Journal of Korea Multimedia Society Vol. 11, No. 8, August 2008(pp. 1101-1110)

Nespot 무선랜 사용자 인증 취약점 분석 및 일회용 세션키 기반 무선랜 인증 기법

이 형 우†

요 약

네스팟(Nespot)은 편리한 무선 인터넷 접속 서비스를 제공한다. 초기 접속 과정에서 사용자 아이디 및 패스워드 정보를 입력받아 IEEE 802.1X EAP-MD5 기반 인증 단계를 수행한다. 하지만 네스팟에서 사용되는 EAP-MD5 기반 사용자 인증 단계에서 송수신되는 패킷을 수집하여 분석한 결과 사용자 ID 값이 노출되어 전송되고 있으며, 네스팟 서버와 접속 장치간 상호 인증의 취약성이 발견되었다. 이에 본 연구에서는 네스팟에서 사용하는 IEEE 802.1X EAP-MD5 기반 사용자 인증 시스템의 취약점을 분석하고, 추가적으로 간략화된 일회용 세션키(one-time session key) 공유 방식을 적용하여 상호 인증 및 무선 구간의 암호화 기능을 제공하는 등 기존 네스팟 공중 무선랜 기반 사용자 인증 서비스에서의 취약점을 보완하고 이를 개선할 수 있는 기법을 제시하였다.

Advanced WLAN Authentication Mechanism using One-time Session Key based on the Vulnerability Analysis in Nespot Wireless Lan System

Hyung-Woo Lee†

ABSTRACT

Nespot provides a convenient wireless internet connection service. The existing IEEE 802.1X EAP-MD5 authentication mechanism can be achieved based on ID/password information for a wireless connection. The Nespot system offers an advanced accounting and authorization procedure for providing wireless user authentication mechanism. However, many problems were found on the existing Nespot EAP-MD5 mechanism such as a ID value exposure, a leakage of personal information on wireless authentication procedure and a weakness on Nespot mutual authentication mechanism. Therefore, we analyzed the limitation of the existing IEEE 802.1X EAP-MD5 certification system, and suggested a one-time session key based authentication mechanism. And then we offered a simplified encryption function on the Nespot certification process for providing secure mutual authentication process.

Key words: Nespot(네스팟), Authentication(인증), Vulnerability Analysis(취약점 분석), One-time Session Key(일회용 세션키)

1. 서 론

현재 무선 장비의 보급과 필요성에 의해 무선 네트워크 사용자가 급증하고 있다. 국내에서도 이런 사용자들의 욕구를 만족하기 위해 2002년 1월부터 KT에서는 네스팟(Nespot) 서비스를 시작하였으며 현재 수도권 지역에 800,000개 이상의 AP 보급과 1,200,000명 이상의 무선 네트워크 사용자를 확보하

※ 교신저자(Corresponding Author) : 이형우, 주소 : 경기도 오산시 양산동(447-791), 전화 : 031)379-0642, FAX : 031)379-0642, E-mail : hwlee@hs.ac.kr
접수일 : 2008년 1월 9일, 완료일 : 2008년 6월 2일

† 종신회원, 한신대학교 컴퓨터공학부 부교수
※ 이 논문은 2008년도 한신대학교 교내 연구비 지원에 의해 수행되었음

고 있다. 2006년까지 국내 네스팟 사용자 수는 322만 명 정도로 추산되며 KT는 ADSL 기반의 통합형 단말기(ADSL + AP)를 제공하여 사설 유선 랜(LAN)을 무선 영역으로도 확장하고 있으며 최근에는 CDMA와 무선랜을 결합한 서비스까지도 출시되고 있다[1].

그러나 서비스의 양적인 성장에 주력한 나머지 보안적인 측면은 아직 초기단계 수준에 머물러 있다. 또한 네스팟에 가입한 불특정 다수의 사용자들이 AP를 공유하여 사용하므로 무선 구간의 암호화 적용이 어려운 실정이다[2]. 또한 네스팟 서비스는 이용 요금 과금에 대한 문제를 해결하기 위해 ID/패스워드 기반의 IEEE 802.1X[3] EAP (Extensible Authentication Protocol)-MD5 무선 인증 방식을 사용하였다. 그러나 EAP-MD5 인증 방식은 사용자와 인증 서버와의 상호 인증 절차 부재로 비인증 AP(Rogue AP)를 이용한 공격에 취약하다[4,5]. 비인증 AP를 이용하여 공격자는 사용자와 서버 사이에 전송되는 네스팟 인증 프레임을 수집하여 정보를 획득하고 이를 통해 사용자와 인증 서버간의 데이터를 수집할 수 있다.

하지만 현재 사용되고 있는 네스팟 기반 무선랜 인증 시스템[6]의 문제점으로는 네스팟 인증 과정에서 송수신되는 패킷에서 사용자의 ID 부분과 사용자 패스워드 관련된 개인 신상 정보가 송수신되는 과정에서 일부 노출되며 악의적인 분석이 가능하다는 점이다. 무선랜 인증 과정에서의 사용자 ID 노출 문제는 네스팟 인증 과정뿐 아니라 무선랜 인증 후 송수신되는 프레임에서 ID/패스워드 방식의 인증 과정에도 악용될 소지가 많다. 또한 MD5 해쉬(Hash) 함수를 통해 전송되는 비밀번호 부분 해쉬 정보에 대한 전수공격(Brute-Force attack) 및 사전공격(Dictionary attack)도 가능[7,8]하다는 취약점을 가지고 있으며, 무선 구간에서 전송되는 메시지가 암호화 되지 않은 형태로 전송되어 스니핑 공격(Sniffing attack)[9]에도 취약하기 때문에 이에 대한 개선 방안이 제시되어야 한다.

