무선 랜을 위한 보안 시스템 설계에 관한 연구

변진영, 김동훈, 이기영

인천대학교 정보통신공학과

A Study of Security System Design for Wireless LAN

Jin Yeong Byeon, Dong-hun Kim, Ki Young Lee

Dept. of Info & Telecom Engineering, University of Incheon

E-mail : bgyjjang@gmail.com

요 약

본 논문에서는 무선 네트워크 기술인 802.11의 보안책인 802.1x의 효율성에 대해 연구한다. 무선 네트워크는 1970년대 라디오 주파수를 사용하여 컴퓨터 통신 네트워크가 구축된 이후 눈부신 발전을 거듭하여 현재 학교나 카페 등에서 쉽게 무선 랜 존을 접할 수 있다. 하지만 최근 스마트폰이나 노트북 등 많은 portable 단말기의 사용자가 급속도로 증가 하면서 무선 랜 존의 수요가 크게 늘어가고 있다. 이렇게 무선 네트워크 구축이 활발히 되면 그와 동시에 증가하는 것이 보안 문제이다. 본 논문에서는 무선 AP와 Radius(AAA) 서버를 이용한 보안 시스템 구축 시 고려해야 할 요구조건과 유지관리를 위한 효율성을 연구하여 제한된 환경에서의 효과적인 보안 시스템을 설계를 위한 방안을 제시한다.

키워드

Wireless LAN, WPA, WEP, radius, AAA server, 802.1x

Ⅰ. 서 론

IP의 개발과 WWW이 확대 되면서 많은 사람들이 웹과 인터넷을 경험하게 되었는데 사람들은 점점 언제 어디서나 서비스를 사용하고 싶은 욕구가 생겨나게 되었고 이를 충족시키기 위하여 무선 랜, 3G 등 많은 분야들 또한 큰 발전을 이루었다. 이러한 무선 네트워크 기반이 충족 되어감에 따라서 노트북, PDA, 스마트폰 등 portalbe한 단말기의 사용자가 급속도로 증가 하게 되었고 그와 동시에 무선 랜 존의 수요가 크게 늘고 있다. 이렇게 무선 랜 존의 영역이 확대 되면서 서비스 공급자는 무선 랜 존의 인증, 권한, 과금, 로밍 등 많은 문제점들이 생기게 되었다.

본 논문 Ⅱ,Ⅲ장에서는 각각 무선 네트워크 기술인 802.11의 기본 인증 방식과 무선 네트워크 보안책인 802.1x의 인증 방식에 대해서 설명하고 Ⅳ장에서는 각 인증의 효율성을 연구하여 제한된 환경에서의 효과적인 보안 시스템을 설계를 위한 방안을 제시하고 V장에서 결론을 맺는다.

Ⅱ. 802.11 기본 인증 방식

802.11 프로토콜의 인증 방식에 대해 설명하기 전에 유선 랜에서 암호 / 인증으로 자리 잡은 PKI(Public Key Infrastructure, 공개키 기반 구조)에 대해서 보면 PKI란 인터넷과 같이 안전이 보장되지 않은 공중망 사용자들이 신뢰할 수 있는 기관에서 부여된 한 의 공개키와 개인키를 사용하여 안전하게 데이터나 자료를 교환할 수 있게 해준다. PKI의 PKI의 구성요소는 일반적으로 알려져 있지만 공급자 별로 많은 접근 방식이나 서비스들이 생겨나고 있으며, 그동안에도 PKI를 위한 인터넷 표준은 계속하여 작업이 진행되었다.

