 단말은 PPP-PAP(Pass-word Authentication Protocol)나 PPP-CHAP(Challenge Handshake Authentication Protocol), UNIX 로그인과 같은 다양한 방법으로 인증된다.
- 확장성 있는 프로토콜 구조 : 모든 트랜잭션은 속성(attribute)값에 의해서 이루어지는데, 추가되는 속성은 attribute 필드에 덧붙임으로써 기존의 프로토콜 실행에 방해를 주지 않고 추가 할 수 있다[2].

Ⅲ. 무선라우터 보안

무선라우터의 보안모드에서는 WEP에서 WPA2 Enterprise 까지 여러 항목이 있으며 보안 수준도 차이가 있다. 어떤 보안모드 종류가 있고, 보안수준은 얼마나 되는지 알아보고 무선라우터와 RADIUS의 문제점은 무엇이 있는지 알아본다.

1. 무선라우터 보안모드와 보안수준

- WEP = 매우낮음
- WPA Personal(PSK Personal) = 낮음
- WPA Enterprise(PSK Enterprise) =보통
- WPA2 Personal(PSK2 Personal) = 높음
- WPA2 Enterprise(PSK2 Enterprise)=매우높음

무선라우터의 보안모드는 위와 같이 있으며 WPA보다는 WPA2를 사용하는 것이 안전하다[3]. 그리고 Personal과 Enterprise는 RADIUS서버 사용 유무를 뜻하는 보안모드이다. Personal모드는 RADIUS서버를 사용하지 않는 보안모드이며, EnterPrise모드는 RADIUS서버를 사용하여 기존 보안방식보다 더 강한 보안모드를 제공한다.

2. 무선라우터의 문제점

2.1 SSID : 보통 무선라우터의 SSID는 무선라우터의 이름(기본값)이나 해당 장소에 맞는 이름을 많이 사용한다. 이렇게 무선라우터의 SSID를 알림으로 인해서 쉽게 무선라우터의 장소를 노출하게 된다. 이것은 공격자에게 있어서 정보를 제공하는 것과 같다[4].

2.2 무선 네트워크 채널 : 대부분 무선라우터의 기본적인 채널(1Ch, 6Ch, 11Ch)[5]을 사용하는 경우가 많지만 채널을 다르게 설정하더라도 근처에 있는 액세스 포인트(Access Point)와 채널이 같다면 오히려 같은 채널에 속해있는 무선라우터는 서비스 거부공격인 DoS(Denial of Service)공격에 당할 위험도 있다.

3. RADIUS서버의 문제점

3.1 ID/Password : RADIUS서버에 인증요청을 할

경우 ID/Password를 입력하게 되는데 이 때 누군가가 사용자 아이디를 알고 있다면 동시접속이 가능하다는 문제점이 있다.

Ⅳ. 실험 및 분석

II, III장에서 알아보았던 정보를 이용하여 무선 네트워크를 직접 구성해 본다. 구성하는데 사용하는 프로그램은 PacketTracer5.3.3 버전을 이용하였으며, 네트워크를 구성한 후 문제점을 분석해 본다.

1. 무선 네트워크 구성

실험은 PacketTracer5.3.3으로 하였으며 구성하는데 필요한 장비로는 PC 2대, 무선라우터(Linksys-WRT300N), 라우터(2811), 서버 PC(RADIUS)를 사용하였으며 IP주소 및 장비배치 구성도는 아래 그림1과 같다.

그림1은 무선라우터 보안설정 WPA2 EnterPrise 인증방식을 사용하고 AES암호화를 적용하였으며, RADIUS서버에 사용자2명 ID와 Password를 등록하였으며, 해당 Client인 PC1과 PC2는 부여한 ID와 Password를 입력하여 정상 연결된 상태이다.

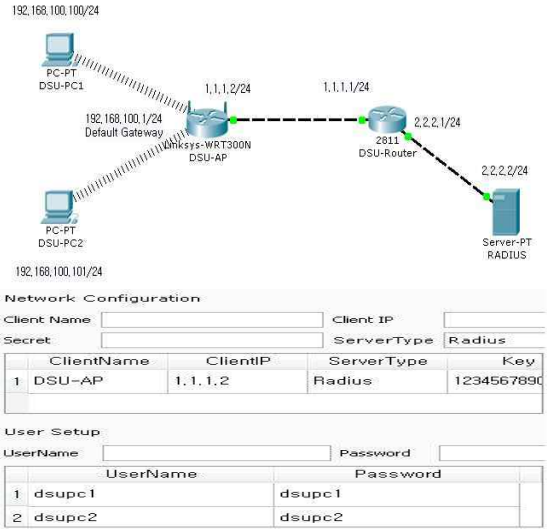


그림1. 구성도

1.2 문제점 분석

보통 AP는 그림1과 같이 네트워크를 구성하여 사용하는 경우가 많다. 이렇게 ID와Password를 알게 된다면 누구나 접근할 수 있는 문제가 발생하게 된다. 그 밖에도 공개키를 적용했을 때, 또한 같은 현상이 나타난다. 그리고 하나의 사용자 ID(dsupc1)와 Password(dsupc1)로 접속하는 실험도 같이 해보았다. 결과는 그림1과 같이 정상적인 연결이 되었다.

2. 보완된 네트워크 구성

문제점인 공개키 및 ID, Password를 좀 더 보완하여 제한된 연결을 할 수 있는 네트워크를 구성해본다.