따라서 본 연구에서는 네스팟 시스템에서 사용하고 있는 기존의 IEEE 802.1X EAP-MD5 기반 인증 시스템의 취약점을 직접 분석하였으며 이를 보완하기 위해 무선 사용자와 인증 서버간 세션키 공유 및 AP와 인증 서버간 일회용 세션키 공유를 통해 상호 인증 기능을 강화하고 무선 구간의 암호화 과정을 수행하여 네스팟 서비스에서 송수신되는 메시지에 대한 보안 가능을 강화하는 방안을 제안하였다. 본 연구에서 제시한 방식은 현재 사용되고 있는 네스팟 서비스의 보안 취약성을 분석하고 이에 대한 해결방안을 제시한 것으로, 안전성 평가 분석 결과 일회용 세션키를 이용하여 네스팟 사용자에 대한 개인 정보 보호 및 메시지 보안 강화 기능을 제공할 수 있는 방식이다.

본 논문의 2장에서는 기존의 EAP-MD5 인증 방식에 대해 고찰한다. 3장에서는 네스팟의 인증 시스템 절차를 설명하고 네스팟 기반 무선 인증기법의 취약점을 분석한다. 4장과 5장에서는 본 연구에서 제시한 기법과 기존 인증 시스템과의 안전성 비교 분석 과정을 수행하고, 6장에서 결론을 제시한다.

2. 무선랜 사용자 인증

2.1 기존의 무선 네트워크 인증 시스템

기존의 무선 네트워크 인증 시스템은 단말들이 개방된 인증 시스템(Open Authentication System) 또는 공유키를 사용한 인증 절차를 수행하여 AP 기반 무선 인터넷 망에 연결된다. 이때 AP와 클라이언트 사이에서는 필요에 따라 아래 그림 1과 같이 WEP (Wired Equivalent Privacy)[2] 암호화 방식 및 WPA (Wi-Fi Protected Access) 기반 무선 프레임 데이터 암호화 방식을 적용하여 클라이언트 시스템과 AP간에 전송되는 IEEE 802.11 프레임을 보호한다.

그러나 기존의 무선랜 인증 절차에서 사용하는 AP용 WEP 키는 해당 단말 시스템에 대한 키일 뿐 단말을 사용하는 사용자에 대한 안전한 인증 및 데이터 암호 기능을 제공하지 못하고 있다[10]. 또한, 네

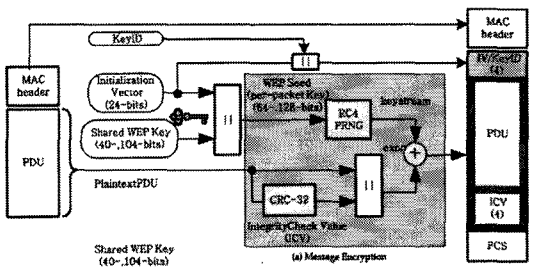

그림 1. WEP 암호화 과정[10]

스팟과 같은 공중 무선랜에서 사용자별 로그인 계정 관리 및 AAA 기반 과금 처리 등의 부가 기능을 지원되지 못한다는 단점이 있다.

물론 IPSec 프로토콜을 이용하여 무선 구간에 대한 보안성을 높일 수도 있다. 하지만 이 경우에도 데이터링크 계층에서의 보안 취약점을 해결하지 못한 것이기 때문에, 기존의 MAC 스푸핑 공격(Spoofing attack), 채널 호핑(Channel Hopping) 및 ARP 변형 공격(ARP Poisoning attack)[9] 등을 통해 손쉽게 공격이 가능하다.

따라서 기존의 유선 PPP망에서 사용되고 있던 사용자 인증용 프로토콜인 EAP를 공중 무선랜에 적용하기 위해 IEEE 802.1X 표준이 개발되었다. IEEE 802.1X[3,6] 표준은 EAP 메시지를 PPP 프레임 대신에 포함시켜 전달할 수 있는 EAP over LAN (EAPoL) 프레임 형식과 절차를 정의하고, 사용자별로 브리지 또는 무선 AP의 물리적인 포트 사용권을 외부의 인증 서버로부터 획득해야만 해당 사용자는 무선 인터넷망에 대한 접근을 허용하도록 포트 접근 제어 프로토콜을 제공한다[11].

네스팟 AP는 공격자에게 손쉽게 노출되어 있다. BSSID를 통해 손쉽게 네스팟 존에 설치된 AP의 위치 및 신호 강도 등을 확인할 수 있다. 따라서 AP에 대한 접근제어 기능이 포함되어 있지 않아서 AP에 대한 DoS 공격 등이 가능하며 이 경우 일반 사용자에 대한 서비스가 중지되는 문제점을 보인다.