PKI 구성요소

- 디지털 인증서를 발급하고 검증하는 인증기관
- 공개키와 정보를 포함하는 인증서
- 인증기관의 입증을 대행하는 등록기관
- 인증서를 보관하는 하나 이상의 디렉토리
- 인증서 관리 시스템

PKI 제공자

- PKI가 사용하는 알고리즘 개발했던 RSA

- 인증기관으로 활동하며 인증기관 소프트웨어를 판매하는 Verisign
- 넷스케이프 디렉토리 서버에 기반을 둔 VPN-1 Certificatie Manger의 Check Point

무선 랜은 비교적 단순한 유선 Ethernet 프로토콜과 달리 RF(무선 주파수) 데이터가 송출되는 것을 클라이언트가 수신하는데 RF만 같다면 누구든 수신할 수 있으므로 이 과정을 보호하는 접근 제어인 인증에 관한 부분이 보안 메카니즘으로 요구된다.[1]

1. 개방 인증 방식

개방 인증 방식은 그림 1과 같이 통신 간 메시지를 암호화 하지 않은 평문으로 통신하며 인증 단계는 6단계로 구성되어 있다.

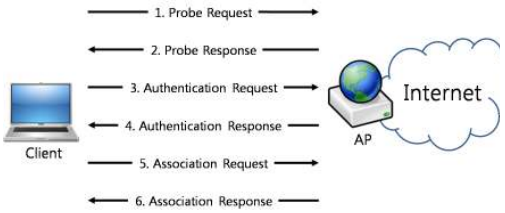

그림 1. 개방 인증 방식

1. 클라이언트가 모든 채널에서 프로브 요청 프레임 송출
2. 수신된 AP는 프로브 응답 프레임 응답
3. 클라이언트는 응답한 AP중 가장 적합한 AP 결정 후 인증 요청 전송
4. AP 인증 응답 전송
5. AP에게 연결 요청 프레임 전송
6. AP는 연결 응답을 전송

도중 인증이 거부 될 경우엔 거절 메시지를 전송하게 된다. 개방 인증 방식과 같은 암호화를 적용하지 않는 평문 전송 방식의 경우 도청이나 신분 위장 등 다양한 위협에 노출되기 쉽다.

2. WEP 인증 방식

WEP 인증 방식에는 Open System Authentication과 Shared Key Authentication 두 가지 방식으로 동작한다. Open System Authentication 방식은 단순히 데이터 프레임의 암호화를 사용할 뿐 어떠한 인증도 일어나지 않는다. 인증이 일어나지 않기 때문에 인증서 또한 필요하지 않다. 사용자는 AP에 인증 받기 위하여 적합한 WEP Key만 가지고 있으면 된다.

클라이언트는 AP에게 연결 요청을 한 후 인증 과정을 거치게 된다.

1. 클라이언트가 AP에게 인증 요청 전송
2. AP는 인증 응답과 자신의 인증 방식과 암호화 방법을 전송
3. 자신의 상태와 정보 초기값을 AP에게 전송
4. AP는 clear-text challenge를 전송하고 클라이언트와 그 정보를 기억
5. 클라이언트는 수신한 challenge text를 설정된 WEP Key를 이용해 암호화 한 후 인증 요청 메시지를 전송
6. AP는 수신한 데이터를 복호화 하여 자신이 보낸 clear-text와 비교, 확인 하여 클라이언트의 인증여부를 판단
7. 인증 완료 후 데이터를 WEP Key를 사용하여 암호화 후 데이터 통신

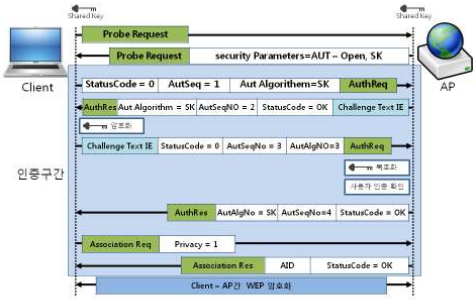

그림 2. WEP 인증 방식

3. WPA / WPA2 인증 방식

WPA는 802.11i가 완성되기전 WEP의 취약점을 일시적으로 보안하기 위해 개발된 프로토콜이다.

WPA는 TKIP 암호화 방식을 사용하고 WPA2는 PSK, AES 암호화 방식을 사용하는 것이 다르다. 사용자 인증은 그림 3의 기본 요청이 완료된 후 802.1x의 확장 인증 방식인 EAP를 사용하여 인증을 실행하게 된다.

