Wireless Network에서 개선된 PPP CHAP를 사용한 효율적 인증 방법

*강남구^{O} , *김수성, *유행석, *장태무
동국대학교 컴퓨터 공학과
{whitekis^{O}, kercury, heehang ,jtm}@dongguk.ac.kr

Efficiency Authentication Method Using Enhanced PPP CHAP On Wireless Network.

*Nam-Gu, Kang ^{0} ,*Su-Sung Kim, *Hang-Suk Yoo, *Tae-Mu Chang
* Dept. of Computer Engineering, Dongguk University

요 약

무선 통신의 발달로 언제 어디서나 누구와도 통신이 자유롭게 되었다. 하지만, 무선 통신을 사용하게 됨으로써 통신 사용자와 액세스 포인트, 액세스 포인트와 서버(Server)가 통신을 할 경우 유선 네트워크와는 다른 인증 방식이 요구되었다. 무선 네트워크에서 사용자 인증을 위해 801.x EAP, SSID, CHAP 및 WEP를 이용한 다양한 인증 방식이 사용되고 있다. 본 논문에서는 사용자를 안전하게 인증할 수 있는 효율적인 인증 방법을 제안한다. 여기서는 기존의 PPP CHAP을 수정하여 인증 서버와 사용자간의 상호 인증을 할 수 있도록 했다. 또한 강한 일-방향 해시 함수(Strength One-Way Hash Function)을 사용하여 생성된 결과 값을 일회용 패스워드(One Time Password:OTP)로 사용하여 재공격(Reply Attack)을 방지했다.

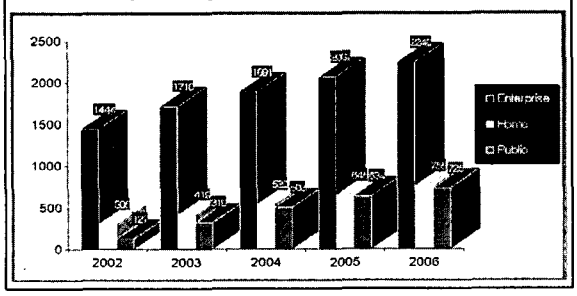
1. 서 론

많은 사람들이 "선(Line)으로 부터의 자유"를 주장하며 언제 어디서나 네트워크(Network) 환경에 보다 손쉽고 빠르게 접속하기 위해 무선 랜(Wireless Lan)을 사용한다.

2002년 KT, 하나로 통신등 사업자들이 대학, 호텔, 일반 기업, 가정에 핫스팟(Hot Spot) 설치와 공중 무선 랜 서비스의 확대로 무선 랜 사용자는 [그림 1]에서 보듯이 꾸준히 증가하고 있다[1]. 그러나 무선 랜은 설계 시 부터 보안에 큰 관심을 두지 않았다. 무선 랜은 브로드 캐스팅(Broadcasting)이 가지는 특성으로 인해 전파 스캐너만 있으면 언제나 무선 데이터(Data)의 프라이버시(Privacy)를 침해 할 수 있는 무선 트래픽(Traffic) 감청이 가능하다[1,2].

유선 랜(Wire Lan)에서는 물리적으로 연결된 단말기들만이 트래픽을 감청할 수 있다. 하지만 무선 랜의 경우 브로드캐스팅 망이므로 액세스 포인트(Access Point)의 수신 영역 내에서는 모든 사람들이 송·수신되는 통신 데이터의 내용을 쉽게 접할 수 있다. 예를 들어 LINUX 랩탑 컴퓨터와 TCPDUMP와 같은 프로그램만 있으면, 누구든지 이 문제점을 이용하여 임의의 무선 랜 상에서 돌아다니는 모든 데이터 패킷들을 받아서 저장할 수 있다[3].

[그림 1] 무선 랜 시장 동향[4]



따라서 무선 랜에서는 정당한 수신자 이외의 다른 사람들에게 메시지(Message)의 내용을 알 수 없도록 하는 데이터의 프라이버시와 상호 인증 서비스가 매우 중요하다. 무선 랜을 사용하여 네트워크 접속할 경우 두 개의 보안 구간이 필요하다. 하나는 사용자(또는 클라이언트)와 액세스 포인트 사이에서의 무선 접속 구간에 대한 보안이고, 다른 하나는 액세스 포인트와 인증 서버사이의 유선 구간 보안이다. 여기서 액세스 포인트는 유선 랜과 무선 랜을 연결 시켜 주는 장치이다.