2.2 EAP-MD5 인증 방식

노트북, PDA 등의 단말기를 사용하여 네스팟 AP가 설치된 장소(공공장소, 대학교 , 편의점 등)에서 무선랜을 통해 초고속인터넷과 각종 콘텐츠를 이용할 수 있는 서비스를 네스팟 존(Nespot Zone)이라고 한다[1].

현재 네스팟 ID만 있으면 전국 13,000여개 네스팟 존에서 무선인터넷을 손쉽게 접속하여 사용 가능하다. 무선이므로 편리한 점을 제공하며, 케이블 연결 과정이 없으므로 손쉬운 설치가 가능하고, 네트워크 구축비용이 절감되는 효과를 볼 수 있다. 또한 유선으로 설치하기 곤란한 곳에도 설치가 가능하며 이동통신 서비스에 비해 저렴한 서비스를 제공하다. 특히 네스팟 서비스는 보안성이 강화된 인증방식(IEEE 802.1X 표준)을 채택하여 무선구간에서 전송되는 메시지에 대한 안전성을 보장하고자 하였다.

IEEE 802.1X 기반 무선랜 방식은 RADIUS 인증 서버 기반 강화된 보안 기능을 제공하기 위해 제시되었으며 현재 네스팟 등에서 사용하고 있는 기술이다. 네스팟 인증서버는 사용자 식별 정보에 해당하는 사용자 ID 값을 별도의 홈페이지를 통해 부여하고, 이를 통해 AP에 대한 접속 포트를 제어하고 있다. 인증 서버에서 확장 가능한 인증 프로토콜(Extensible Authentication Protocol : EAP)을 통해 MAC 계층에 대한 접근 제어 기능을 제공한다.

네스팟 존에서는 무선 사용자에 대한 네스팟 AP 기반 인증 방식으로 EAP-MD5를 사용하고 있다. 하지만 네스팟에서 사용하는 EAP-MD5 방식은 일회용 세션 키 방법 등을 이용한 암호화 기능을 제공하지 않기 때문에 EAP-TLS, EAP-TTLS 등에 비해 보안이 취약할 수밖에 없다. 기업 내 무선 인트라넷 환경 구축시 AP 설정을 EAP-TTLS 방식으로 하고자 해도 윈도우즈 비스타용 네스팟 지원 툴에서 지원하지 않기 때문에 인증 과정에 취약점을 보이고 있다[10].

그림 2는 현재 네스팟에서 사용하고 있는 EAP-MD5 인증 구조를 보인다. RADIUS 서버에 네스팟 사용자 가입 과정을 수행한 후 관련 정보 등이 기록되어 있으며 과금 및 사용 기간에 대한 정보 등을 저장하고 있다. 이제 사용자는 네스팟 존에서 무선 NIC를 이용하여 네스팟 AP에 접속을 시도하게 된다. 기존의 네스팟에서 사용하는 EAP-MD5 기반 인증 방식은 그림 3과 같다.

3. 네스팟 무선랜 인증 시스템 취약점 분석

네스팟 서비스에 대한 취약성을 분석하기 위해 본 연구에서는 다음과 같은 실험 환경을 구축하였다. 공중 무선랜 환경에서 네스팟 서비스를 지원하는 AP를 확인하고 이를 중심으로 무선랜 트래픽 분석 모듈

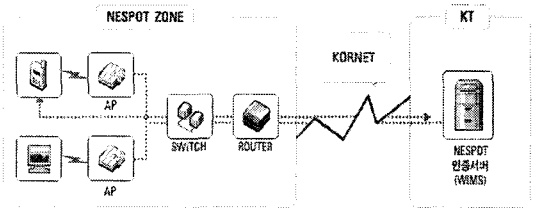

그림 2. 네스팟 존 및 기존의 서비스 구성도

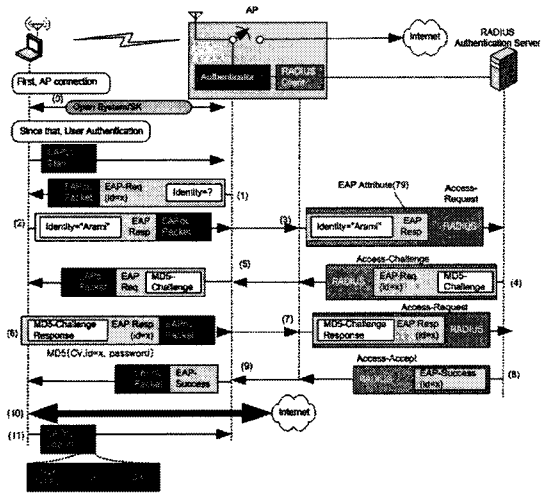

그림 3. EAP-MD5 방식[10]

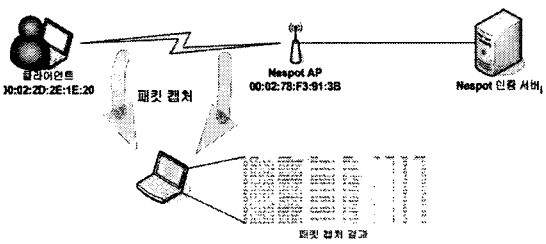

그림 4. 네스팟 패킷 캡처 실험 환경

을 통해 네스팟 AP와 무선 단말 간에 전송되는 인증 패킷 등에 대해 캡처하여 분석 과정을 실시하였다. 그리고 무선 패킷의 캡처는 Airopeek을 이용하여 네스팟 무선랜 인증 과정에서 송수신되는 패킷에 대해 분석하였다.

