고속 무선랜 통신을 위한 보안 프로토콜에 관한 연구

정우길* · 박경수** · 이영철*

*경남대학교 정보통신공학과
**원테크정보기술(주)

Analysis of Secure Protocol for Hight Speed Wireless LAN Communication

Woo-Kil Jung* · Kyung-soo Park** · Young-Chul Rhee*

*Div. of Information & Comm. Eng., Kyungnam University

**WONTECH L.T.D

E-mail : realgisa@hotmail.com, micropt@kyungnam.ac.kr

요 약

본 논문에서는 무선랜 시스템에서 보안상의 취약점을 해소하기 위해 적용되고 있는 보안 기법들에 관해 분석하였다. WLAN에서 적용되고 있는 보안규정 WEP는 RC4 스트림 키퍼의 특징에서 오는 IV Reuse 문제 및 ICV를 생성하는 CRC-32의 선형특성에 따른 문제를 분석하고 현재 사용되는 보안기법인 액세스컨트롤의 강화와 WEP 키관리 및 VPN에서의 사용자 인증알고리즘 및 데이터 암호화기술을 분석하고, 802.11a에서 보안모델의 나아갈 방향을 제시하였다.

Ⅰ. 서 론

최근 급부상한 무선LAN 시장의 중심에는 IEEE 802.11b 표준을 따르는 무선LAN 시스템이있다. 2.4GHz 대역에서 11Mbps의 데이터 전송속도를 지원하는 IEEE 802.11b는 무선 LAN 시장의 급성장을 예고했다. 하지만 그 효용성과 달리 보안 측면에서는 많은 문제점이 지적되고 있다[1]. IEEE 802.b 표준은 WEP(Wired Equivalent Privacy) 프로토콜을 사용하여 보안을 하고 있다 그러나, 공중 무선 LAN 서비스를 제공하기에는 보안에 취약한 것으로 알려져 있어 802.1x 표준을 구현할 것을 요구하고 있다[1]. 802.1x는 WEP을 보완하여, 기존 무선랜 보안 메커니즘인 WEP과 IP 환경에서의 AAA(Authentication, Authorization, Accounting)프로토콜을 잘 연동시켜주기 위해 부가 기능 제공한다. 이용자 단말과 인증 서버간에 EAP(Extensible Authentication Protocol) 프로토콜이 돌아갈 수 있게 함으로써, AAA 서버가 이용자를 인증할 수 있도록 한다. 프로토콜 수행의 결과로 이용자 단말과 AAA 서버에는 서로 동일한 암호화 key가 생성되며, AAA 서버는 이 key를 AP로 전달해주고, AP는 이 key를 기존 WEP 암호화 메커니즘을 위한 WEP key로 이용하여 단말과 AP간의 무선 구간을 보호한다[2]. 그러나, 802.1x 역시 보안을 완벽히 제공하지는 않는 것으로 알려져 있다. 802.1x는 접속을 요청하는 단말(supplicant), 인증을 수행하는 장치(authenticator), 그리고 인증서버(AAA 서버)로 구성되어 있는데, 인증을 요청하는 단말과 인증수행 장치 사이에 다른 불법 단말이 끼어들어 정보를 엿듣는 man-in-middle문제와, 인증을 요청하는 단말의 인증을 가로채는 Hijack 문제가 발생할 수 있다[3]. IEEE에서도 이를 보안하기 위해 RSN(Robust Security Network)을 제안하고 있으며, 802.11i에서도 보다 진보된 보안 메커니즘에 대해 연구가 진행중이다. 802.1x의 표준이 발표되길 기다리는 동안 설치하고 있던 무선랜에서는 그동안 보안의 해결을 위해 RADIUS(Remote Authentication Dial-In User Service) 서버의 인증이나 VPN(Virtual Private Network)등 여러 가지 방법이 고려되고 있다. VPN을 이용하는 것은 무선랜의 보안 측면에서 큰 장점이 있다. 사용자 인증뿐만 아니라, 데이터 자체에도 고급 암호화 기술을 사용할 수 있기 때문이다[4]. 그러나 관리측면에서 VPN을 이해하기 위한 노력과 VPN의 문제 발생시 해결을 위한 노력이 쉽지만은 않은 상태에 그 발전 가능성은 대단하다.