본 논문에서는 사용자와 액세스 포인트 사이에서의 무선 접속 구간에 대한 보안에 초점을 맞추어, 1장 서론에 이어 2장의 관련 연구에서는 현재 사용되고 있는 인증 방법과 문제점을 살펴보고 3장에서는 보다 효율적 인증 방법인 CHAPv3(가칭)을 제안한다. 마지막으로 4장에서는 결론 및 향후 과제에 대하여 기술 하였다.

2. 관련 연구

IEEE 802.11b표준은 무선 랜의 접근제어 및 프라이버시에 2가지 방식의 보안 메커니즘을 무선 랜 보안(Wireless LAN Security)으로 정의하고 있으며, 하나는 서비스 집합의 SSID이고 다른 하나는 유선 랜과 동등한 형태의 보안 메커니즘인 WEP이다[5]. SSID와 WEP의 많은 문제점들이 발견되고 난후 SSID와 WEP의 문제점들을 보완하여 나온 다양한 인증 메커니즘들이 있다. 예를 들면 EAP(Extensible Authentication Protocol) Method나 마이크로소프트사에서 CHAP을 수정하여 제안한 MS-CHAPv1, MS-CHAP-v2등 있다.

2.1 SSID(Service Set Identifier) 와 WEP(Wired Equivalent Privacy)

SSID는 무선 랜 서브시스템(Sub System)에서 장비의 네트워크 이름을 지칭하는 것으로 접속 제어에 대한 초보적인 기능만을 제공한다. 유선 랜과 무선 단말을 연결해 주는 장치 액세스 포인트는 자신이 주기적으로 보내는 비콘(Beacon)신호에 SSID를 포함하여 브로드캐스팅하기 때문에 SSID를 이용하여 네트워크의 접속허용 여부를 묻는 것

은 매우 위험하다[6].

WEP는 데이터 링크 레이어(Data Link Layer)에서 작동하고, 통신을 하고 있는 모든 사람이 동일한 비밀 키를 공유하게 된다. WEP는 가변 길이 키를 지원하는 RC4알고리즘을 사용하지만 복잡한 네트워크에서 약 15~20분 정도면 128bit 정적 WEP 키를 알아 낼 수 있다[3]. 또한 WEP 프로토콜은 크랙(Crack)이 쉽고 무선 데이터 정보 전송 시 정보의 노출될 가능성이 높다고 알려져 있다[7].

2.2 EAP-Method

EAP-Method들은 빈약한 무선 랜 보안 환경을 보완하기 위해 자주 사용하는 인증 프로토콜이다. EAP 자체로는 실제 사용되는 인증 프로토콜을 지정하지 않고, 단지 EAP 인증 프로토콜을 사용하기 위한 인프라만을 제공한다[8].

2.2.1 EAP-MD5(Message Digest) Challenge

EAP-MD5는 가장 초기의 인증 유형이고, EAP Method 중 유일하게 의무사항으로 정의되어 있는 인증 방법으로 아이디(ID)와 패스워드(Password)을 이용한 방식이다. 구현이 단순하지만, 단방향 가입자 인증만을 지원하기 때문에 상호인증이 불가능 하다[9]. 또한 무선 랜 접속 구간보안에 필요한 마스터키 생성방식을 정의 하지 않고 있어 문제가 되고 있다[10]. 그래서 세션 하이재킹(Session Hijacking)이나 MITM(Man In The Middle)에 취약하여 무선 랜에 적합하지 않다.[8,9]

2.2.2 EAP-TLS(Transport Layer Security)

EAP-TLS는 사용자와 인증 서버 사이의 상호 인증과 무선 랜에서의 비밀성 제공을 위해 사용하는 암호화에 필요한 키 분배 메커니즘을 제공하고 있다[11]. EAP-TLS을 이용한 인증서버와 사용자에 대한 인증 방법은 인증 서버와 사용자가 PKI(Public Key Infrastructure) 기반의 인증서를 사용하여 상호 인증을 한다. 안전한 연결성을 보장하기 위해 사용자 기반, 세션 기반의 동적인 WEP키를 생성하여 분배해야한다. TLS의 핸드쉐이크(Handshake) 메커니즘을 이용하여 사용자와 인증 서버 간에 상호 인증을 완료한 후 인증 서버는 인증 성공 메시지와 마스터키를 액세스 포인트에게 전송하고 액세스 포인트와 사용자는 마스터키를 서로 공유하고 이 키를 사용하여 암호 키를 전송한다[4].