3.1 네스팟 인증 절차 및 분석

앞에서 제시한 네스팟 인증 과정을 본 연구의 패킷 분석 실험과정에서 조금 더 자세히 분석하면 다음 그림 5와 같다. 네스팟의 인증 시스템은 개인 인증과 과금 정책의 적용을 위해 패스워드 기반의 개인 인증 방식인 EAP-MD5 인증 방식을 사용하고 있다. 따라서 사용자 ID 값을 설정하고 네스팟 인증 과정을 수행하면서 캡처된 내용을 단계적으로 제시하면 아래와 같다.

사용자 클라이언트(User Client)는 개방형 인증(Open Authentication) 또는 공유키(Shared Key) 방식으로 인증절차를 수행하여 AP와 연결한다. 이 과

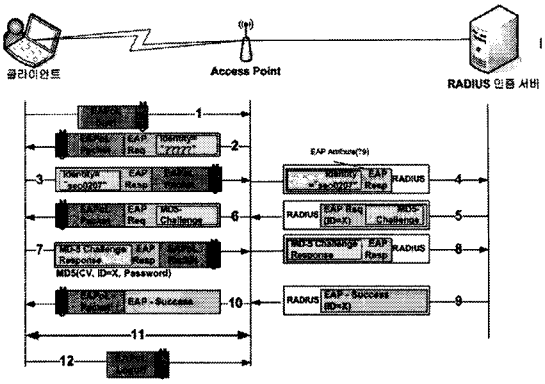

그림 5. 무선 네스팟 인증 과정

정은 이더넷 단말이 스위치에 케이블로 연결한 것에 불과하다. 이후 EAP 절차에 의해 사용자 수준의 인증 절차를 수행한다. 1단계로 단말로부터 EAPoL Start 메시지를 수신하거나, 단말이 접속된 사실을 감지하면 사용자 이름을 전송하라는 EAP-Request [Identity] 메시지를 EAPoL 패킷에 포함하여 단말에게 요청한다. 이 경우의 식별자(identity) 항목에는 사용자 이름은 없는 대신에 AP의 정보인 SSID, AP의 이름 등이 포함되어 2단계 과정에서 클라이언트 단말로 전송된다.

다음 3단계에서는 클라이언트 단말은 사용자 이름이 포함된 EAP-Response[Identity] 메시지를 생성하여 AP에 전송한다. 단말로부터 수신한 EAP-Response [Identity] 메시지를 RADIUS 서버로 전송되는 EAP 필드 내에 Access-Request 메시지 형태로 생성하여 4단계 과정과 같이 전송하며, RADIUS 서버는 MD5-Challenge Value(CV)가 포함된 EAP Request 메시지를 구성한 후, 이것을 다시 5단계 과정에서 RADIUS Access-Challenge 메시지의 EAP 속성에 포함하여 AP에 송신한다. AP는 6단계 과정에서 RADIUS 메시지의 EAP 필드에 기록된 속성 정보를 꺼낸 후 , EAPoL 패킷에 다시 생성하여 클라이언트 단말에 전달한다.

클라이언트 단말은 {자신의 패스워드, CV, 자신의 사용자 이름}을 MD5 알고리즘을 이용하여 해쉬 값이 포함된 EAP-Response [MD5-Challenge Response] 메시지를 다시 AP에 전달하는 7단계 과정을 수행하며, 단말로부터 전달받은 EAP-Response [MD5-Challenge Response] 메시지를 8단계 과정에서 AP는 RADIUS 인증서버에게 전송한다.

9단계 과정에서 RADIUS 서버는 정당한 사용자 인증 과정을 수행한 후 EAP Success 메시지를 구성하여 이를 RADIUS Access-Accept 메시지의 EAP 속성에 포함하여 다시 AP에 송신한다. AP는 10단계 과정을 통해 EAP Success 메시지를 클라이언트 단말에 전송하면서 사용자를 인증하고, 해당 단말이 인터넷에 접근할 수 있도록 허용한다. 최종 11단계 및 12단계를 통해 클라이언트 단말은 EAP Success 메시지를 수신하면 이제 AP를 경유하여 외부 인터넷에 접근할 수 있게 되며, 사용자는 로그-오프시 EAPoL Logoff 메시지를 AP에 송신한다.

여기서 알 수 있듯이, EAP-MD5는 EAP 방식을 준용하는 CHAP 인증 방식이다. 그림 7은 실제 인증 과정에서 전송 되었던 무선 구간의 패킷을 캡처한 결과를 보인다. 그리고 그림 7의 오른쪽 숫자는 그림 6의 네스팟 인증 단계 번호에 해당하는 것을 표기한 것이다.

3.2 네스팟 인증 시스템의 취약점

3.1에서 살펴본 바와 같이 네스팟 인증 시스템은 IEEE 802.1X의 EAP-MD5 인증 알고리즘을 사용하고 있다. 그러나 EAP-MD5 인증 알고리즘은 다음과 같이 크게 세 가지 형태의 인증 취약점을 보이고 있다.