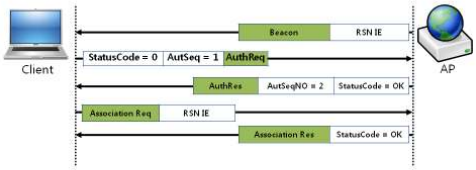

그림 3. WPA / WPA2 인증 방식 기본 요청

Ⅲ. 802.1x 인증 방식

802.1x는 802.11의 확장 보안 인증 프로토콜이다. 포트 기반 네트워크 접근 제어를 이용한 인증을 수행하고 인증이 완료되면 가상 포트를 이용해 통신이 이루어진다. 802.1x에서 사용하는 확장 인증 프로토콜 (Extended Authentication Protocol-EAP)은 EAP-MD5, EAP-TLS, EAP-TTLS, LEAP, PEAP 등이 있고 이를 표1에 정리하였다. EAP 인증은 상호 인증 방식과 클라이언트 인증으로 나눌 수 있고 상호 인증 방식에도 인증서 기반과 그렇지 않은 경우로 나눌 수 있다.

단일 인증 방식에는 EAP-MD5가 있고 쌍방향 인증에는 TLS, TTLS, PEAP 등이 있다. 그리고

PAC 기반의 EAP-FAST가 있다.[2]

표 1. EAP 인증 종류 / 특성

유형	MD5	TLS	TTLS	PEAP	FAST	LEAP
Client 인증서	무	유	무	무	무	무
Server 인증서	무	유	무	유	무	무
WEP 키관리	무	유	유	유	유	유
인 증 방 향	일방	쌍방	쌍방	쌍방	쌍방	쌍방
구 축 난이도	하	상	중	중	중	중
보안성	하	상	상	상	상	중

EAP 인증은 사용자 정보를 사용하여 인증하기 때문에 이를 처리할 수 있는 인증 서버(radius)를 그림4와 같이 설치할 필요가 있다.

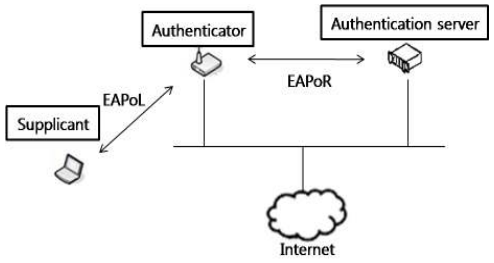

그림 4. 8021x 기본 요소

EAP의 인증 절차는 그림5와 같은 순서로 이루어진다.

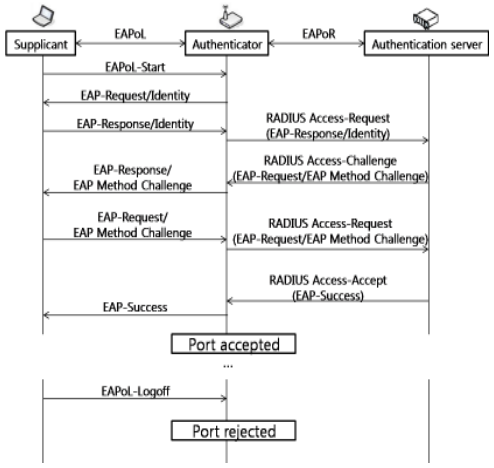

그림 5. EAP 인증 절차

1. 새로운 요청자를 발견하면, 인증자의 포트 스위치가 활성화 되고 “unatuthorized" 상태로 바뀐다.
2. 인증을 하기위해 인증자는 주기적으로 EAP - request Identity 프레임을 송출한다. 요청자는 이 프레임을 수신하고, 사용자 ID와 같은 식별자를 포함하는 EAP-Response Identity 프레임을 응답하게 된다. 그 후 인증자는 이 Identity response를 RADIUS Access-Request packet 안에 캡슐화하여 이 정보를 인증 서버로 보낸다.
3. 인증 서버는 인증자에게 응답으로 EAP Method가 포함된 Radius Access-Challenge packet을 인증자에게 보내다. 인증자는 EAPOL(EAP over Lan) 프레임에 EAP request를 캡슐화해서 요청자에게 전송한다.
4. 만약 인증 서버와 요청자가 EAP Method를 동의하면, 인증 서버가 EAP-Success 메시지를 응답할 때 까지 이들 간에 EAP Request 와 EAP Response 가 보내진다. 인증이 성공되면, 모든 트래픽들을 허용한다.