문제점은 인증서의 안전한 배포와 사용자와 인증 서버 모두에서 인증서를 관리해야 한다는 점이다. 이는 규모가 큰 WLAN을 설치하는 경우 번거로운 작업이 될 수 있다[12]. 또한 사용자가 인증 서버의 인증서가 정당한 인증서인지를 판단해야 한다. 그러기 위해서는 서버의 인증서가 미리 설치되어 있어야한다는 문제점이 발생한다[6]. 또한 PKI 인프라의 유지보수 작업에는 예상보다 많은 노력과 시간이 필요하고, 모든 사용자에게 PKI을 요구하기에는 현실적으로 어려움이 있다[11].

2.2.3 EAP-TTLS(Tunneled Transport Layer Security)

EAP-TTLS는 EAP-TTL의 확장 형태이다. 열악한 무선 환경에서 무거운 인증서를 보관하고 전송하는 문제를 보완하기 위하여 사용자에 대한 인증은 비밀번호로 하고 서버 인증은 인증서를 이용하여 상호 인증을 하는 방법이다. 사용자 정보는 TLS 프로토콜을 통해서 안전하게 터널링(Tunneling) 함으로써 무선 링크를 포함한 인증서버까지 외부 도청자에 대한 익명성이 보장된다[12]. 또한 TLS을 사용하여 모니터링이 불가능하기 때문에 전송 중인 내용을 제 3자가 해독할 가능성은 거의 없다. 하지만 인증서가 없는 환경에는 적합하지 않고, 사용자가 서버 인증서를 얼마나 정확하게 확인 할 수 있는지에 대한 문제가 발생한다[8]. TTLS는 주로 Funk에서 관리하며 요청자 및 인증 서버 소프트웨어에 대한 대가를 별도로 지불해야하는 또 다른 문제점이 있다[13].

2.3 PPP(Point to Point Protocol) CHAP(Challenge Response Authentication Protocol)[14]

기존에 유선 네트워크에서 사용자와 인증 서버(Authentication Server)간의 인증을 하기위해 사용되었던 PPP CHAP 방식은 3 방향 핸드쉐이크(3Way Handshake)를 사용하여 사용자를 주기적으로 확인하는데 사용하는 인증 방법이다. 이것은 링크(link) 설정 초기에 이루어지고, 링크가 확립된 후에도 서버가 언제든지 사용자를 재 인증 할 수 있다는 장점을 가지고 있다. 링크 설정이 완료된 후 인증 서버는 통신 사용자에게 챌린지 메시지(Challenge Message)를 보내면 사용자는 일-방향 해시 함수를 사용해서 계산되어진 결과 값을 서버에게 리플라이 메시지(Reply Message)로 보낸다. 서버는 자신이 계산한 값과 리플라이 메시지의 값을 비교하여 일치하면 Success Ack 메시지를 보내고 일치하지 않으면 접속을 끊는다. CHAP은 식별자와 랜덤 값의 변경으로 재공격을 대처 할 수 있다. 인증 방법은 인증 서버와 사용자간의 비밀 키를 온/오프라인을 통해 공유하여 사용하기 때문에 비밀 키 값은 네트워크에 공개되지 않는다. 하지만, CHAP는 단일 인증만을 지원하고, 모든 가능한 비밀 키 값을 양단에서 가지고 있어야 하는 단점이 있다.

2.4 MS-CHAPv2(Microsoft CHAP Version2)[15]

MS-CHAPv2은 MS-CHAP version1을 수정 보완하여 이름을 개명한 인증 프로토콜이다. 이 프로토콜을 상호 인증이 가능하고 MS-CHAPv1에서의 문제점을 상당히 개선했다. MS-CHAPv2의 문제는 서버로부터 받은 챌린지 메시지를 직접 사용하지 않기 때문에 도청이 가능하고 매우 복잡한 과정을 요구한다.