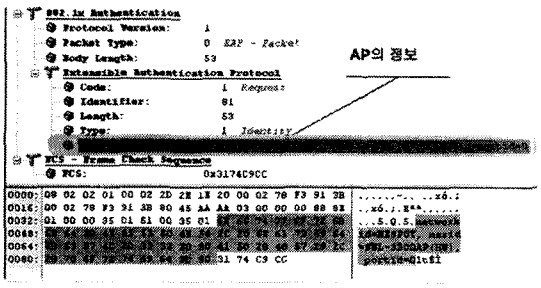

그림 6. EAP-Request 패킷 분석

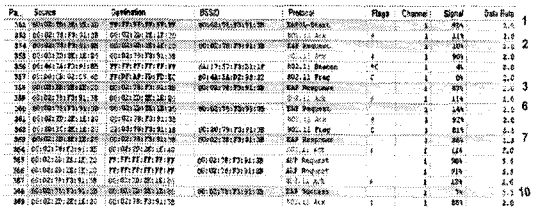

그림 7. 네스팟 인증 패킷 리스트

첫째로 사용자의 ID가 노출된다. EAP-MD5 인증 과정에서 송수신되는 패킷을 캡처해 보면 네스팟 서비스 가입자가 아니더라도 손쉽게 일반 사용자의 ID 정보를 획득할 수 있다.

두 번째로는 MD5 해쉬 함수가 메시지 인증에 사용될 경우 취약점[7,8]이 존재하기 때문에, 응답 메시지에 대한 전수 공격에 취약하다. 초기의 EAP-Request/Identity 메시지에 대한 응답인 EAP-Response/Identity 메시지는 사용자의 ID 값을 포함하고 있다. 따라서 공격자는 무선 구간의 패킷 수집을 통해 사용자의 ID와 서버의 도전(Challenge)값과 패스워드 값 등 인증에 필요한 정보를 포함하여 생성된 클라이언트의 응답(Response)값을 얻을 수 있다. 결국 공격자는 EAP ID | PW | Challenge 값에 대한 MD5 해쉬 값을 획득할 수 있다. 물론 일반적으로 MD5 해쉬 함수는 단방향 함수(One-way Function)로 충돌 회피 기능을 제공하는 다이제스트 함수이다. 따라서 공격자는 일반적으로 해쉬 값으로부터 PW 값을 추출할 수 없다. 하지만 MD5 알고리즘에 대한 전수 공격을 시도할 경우 8자리에 해당하는 PW 정보인 경우 현재의 시스템을 이용할 경우 수일 이내에서 복호화가 가능하기 때문에 이에 대한 보안 강화 등이 요구된다.

셋째로는 네스팟 인증 과정 이후에 전송되는 메시지에 대한 암호화 과정이 없어서 메시지에 대한 보안 취약성을 보이고 있다.

또한 기존 네스팟인 경우 인증 과정에 해당하는 헤더 정보 등을 삭제하는 등 인증 과정을 하지 않고서도 통신이 되는 등의 문제가 발생한다. 따라서 기존의 네스팟 시스템에 대한 공격이 가능하여 무선랜 사용 환경의 취약점에 대한 개선이 시급한 시점이다.

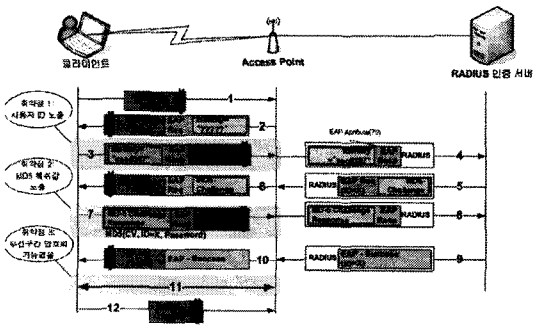

그림 8. 네스팟 인증 절차 및 취약점

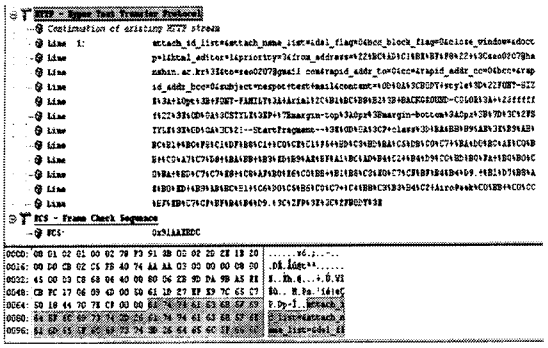

그림 9. 무선 구간의 Sniffing 결과 분석

패스워드 기반의 EAP-MD5 인증 방식은 사용자와 인증 서버 간에 상호 인증 기능이 없어 사용자는 서버를 무조건 믿어 Rouge AP에 의심 없이 접속할 수 있는 문제가 있다.

무선 구간의 메시지 비암호화로 패킷 스니핑(Packet Sniffing)을 통한 메시지 내용의 유출 문제가 심각하다. 그림 5에서 (11) 단계의 패킷 분석 결과 사용자의 메일 내용까지 확인 할 수 있다. 그림 9는 사용자의 메일 내용을 수집한 결과이다.

아래 그림 10은 앞에서 제시한 그림 5의 (3)단계에서 ID 값이 노출된 형태로 전달된다는 문제점을 보인다. Airopeek을 이용하여 네스팟 인증 과정에서 전달되는 패킷을 분석한 경우 사용자 ID 정보가 노출되어 공격자에 의해 악용될 수 있다.