다음의 EAP Method 들의 인증절차는 위에 기술된 802.1x의 인증과정 중간에 위치하게 된다. (Method를 선택하고 인증서버에서 EAP-Success (RADIUS Access-Accept)를 보내기 전의 중간과정이다.)[2]

802.11에서 정의한 프레임워크에서는 안전한 키 분배와 상호 인증 지원원을 요구하고 있는데 이를 위한 방안으로써 여러 무선랜 사업자들은 각각 독자적인 EAP 인증 혀형을 개발하고 있다. 주로 사용되는 EAP 인증 유형은 다음과 같다.

1. EAP-MD5

가장 초기의 인증 유형으로 모든 EAP 인증의 필수 구현 방식이다.

2. EAP-TLS

사용자와 radous서버와의 인증서를 서로 교환함으로써 인증서 기반의 상호 인증을 제공한다. 암호화를 위하여 동적인 WEP 키를 생성하여 분배한다.[4]

3. EAP-TTLS

TLS의 확장 형태로 radius의 인증서만을 필요로 하는 형태로 TLS 터널링을 통해 전체 네트워크상에서 사용자의 익명성이 보장된다.[3]

4. PEAP

클라이언트와 인증 서버 간 터널링을 사용하여 인증을 제공한다. TTLS와 유사한 방식으로 동작하며 이 방식 또한 서버 측 인증서만을 필요로 한다.

5. EAP-FAST

Cisco에서 개발한 인증방식으로 서버 측 인증서만으로 쌍방 인증을 제공한다. 인증 서버가 동적으로 관리할 수 있는 PAC(Protected Access Credential)를 사용하여 구현된다. 인증 서버는 클라이언트에게 수동(디스크, 보안 네트워크 분배) 또는 자동(주파수를 통한 무선 분배)으로 인증서를 1회 분배하여 이를 이용하여 인증을 실행한다.[3]

6. LEAP

시스코 무선 랜 AP에서 주로 사용되는 프로토콜로 데이터 전송은 dynamic WEP key를 이용하여 암호화 되며 상호인증을 지원한다.[4]

Ⅳ. EAP의 효율성

이번 장에서는 위에서 언급한 EAP Method를 활용하기 위한 기본 인프라와 그 효율적인 우영을 위한 방안을 제안한다.

1. EAP-MD5

MD5 자체로도 인증 기능을 제공하지만 그 보안성은 너무나 취약하다. 암호화를 제공하는 해시 함수는 딕셔너리 공격에 취약하고, 키 생성에 관여하지 않는 점에서 dynamic WEP이나 WPA, WPA2에 적합하지 않다. 그리고 클라이언트는 AP를 인증할 수 없기 때문에 불법 AP의 스니핑에 노출이 쉽다. MD5의 구현은 radius 서버만을 필요로 하여 그 어떤 Method보다 구현이 단순하다. 하지만 취약한 보안성 때문에 MD5만 사용하기를 권장하지 않는다.

2. EAP-TLS

TLS를 구현하기 위해서는 radius서버와 각 워크스테이션에 클라이언트 인증서를 설치하기 위한 SA 서버가 필요하다. TLS방식은 보안 기능은 뛰어나지만 그만큼 설치가 어렵고 모든 클라이언트에 인증서를 설치해야 한다는 불편함이 있다. PKI 인프라를 관리하기 위해 WLAN 관리 외에 추가 관리 전문 기술과 시간이 필요하며 일정기간 이후에 인증서를 재발행 하는 등 유지 비용 또한 지속적으로 소비되기 때문에 최상위 보안을 유지하기 위한 곳에서만 사용하길 권장한다.

3. EAP-TTLS

TTLS는 TLS과 비교하여 보안이 약한 편이지만 서버 측의 인증서를 설치하지 않아 네트워크 구축이 용이 하다. 하지만 클라이언트는 TTLS 접속 소프트웨어를 설치해야 한다. TTLS 방식은 설치가 손쉽고 보안성도 보장되지만 TTLS는 주로 Funk에서 관리하며 요청자 및 인증 서버 소프트웨어에 대한 대가를 별도로 지불해야 한다.