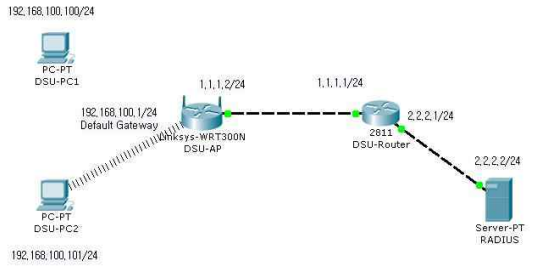
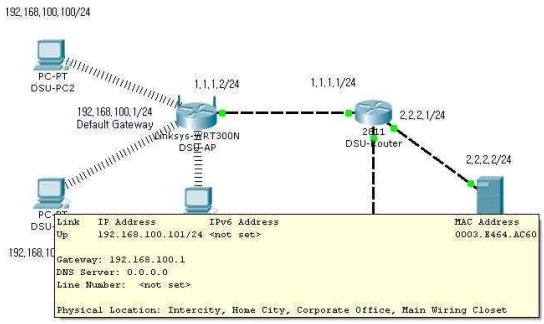


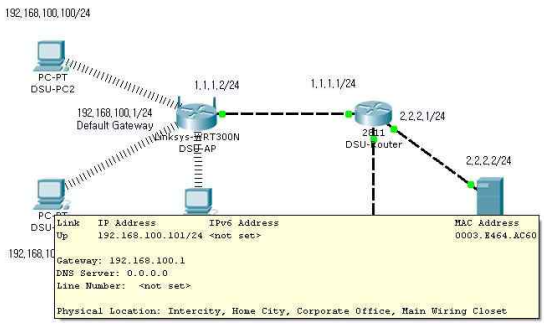
그림2. 네트워크 구성도

그림2는 무선라우터 설정에서 MAC Address를 등록하여 등록된 MAC Address만 접속을 허용하는 실험결과이다. 허용된 MAC Address만 접속이 가능하기 때문에 기존방법보다 좀 더 높은 보안 수준을 유지 할 수 있는 방법이다. 비슷한 실험으로 무선라우터에 접속인원제한을 설정해서 PC3을 추가하여 PC1과 PC2만 접속이 허용되도록 실험해 보았다. 실험결과는 그림3과 같다.

그림3은 PC1, PC2가 무선라우터로부터 IP주소를 할당 받고, 이 후 PC3을 추가하였다. PC3은 무선라우터로부터 IP주소를 할당받으려고 접속을 계속시도 한다. 그러나 결과와 같이 IP주소를 할당받지 못하고 있다.

실험결과와 같이 무선라우터에서 PC2대만 접속할 수 있게 설정하여 더 이상의 무선접속이 불가능하도록 접속을 차단한다.





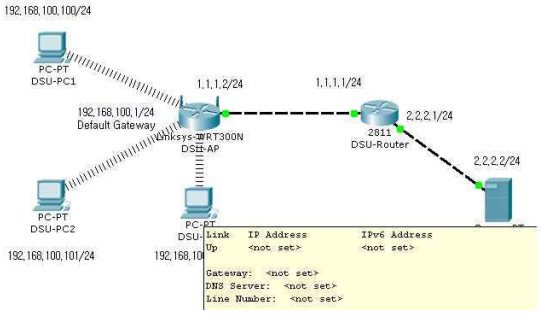


그림3. 접속인원제한을 적용

V. 결 론

본 논문에서는 최근 무선 랜 발전으로 인한 스마트폰, 노트북, 태블릿PC와 같은 무선 단말기기가 많아지면서 무선라우터 및 RADIUS서버의 보안과 문제점을 알아보기 위해 직접 무선 네트워크를 구축 한 후 실험을 통해 알아보았다. 그러나 현재 무선 네트워크 사용자 대부분은 무선라우터의 기본설정인 개방형 네트워크와 기본채널(1Ch, 6Ch, 11Ch), SSID와 보안이 취약한 WEP방식을 사용하는 경우가 많고, RADIUS서버는 ID/ Password가 노출되면 동시접속이 가능하다는 문제점을 알아보았다.

요즘 무선라우터 제조사의 펌웨어는 사용자들의 간편성과 안전성을 고려하여 누구나 쉽게 무선라우터 설정을 할 수 있도록 제공하고 있다.

최근 개인정보 유출이나 DDoS공격으로 인한 피해가 많이 발생하고 있다. 그러나 대부분 사용자들은 이에 대한 심각성을 인식하지 못하고 이용하는 경우가 많다. 따라서 개개인의 보안의식을 더 높이기 위해 정부, 무선 네트워크 서비스제공자, 무선라우터 제조사는 보안의식을 강조하는데 노력 할 필요가 있으며 개개인 사용자는 ID/Password를 철저히 관리하고, 무선라우터 사용시 권장하는 방식을 이용하여 안전한 무선 네트워크 환경을 구성하여 사용 할 수 있도록 노력이 필요하다.

참고문헌

[1] 변진영, 김동훈, 이기영, “무선 랜을 위한 보안 시스템 설계에 관한 연구” 한국해양정보통신학회, 2010.
[2] 송창렬, 정병호, 조기환, “무선랜 보안 구조” 정보과학회지 제20권 제4호, 2002. 4.
[3] 백종현, 박순태, “국내 무선랜(WiFi) 보안 운영 현황 및 정책 방향” 정보보호학회지, 제20권 제1호, 2011.2.
[4] 박재성, 한승조, “무선 네트워크 기반에서 PKI방식을 이용한 상호인증 프로토콜 설계” 한국해양정보통신학회, 추계종합학술대회, 2008.
[5] 심용섭, 전상봉, 박승근, “AP의 채널 설정 및 밀집도에 따른 무선 랜의 전송 속도에 관한 실험” 한국전파학회논문지, 2012.5.