아래 그림 11은 그림 5의 (7)단계에서 EAP-MD5 결과 값을 보인다. 이때 응답 결과 값에 포함된 CV, ID, PW의 연접한 뒤 MD5 알고리즘을 적요한 해쉬 값이 전달되며 앞에서 제시한 바와 같이 미리 노출된 ID 정보 노출로부터 MD5 해쉬 함수 결과에 대한 전수 공격 및 사전 공격이 가능하다는 취약점을 보인다.

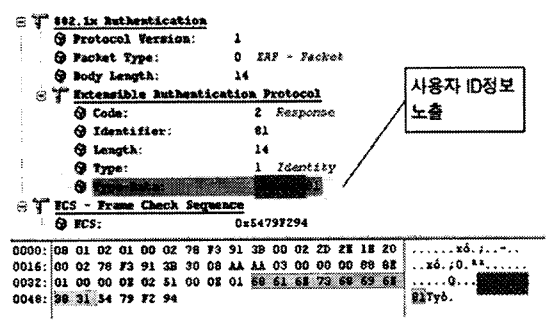

그림 10. 사용자 ID 정보의 노출

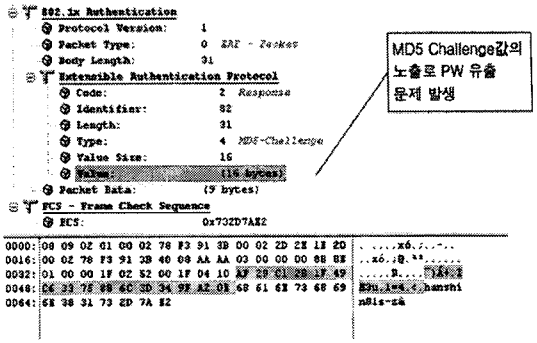

그림 11. MD5 도전/응답 메시지 노출

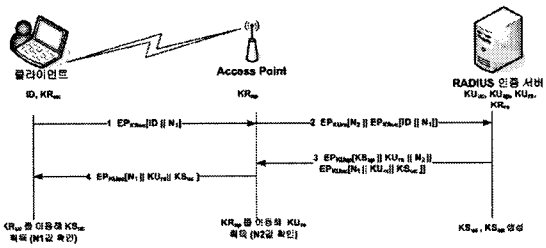

그림 12. 일회용 세션키 분배 과정

4. 네스팟 인증 취약점에 대한 해결 방안

3장에서의 무선랜 취약점의 해결 방안으로 공중 무선랜 인증 시스템을 구성하는 과정에서 RADIUS 인증 서버와 클라이언트 간의 세션키 공유를 통해 상호 인증 및 메시지 암호화 기법을 제공하고, 그 결과 인증 과정에서의 취약점을 보완 할 수 있다.

제안한 기법을 사용할 경우 RSN 인증 및 암호화 전송과정을 통한 EAP 기반 상호인증 절차, 키 관리 및 분배 절차를 이용해 기존 공중 무선랜 인증 시스템에서의 보안 취약점을 해결할 수 있다.

4.1 네스팟 일회용 키 분배 방식

본 논문이 제안하는 기법의 키 분배 방식은 RSA 등과 같은 일반적인 공개키 알고리즘을 이용해 세션키를 안전하게 분배하고 인증서버의 공개키를 사용자 및 AP에 전달하는 것이 그 목적이다. 이를 이용하여 네스팟 인증 과정의 안전성을 높일 수 있다.

위 그림 12는 본 연구에서의 키 분배 과정을 나타내며 사용된 수식 및 기호는 아래와 같다.

KSx={uc, ap, rs} : 관용암호에서 사용하는 세션키

KRx={uc, ap, rs} : 공개키 암호 방식에서 사용되

는 사용자 x의 개인키

KUx={uc, ap, rs} : 공개키 암호 방식에서 사용되는 사용자 x의 공개키

EP : 공개키 암호방식을 이용한 암호화

DP : 공개키 암호방식을 이용한 복호화

EC : 관용암호방식을 이용한 암호화

DC : 관용암호방식을 이용한 복호화

H : 해쉬 함수

‖ : 연접

Z : ZIP 알고리즘을 이용한 압축

N : nonce 값(난수 값으로 재전송 공격(Replay attack)을 방지하기 위해 사용함)

사용자는 자신의 ID와 N1값을 생성하여 자신의 공개키로 암호화 하여 AP에게 전송(EPKRuc[ID ‖ N1])한다. AP에서는 사용자에서 전송 받은 EPKRuc[ID ‖ N1]과 자신이 생성한 N2를 연접하여 자신의 공개키로 암호화(EPKUrs([N2 ‖ EPKRuc[ID ‖ N1]]))하여 인증 서버에 전송한다.

RADIUS 서버는 KSuc 와 KSap를 생성하여 KSuc은 사용자와의 암호화 과정에 이용하고 KSap은 AP와의 유선 구간에서의 암호화 과정에 이용된다.

EPKUap[KSap||KUrs||N2||EPKUuc[N1||KUrs||KSuc]]. EPKUuc[N1||KUrs||KSuc]

사용자와 인증 서버와의 암호화를 수행하기 위해 인증 서버의 공개키와 세션키를 사용자의 공개키로 암호화 전송한다. 위 키 분배 과정은 인증 서버의 공개키 분배와 각각의 세션키 분배를 목적으로 한다.