4. PEAP

PEAP는 Cisco와 Microsoft에서 지원하는 방법이며 추가 비용을 지불하지 않고 사용이 가능하다. LEAP에서 PEAP로 데이터 전송도 ACS 인증서버를 통해 가능하다. 사용자 측면에서 ID와 Password만 입력하면 간단히 인증이 가능하며 설치 / 유지 관리가 쉽다.

5. EAP-FAST

시스템 구성이 간편하고 별도의 SA 서버를 필요로 하지 않기 때문에 강력한 암호 정책을 필요로 하지만 SA의 구축을 원하지 않는 기업의 경우 이 방식이 유리하다.

6. LEAP

이 방식의 경우 암호화 알고리즘을 선택할 수 있기 때문에 암호화 알고리즘을 어떤 것을 사용하느냐에 따라 보안 강도가 변화한다. Cisco 어뎁터가 구축되어 있는 경우 별도의 설치 비용 없이 사용할 수 있으며 암호 키 관리와 인증서를 사용하지 않는 방식으로 유지 / 관리가 편리하다.

그림 6, 7, 8의 그래프는 각 Method들을 상대적으로 표현한 그래프이다.

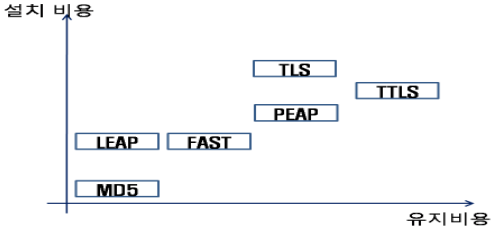

그림 6. EAP 설치비용 / 유지비용

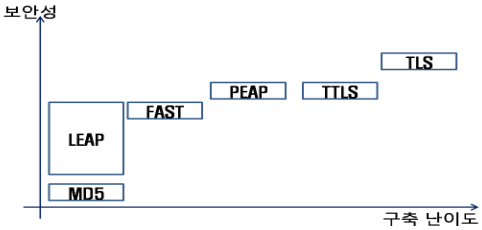

그림 7. EAP 보안성 / 구축 난이도

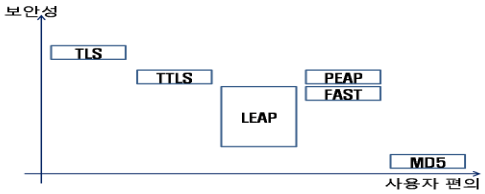

그림 8. EAP 보안성 / 사용자 편의

Ⅴ. 결 론

무선 랜 존이 급속도로 확장 되어가는 현재 서비스 공급자는 보안성과 사용자의 편의성 두 가지 관점에서 많은 고민을 하고 있다. 하지만 어느 하나도 포기할 수 없는 중요한 과제이며 소홀히 생각할 수 없는 문제이다. WEP과 WPA의 경우엔 보안 취약점이 존재하며 WPA2의 경우 시스템 인프라 구축에 자원이 소비된다. 서비스 공급자는 자신의 인프라와 소비자 편의를 고려한 무선 랜 존을 구성해야 될 것이다.

카페와 같은 오픈된 공간에서의 무선 랜 존에서는 개방 인증 방식이 주로 사용되고 있는데 이는 보안상 취약한 구조이다. 하지만 인증 방식을 강화하게 되면 사용자 등록과 인증 과정 때문에 사용자들에게 배척당하게 된다. 이를 위한 OTP를 이용한 인증에 관한 추가 연구가 요구된다.

참고문헌

[1] Willam Stallings, Data and Computer Communications 8ed, Prentice Hall, 2007.
[2] RFC 2284
[3] http://www.cisco.com/en/US/products /hw/wireless/index.html
[4] 송창렬, 정병호, 조기환, “무선랜 보안 구조”, 정보과학회지, 한국정보과학회, 2002.