지금까지 현재 사용되고 있는 인증 메커니즘과 문제점에 대해 살펴보았다. 많이 사용되고 있는 인증 메커니즘들은 Rouge 액세스 포인트(소프트웨어적이나 물리적인)에 대한 적절한 대응 방법이 없다. 공격자가 Rouge 액세스 포인트(이하 RAP)를 세팅하게 되면 RAP는 진짜(Real) 액세스 포인트와 똑같은 SSID와 채널을 설정하여 사용하게 된다[8]. 이렇게 되면 사용자는 RAP와 진짜 액세스 포인트를 구별할 수 없다. RAP를 사용한 공격을 당할 경우 무선 랜 사용자들은 자신이 공격을 당하고 있는지 알 수 없게 되어 전파가 강한 엉뚱한 액세스 포인트로 접속을 하게 된다. 이럴 경우, ID와 패스워드 MD5 hash 값이 노출되어 크랙(Crack)될 가능성이 생기게 된다[8].

본 논문에서는 현재 사용되고 있는 인증 메커니즘보다 RAP에 보다 효율적인 인증 메커니즘을 제안한다.

3. 제안하는 CHAPv3 인증 메커니즘

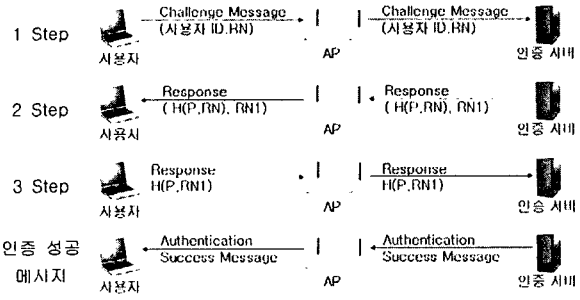
이 장에서는 인증서를 사용하지 않고, 패스워드만을 사용하여 사용자 및 서버에 대한 인증을 수행하는 새로운

CHAP을 제안한다. 비슷한 연구로서, 인증서를 사용하지 않고, 사용자이름과 패스워드를 이용하여 사용자 인증을 하는 방안이 IETF 인터넷 드래프트 문서로 존재한다 [16].

무선 랜에서 액세스 포인트와 서버간의 통신은 기존의 유선 네트워크에서 사용하던 암호화 방식을 그대로 사용한다. 그리고 사용자(Client)와 액세스 포인트 간의 인증은 PPP CHAP방식을 수정하여 더 적은 스텝(Step)으로 상호 인증을 할뿐만 아니라 RAP을 이용한 공격을 방지한다. 먼저 사용자는 자신의 아이디(ID)와 랜덤하게 생성되어진 임의의 숫자 RN(Random Number)을 챌린지 메시지로 사용하여 액세스 포인트에 접속요청을 하게 된다. 요청과 동시에 RN과 자신의 패스워드를 가지고 SHA 암호화 알고리즘을 이용하여 생성된 해시 결과 값 R1(OTP)을 생성한다. 여기서 액세스 포인트는 진짜 액세스 포인트든 RAP이든 상관이 없다. 액세스 포인트는 사용자로부터 받은 아이디와 RN을 사용하여 인증서버에 네트워크 접속을 위한 인증 요청을 하게 된다. 인증서버는 아이디와 일치하는 패스워드와 RN을 이용하여 SHA을 이용하여 생성된 해시 결과 값 R2을 생성한다. 인증서버는 결과 값 R2와 랜덤하게 생성되어진 챌린지 메시지 RN2 값을 액세스 포인트를 거쳐 리스폰스(Response)한다. 사용자는 R1과 R2을 비교하여 일치하면 사용자는 인증 서버를 신뢰할 수 있게 된다. 사용자는 인증 서버로부터 받은 챌린지 메시지 RN2와 자신의 패스워드를 사용하여 다시 해시 결과 값 R3을 생성하여 인증서버에 리스폰스하면 인증 서버는 RN2와 사용자의 아이디와 일치하는 패스워드를 사용하여 해시 결과 값 R4을 생성하고 R3와 R4을 비교하여 일치하면 상호 인증이 이루어지는 방식이다.