4.2 세션키 기반 개선된 인증 방안

네스팟 인증 시스템의 취약점은 상호 인증 부재와 메시지 비암호화로 인한 스니핑 공격, 사전 공격 등 다양한 공격들이 존재한다. 이러한 취약점들을 보완하기 위해 본 연구에서는 아래 그림 13과 같이 앞에서 제시한 일회용 세션키를 이용하여 개선된 네스팟 무선랜 인증 기법을 구축할 수 있었다.

· 1단계 : EAP-Start 과정에서 사용자는 자신의 인증 절차 시작을 네스팟 AP에 알린다.

· 2단계 : 네스팟 AP는 사용자의 ID 정보를 사용자에게 요청한다.

· 3단계 : 이때 기존의 EAP-MD5 인증 방식에서는 ID 정보를 비 암호화해서 인증서버에 전달했다.

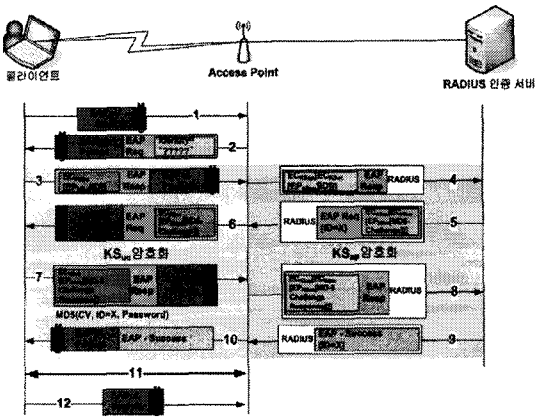

그림 13. 일회용 세션키 기반 공중 무선랜 인증 방법

그러나 사용자 ID 정보의 노출로 인해 사전공격 가능성이 높아졌다. 따라서 본 연구에서는 일회용 세션키 키분배 과정을 적용하였다. 네스팟 인증 서버로부터 전달 받은 KSuc를 이용하여 자신의 ID 정보를 암호화한다. 물론 이때 생성하는 일회용 세션키는 기존의 OTP 기법을 적용할 수도 있고, 네스팟 인증 서버 내에 소프트웨어 형태로 구현가능한 부분이다. 일회용 대칭키 KSuc를 이용하므로 인증 서버에서만 해당 ID 정보를 확인할 수 있다. 또한 공개키 기반 암호화 방식을 이용하여 사용자 자신의 개인키로 암호화(EPKRuc[ID])한 후 분배된 대칭키를 이용하여 다시 암호화 ECKSuc 과정을 수행한다.

· 4단계 : 사용자의 공개키로 암호화된 사용자 정보를 세션키 KSuc를 이용해 암호화했다. 이 효과는 무선 구간에서 있을 수 있는 공격에 대비하기 위해 인증 서버와 사용자간의 암호화이다. 그러나 AP와 인증서버(유선 구간)에 대한 암호화도 필요하다. 그래서 본 논문에서는 KSap를 이용해 유선 구간의 암호화과정을 수행하고 있다. (3)에서 전송 받은 ECKSuc[EPKRuc[ID]]을 AP와 RADIUS 서버와의 세션키로 암호화하여 전송한다.

· 5단계 : 인증 서버는 자신의 개인키를 이용해 MD5-Challenge 문에 서명을 하여 암호화한다. 서명된 MD5-Challenge문은 다시 세션키로 각각 암호화된다. RADIUS 서버는 MD5-Challenge를 위해 자신의 개인키를 이용해 챌린지 문을 암호화함 그리고 각각 사용자와 AP간의 세션키로 암호화한다.

· 6단계 : AP는 KSap를 이용해 인증서버와의 암호화된 메시지를 복호화 한다. 그리고 사용자에게 전

달할 Challenge 메시지를 전달한다.

· 7단계 : 사용자는 자신의 ID, Challenge Value, password를 MD5 해쉬하여 인증 서버에게 전달한다. 이때 이 MD5값의 노출되는 점이 기존의 인증 시스템에서 취약점으로 지적 되었다. 그러므로 본 논문에서는 MD5 해쉬 결과를 사용자의 개인키로 서명하고 그 결과를 인증 서버와의 세션키로 암호화했다.

· 8단계 : 사용자에게 전달된 메시지는 AP에 의해 암호화된다. 인증서버에서는 사용자에 의해 받은 H'(해쉬 결과)를 이용해 인증 DB에 있는 사용자 정보를 참조해 해쉬 결과(H)를 만들어 그 결과의 일치 여부에 따라 인증을 수행 한다. H'=H 경우는 정상적인 사용자로 인식하게 된다.

· 9단계 : RADIUS AP에서 사용자의 인증 성공 메시지를 전송한다.

· 10단계 : AP는 EAPoL 프로토콜에 의해 RADIUS로부터 전송 받은 인증 성공 메시지를 사용자에게 전송한다.

· 11단계 : 사용자는 AP를 통해 통신을 한다.

· 12단계 : 사용자는 AP에게 접속 해지를 요청하고 접속이 종료된다.