II. 현재 사용되고 있는 보안기법들

IEEE 802.11b 표준에는 액세스제어와 프라이버시를 보장하는 구성요소를 포함하고 있는데, 액세스제어는 SSID(Service Set Identifier) 메커니즘을 통해, 프라이버시는 WEP(Wired Equivalent Privacy) 메커니즘을 통해 제공하고 있다. SSID 메커니즘은 사용자가 AP에 접속하기 위해서는 SSID를 지정해주어야 한다. 그러나 대부분의 무선랜 카드는 프로브 리스판스(Probe Response)와 비콘(Beacon)신호를 이용해, AP의 SSID를 획득할 수 있으므로 사용자가 SSID를 모르더라도 AP에 접속할 수 있는 방법을 제공하고 있다. 이러한 접근을 막기 위해 비콘이나 프로브 리스판스에 SSID를 숨기는 방식이 권장되고 있다. 그러나 사용자가 AP에 접속되는 순간에 SSID가 실려가므로 주의깊은 공격자라면 이를 통해 SSID를 알아낼수 있을 것이다. WEP 메커니즘은 유선랜과 비슷한 수준의 보안을 무선랜에서 제공한다는 의미를 가진 WEP을 통해 인증 및 보안서비스를 제공한다. WEP는 RC4 스트림키퍼(Stream Cipher)를 암호화알고리즘으로 사용하고, CRC-32를 이용해 데이터 무결성을 확인하며, 24비트의 IV(Initialization Value)를 이용해 키 스트림을 생성하는 구성을 가진다[1].

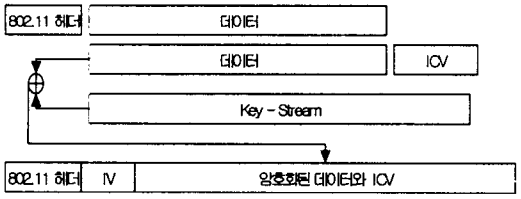

그림 1. Encrypted WEP Frame

그림 1.은 데이터로부터 CRC-32를 계산하여 ICV (Integraty Check Value)를 생성하고, 이 ICV와 데이터를 키스크림과 XOR(exclusive-or)하여 데이터를 암호화(C) 블록다이어그램이다. WEP는 통신 노드간에 공유된 비밀키 k(WEP 키)를 사용하여 전송 데이터를 암호화 하는데 암호화 과정은 다음과 같다[5].

■ Checksumming : 먼저, 메시지 M 에 대한 무결성 체크섬인 c(M)을 계산한 다음, 메시지 M에 c(M)을 추가하여 평문 P = <M, c(M)>을 만든다. 이렇게 만들어진 평문 P가 두 번째 단계의 입력으로 들어간다.

■ 암호화 : 초기백터IV와 공유된 비밀키 k 를 조합하여 RC4에 의해 스트림을 생성함으로써 이루어진다. 이렇게 생성된 keysream은 RC4(v,k)로 나타낸다. 이렇게 생성된 keystream과 checksumming 단계에서 생성한 평문 P를 XOR(⊕로 표현)를 수행한 결과가 식 (2-1)과 같이 얻을수 있다.

$$C = P \oplus RC4(v,k) \qquad (2\text{-}1)$$

■ 전송 : 마지막 단계로, IV와 암호문 C를 데이터 링크계층을 통해 전송한다.

키 스트림 생성은 24비트 난수와 키번호로 이루어진 이렇게 암호화한 데이터를 받은 수신측에서는 식 (2-2)와 같이 역과정을 통해 데이터를 해독하는데, 수신된 IV로부터 키 번호와 24비트 난수를 알아낸 후, 지정된 키와 이난수를 이용해 RC4 키 스트림을 생성해 데이터를 해독하고 마지막으로 CRC-32로 계산한 값과 수신된 ICV를 비교해 데이터 무결성을 확인함으로써 복호화 과정을 마치게 된다.

$$\begin{aligned} P' &= C \oplus RC4(v,k) \\ &= (P \oplus RC4(v,k)) \oplus RC4(v,k) \\ &= P \end{aligned} \qquad (2\text{-}2)$$

WEP에서는 몇가지 문제점을 내포하고 있다.

■ 부르트포스 공격의 위험 : 40비트 키 길이는 현재 컴퓨팅 파워에 비교할때, 너무 작다 . 대부분의 업체는 이를 해결하기 위해 128비트 WEP를 지원하고 있다. 하지만 이또한 표준으로 자리잡고 있지 않아 호환성 문제가 대두되고 있다.