기존의 방법들은 4번 이상의 스텝 후 인증 성공 메시지를 사용자에게 리스폰스하지만 본 제안 방법은 3번의 스텝이 이루어진 후에 인증 성공 메시지를 리스폰스 한다. 즉, 스텝수가 적고, PPP CHAP의 장점인 서버(또는 사용자)가 원할 때 수시로 서로를 확인 할 수 있다는 장점이 있다. [그림 2]는 제안 인증 메커니즘의 접속 흐름도이다.

[그림 2] 제안 인증 메커니즘 접속 흐름도



위 과정에서 정당한 액세스 포인트가 아닌 RAP일 경우 사용자의 ID는 공개되어지더라도 패스워드는 공격자에게 공개되지 않는다. 현재 사용되고 있는 많은 인증 방법들은 유선 랜에서 사용하던 방식을 무선 랜으로 옮겨왔기 때문에 서버가 사용자를 인증 한 후 사용자가 서버를 인증하는 방식을 사용한다. 무선 랜에서는 RAP가 존재하기 때문에 이런 방식은 위험 할 수도 있다.

4. 결론 및 향후 과제

현재 사용하고 있는 인증 방법으로는 RAP을 사용자가 식별할 수 없는 문제가 발생한다. 이 문제를 어느 정도 보완하기 위해 본 논문에서는 PPP CHAP을 수정하여 사용자가 서버를 먼저 인증한 다음 서버가 사용자를 인증하는 상호 인증 방식인 CHAPv3을 제안하였다. 기존의 인증 방법들보다 한 스텝이 줄기 때문에 통신비용이 적게 들고, RAP에 의한 사용자의 패스워드 유출이 불가능하다. 또한 간단한 모듈만 추가 하면 되기 때문에 어떤 서버에도 적용이 가능하다.

향후 과제로는 사용자가 RAP인지 또는 진짜 액세스 포인트인지를 구별 하여 정당한 AP와 통신이 이루어지도록 해야 한다.

참 고 문 헌

[1]김기태,"무 선랜 보안을 해결하라",Network Times, Feb, ,2003
[2]권혁범, "보안 문제 해결 없이 무선 인터넷 성장도 없다." Network Times, May, 2003
[3]Sean Convery, Darrin Miller, "SAFE: Wireless LAN Security in Depth-version2", 2002www.cisco.com/go/safe
[4]조재유,"Deploying Secure Mobile Access Infrastructure", , Windows Server 2003 Launch, 2003
http://download.microsoft.com/download/1/8/1/ 181b161-b5fe-4b78-87c0-09c7e49afe7d/14_IT_1_mobile_net.ppt
[5]김상철, "무선랜 보안(Wireless Security)", 2002 www.noikorea.com/data_down/wireless_lan_security.pdf
[6] 송창렬,정병호,조기환,"무선랜 보안구조",정보과학회지, 제 20권, 제4호, pp5-13,2002
[7]W.A.Arbaugh,"Your 802.11 Wireless Network has No Clothes",University of Maryland,http://cs.umd.edu/, Mar, 2001
[8]오정욱, "무선 랜 보안, 한 단계 더 깊이", 마이크로소프트웨어(마소), pp.158-164, Jan, 2004
[9] D.Potter et al., "PPP EAP MS-CHAP-V2 Authentication Protocol", http://www.rfc-editor.org/internet-drafts/draft-draft-dpotter-pppext-eap-mschap-01.txt, Jan, 2002
[10]정병호,강유성,김신효,정교일,"Technology Trends on Authentication and Key Management in Public WLAN Networks", 전자통신동향분석 제 17권, 제 4호, August, 2002
[11]"Serial Authentication using EAP-TLS and EAP-MD5", IEEE draft, Jul, 2001
[12] Secure Authentication, Access Control, And Data Privacy on Wireless Lan,http://www.funk.com/radius/wlan/w-lan_solns.asp, Funk Software
[13] 무선 이더넷 장치 무선 보안 - 802.1x 및 EAP 유형 http://support.intel.com/support/kr/network/wireless/sb/CS-008413.htm
[14]W. Simpson, "PPP Challenge Handshake Authentication Protocol(CHAP)", RFC 1994, August, 1996
[15]Bruce Schneier, Mudge "Cryptanalysis of Micorsoft's PPTP Authentication Extensions(MS-CHAPv2)", Secure networking 0000034249권, 192-203쪽 '99,
[16] D. Taylor, "Using SRP for TLS Authentication", Internet, Draft, 2001, IETF