■ IV Reuse 문제 : WEP에서 사용하고 있는 RC4 스트림 키퍼의 특징은, IV값이 같다면 키스트림이 같다는 것이다. 동일한 IV와 동일한 키를 이용해 암호화된 두개의 스트림 키퍼의 경우, 두 암호문을 사용하여 식(2-3)과같이 평문을 알아낼수 있다[5].

$$\begin{aligned} &\text{if, } C_1 = P_1 \oplus RC4(v,k) \\ &\quad C_2 = P_2 \oplus RC4(v,k) \text{ 이라면,} \\ &C_1 \oplus C_2 = (P_1 \oplus RC4(v,k)) \oplus (P_2 \oplus (RC4(v,k)) \\ &\qquad = P_1 \oplus P_2 \end{aligned} \qquad (2\text{-}3)$$

가 되어 두개의 평문을 알아낼 수 있게 된다.

이 문제의 해결은 단순히 키 길이를 늘려서는 해결되지 않고, IV값이 재사용되지 않게 해야한다.

■ 인증의 선형성 : WEP는 전송중 데이터가 수정되지 않았다는 것을 보장하기 위해, ICV를 사용한다. 그러나 ICV를 생성하는 CRC-32가 선형특성을 가지고 있으므로 공격자가 키를 알지 않고서도 전송중인 패킷을 변경하는 것이 가능하다. 이러한 단점을 극복하려면, MD5-HMAC 또는 SHA1-HMAG과 같은 키를 이용한 메시지 인증코드를 사용해야만 한다.

이러한 문제점들 때문에 WEP는 하이엔드 분석장비로 수 초만에 암호를 풀 수 있고 사용자들이 이동성을 얻기 위해서는 모든 AP 들에서 동일한 암호키를 사용해야 한다. 이와같이 많은 사람들이 공유하는 SSID나 WEP 키를 사용하는 보안은 신뢰성이 적고, 많은 MAC 주소를 사용자별로 필터링 하기가 어렵다는 것은 이미 널리 알려진 사실이다. 이러한 문제를 해결하기위해 128비트 WEP키를 사용하고 일정 시간마다 키를 변경함으로써 공격의 위험성을 줄이 수 있다. 그러나 대개의 경우, 키분배가 자동으로 이루어지지 않아서 손수 단말에 변경을 가해야 하므로 확장이 어려어 대규모 사업장에는 적용하기 어렵다. 관리는 통한 보안 방안에서는 IEEE 802.1x를 이용한 키 분배 및 변경방법이 가장 좋은 대책으로 여겨지고 있다[2].

III. 802.1x를 이용한 사용자 인증 및 VPN을 이용한 데이터 보안

IEEE 802.1x 는 원래 스위치 장비에서 포트별 액세스 컨트롤을 위해 표준화가 진행되고 있었으나 무선랜의 보안문제가 대두되면서, 무선망 보안을 위한 표준으로 더 많이 알려졌다. 이표준의 핵심은 EAP (Extensible Authentication Protocol)로 구성원인 인증자(Authenticator : AP), 단말(Supplicant), 인증서버(보통 래디우스 서버) 사이에서 많은 인증프로토콜이 구동 될 수 있는 프레임워크를 제공한다[1].

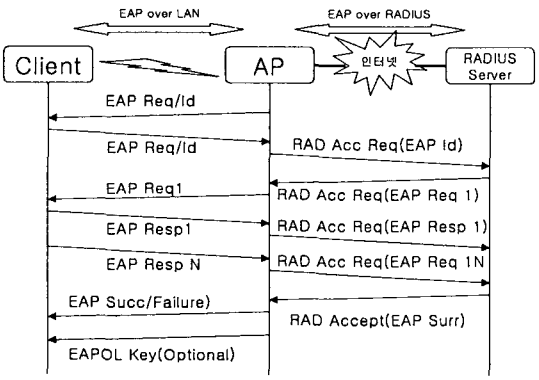

그림 2. 802.1x 구조 및 인증절차

IEEE 802.1x 시스템의 구조는 그림 2 처럼, 크게 supplicant기능을 수행하는 Client, Authenticator 기능을 수행하는 AP, Authenticator와 연결된 인증서버(RADIUS)로 구성된다. 802.1x 는 EAP(Extensible Authentication Protocol, RFC2284) 구조를 채택했다. 또한 사용자 별로 다이나믹하게 키를 만들어 상호 인증을 하게 했으며 패킷 단위 까지도 승인을 받게 준비했다. EAP 는 PPP를 위해 많이 사용하고 링크를 제어하는 특정 프로토콜에 한정하는 승인 메카니즘을 규정하지 않고, 단순한 패스워드뿐만 아니라 지문등의 생체인식이나 스마트 카드등의 패스워드가 아닌 것 까지 지원하도록 설계하였다. 802.1x 자체는 PAP(Password Authentication Protocol)나 CHAP(Challenge Handshake Authentication Protocol)승인을 지원하지 않기 때문에 RADIUS사용자 패스워드를 숨기는 메카니즘이 사용자의 암호에는 적용되지 않아 Man-In-Middle attack에 침입당할 수도 있으며, AP와 상호인증부재를 이용한 AP와 Supplicant 사이에서 불법 단말이 낄 수 있는 기법과 EAP 성공 메시지를 위조한 MIM attack 과 그림 3.과 같은 공격자가 MAC address를 변경한 공격이 가능하다.

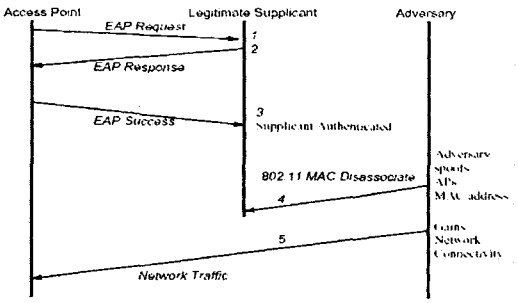

그림 3. The Session Hijacking

802.1x에서는 네트워크에 대한 전반적인 접근에 대한 사용자 인증만을 정의하고 있기 때문에 인증된 사용자에 대한 더 이상의 제어는 불가능하다. 한번 인증을 거친 사용자는 해당 네트워크에 자유롭게 접근할 수 있게 되는 것이다. 이는 일단 외부 사용자가 Firewall 인증 후 내부 망에 들어오고 나면 내부의 모든 IT 자원에 쉽게 접근할 수 있다는 것과 같다. 이러한 문제점을 극복하기 위해 사용자의 인증뿐만 아니라 데이터 자체에도 고급의 암호화 기술을 사용할 수 있는 VPN이 큰 장점으로 부각되고 있다[6].

VPN 기술을 구현하기 위해 반드시 충족시켜야 하는 요구사항은 안정성과 보안이다. 그리고 VPN을 구성하는 모든 지점에 위치한 하드웨어와 소프트웨어간의 상호연동이 중요한 이슈가 된다. 이런 요구조건을 만족시키기 위해서 IETF(Internet Engineering Task Force)에서는 IPSec 이라는 프로토콜을 규정하게 되었고 이것은 TCP/IP로 구성된 네트워크 환경에서 안전한 통신을 가능케 해주는 핵심이 되었다[7].

IPSec이 기존의 보안 프로토콜에 비해 많은 관심을 받게 된 가장 큰 이유는 Layer3에서 동작한다는 것과

Open Standard 이면서 기밀성, 데이터물결성과 데이터 근원지에 대한 인증 등 네트워크 보안에서 필요로 하는 각종 요소를 모두 구비하고 있기 때문이다. 무엇보다도 이종 기기간의 상호연동을 보장하고 인증 메커니즘, 암호 알고리즘과 보안 정책 등을 수립하는데 있어서 많은 유연성을 갖고 있는 것이 IPSec의 최대 강점이라고 할 수 있다. IPSec을 구성하는 3대 요소는 다음과 같다.

A. AH(Authentication Header)

인증 헤더는 IP 데이터그램을 인증하기 위해 필요한 정보를 포함하는 방법으로 보안 효과, 특히 데이터의 인증과 무결성을 보장한다.

그림 4.는 인증 헤더로 보호된 IP 페이로드의 구조를 나타낸다.

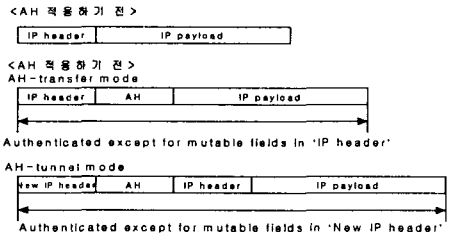

그림 4. 인증 헤더로 보호된 IP Payload 구조

B. ESP(Encapsulation Security Payload)

암호화 기법을 사용하여 데이터의 무결성, 리플레이 방지, 비밀성의 기능을 제공한다.

그림 5.는 ESP 구조를 나타낸다. ESP내의 IP데이터그램 전체를 캡슐화하는 터널 모드와 트랜스포트 계층의 세그먼트를 캡슐화하는 트랜스포트 모드로 되어 있다.

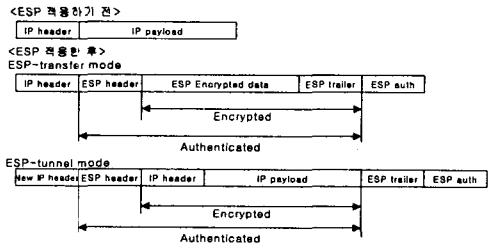

그림 5. ESP의 구조

C. IKE(Internet Key Exchange)

ESP와 AH에서 사용하게 될 키관리 프로토콜로 ISAKMP(Internet Security Association and Key Management Protocol)의 프레임워크에 Oakley 키 결정 알고리즘을 결합한 형태로서 IETF Working Group에 의해 표준으로 제정되었다.

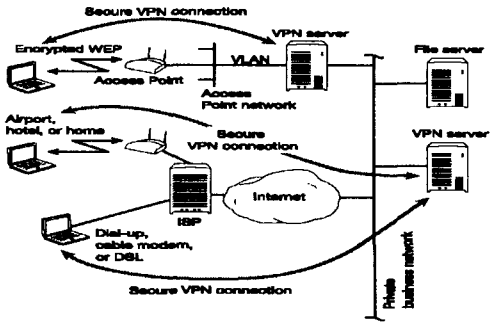

그림 6. 802.11a를 위한 VPN 보안

그림 6.은 무선LAN에서의 VPN구성을 보여주고 있다. VPN을 이용해 전화회선, Cable modem, DSL을 사용하여 인터넷에 연결한다면, 원격잡업등을 VPN Server와 WLAN에 연결할 수 있으며, 공공이나 다른 장소에서 공중 무선 접근 지역에서는 WLAN과 VPN의 설정으로 사용할 수 있다.

AH, ESP, IKE는 서로 유기적으로 동작하면서 네트워크 데이터를 가장 안전하게 보호해 줄 수 있는 솔루션이다.

IV. 결 론

현재의 시장은 무선LAN기술 및 인증, 보안, QoS 등을 만족시키지 못해 공중무선LAN에서의 한계를 들어내고 있다. 802.1x의 응용은 보안과 관리의 측면에서 획기적이기 까지 하다. 802.1x는 인증이 사용자의 신원을 파악하는데 있어서 강력한 메커니즘을 제공한다. 그러나 802.1x로도 부족한 무선 LAN 보안 문제를 해결하기 위해 현재 표준화를 준비하고 있는 802.1e가 급부상하고 있다[6]. 네트워크 접근제어의 한계에 대해 VPN은 WEP와 MAC address Filtering에 대한 대안으로 가장 적당한 것으로 알려졌다. VPN과 802.11a의 조합은 무선 네트워크의 안전에 필요한 이상적인 해답이다. 이과 같은 해답과 함께 무선 AP는 VPN 조작안전과 WEP암호와 함께 open상태에서 접근하기 위해 형성된다. VPN Server는 정보보안과 인증, 무선랜 전체의 암호화를 제공한다. MAC address Filtering과 함께한 WEP와는 달리 VPN은 사용자의 수가 많아져도 사용이 가능하며, 무선랜의 보다 쉽고, 경제적인 확장을 위해 필요한 솔루션이 될 것이다. 앞으로 802.11a에서의 VPN의 구현과 끊임없이 보안에 관한 기능을 향상시켜 늘 최상의 방어막을 갖도록 노력하는 것이 향후 연구 과제이다.

참고문헌

[1] Network Times, "무선 LAN 시대보안은 선택이 아닌 필수", 1 2002.

[2] Sultan Weatherspoon, "Overview of IEEE 802.11b Security," Network Communications Group, Journal 2000.

[3] www.isa.ac.cs.bcrkeley.edu/isaac/wep-faq. html(University of California at Berkeley-provides "frequently asked qusetions" on WEP setup, problems, and attacks).

[4] www.cisco.com (Ciscowebsite-provides information on securing wireless networks).

[5] R.L. Rivest, "The RC4 Encryption Algorithm" , RSA Data Security, Inc, Mar 1992.

[6] RFC 2401, Security Architecture for the Internet Protocal, November 1998.

[7] RFC 2402, IP Authentication Header, November 1998.