5. 안전성 분석 및 평가

기존 네스팟의 인증 시스템은 단순한 해쉬 함수에 의한 단 방향 사용자 인증 시스템을 사용했다. 그러나 이런 인증 시스템은 사용자 정보의 노출 및 상호 인증 부재로 많은 취약점들을 가지고 있었다. 그러므로 본 논문에서 제안하는 인증 기법은 사용자, AP 및 인증 서버간의 상호 인증과 세션키를 이용한 암호화 기법을 사용해 기존의 네스팟 인증 시스템 보다 안전한 인증 과정을 제공하고 있다.

본 연구에서 제시한 기법을 이용하였을 경우 아래 그림과 같이 인증된 네스팟 AP를 통해 송수신되는 패킷에 대해 시간 축으로 분석하였다. 제시한 기법을 적용하여 네스팟 인증을 수행할 경우 인증과정에서 평균적으로 3.5ms의 전송지연이 발생하였다. 하지만 세션키를 이용하여 암호화 과정을 적용하여 전달되므로, 기존의 IEEE 802.1x EAP-MD5 기법에서의 공격 취약점을 보완할 수 있으며, 패킷 스니핑으로 인해 사전공격을 수행할 경우 기존의 기법보다 안전성을 높일 수 있다.

표 1은 기존의 인증 시스템과 제안한 인증 기법에 대한 비교 평가를 보여주고 있다. EAP-MD5 인증과 더불어 인증서를 사용하는 인증 기법과 함께 제안 기법의 성능을 비교하였다.

현재 네스팟은 ID/PW 기반의 인증 시스템을 사용하고 있다. 그러므로 인증서를 이용한 인증 기법의 도입은 많은 부분에서 사용자의 혼란을 불러올 수 있다. 물론 인증 서버에서만 인증서를 필요로 하는 EAP-TTLS 기법을 네스팟에서 지원해 주고 있지만 일반 무선 사용자들에게는 인증 과정이 복잡하고, 인증 방법의 홍보가 제대로 이루어 지지 않고 있는 실정이다.

우선 기존 기법과 제안한 기법의 성능을 비교하기 위해 크게 인증 방식, 상호 인증 기능 여부 및 인증서 사용 기능 등을 중심으로 분석하였다. 그리고 취약점에 대해 분석하여 제시한 기법의 안전성을 분석하였다.

기존의 EAP-MD5 인증 방식에서는 ID 정보를 비

표 1. 기존 인증방식과 제안한 기법의 성능 비교

항목 \ 기법	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	제안기법
인증 방식	MD5 Hash	Public Key	CHAP, PAP, MS-CHAPv2	Any EAP, EAP-MS-CHAPv2, Public Key	Session Key
상호 인증	X	O	O	O	O
인증서 필요	X	O	O	O	X
세션키 이용	X	O	X	X	O
ID 노출 방지	X	X	O	O	O
PW 노출 방지	X	O	O	O	O
취약점	Brute-Force Attack	Identity exposed	MitM attack	MitM attack	-

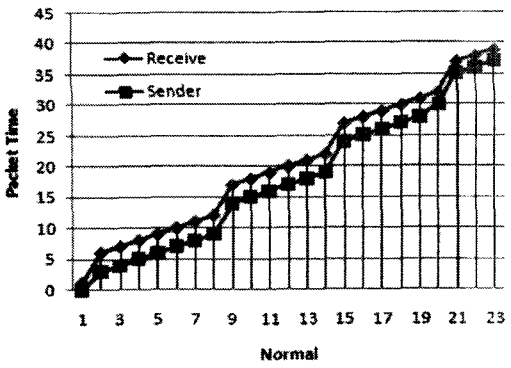

그림 14. 인증된 네스팟 AP에 의해 송수신되는 패킷

암호화해서 인증 서버에 전달했다. 그러나 사용자 ID 정보의 노출로 인해 사전공격 가능성이 높아졌다. 따라서 본 연구에서는 일회용 세션키 키분배 과정을 제시하였으며 네스팟 인증 서버로부터 전달 받은 KSuc를 이용하여 자신의 ID 정보를 암호화하였기 때문에 ID 정보에 대한 노출을 방지할 수 있었다. 일회용 대칭키 KSuc를 이용하므로 인증 서버에서만 해당 ID 정보(ECKSuc[EPKRuc[ID]])를 확인할 수 있도록 하였으며, 공개키 기반 암호화 방식을 이용하여 사용자 자신의 개인키로 암호화(EPKRuc[ID])한 후 분배된 대칭키를 이용하여 다시 암호화 ECKSuc 과정을 수행하였기 때문에 패킷내 정보에 대한 보안성을 높일 수 있었다.

또한 사용자의 공개키로 암호화된 사용자 정보를 세션키 KSuc를 이용해 암호화하였기 때문에 무선 구간에서 전송되는 정보에 대한 보안 기능을 강화하였다. 그리고 KSap를 이용해 AP와 RADIUS 서버간 암호화과정을 수행하도록 하였다. 마지막으로 MD5 값이 노출되는 취약점을 보완하기 위해 MD5 해쉬 결과를 사용자의 개인키로 서명하고 그 결과를 인증서버와의 세션키로 암호화하였기 때문에 안전성을 높일 수 있었다.

결국 본 논문에서 제안한 기법은 기존의 보편화되어있는 ID/PW기반의 인증 시스템에 안정성을 높이기 위한 방법으로 세션키를 사용하였고, 그 결과 사용자와 AP 각각 인증서버와의 세션키를 공유해 암호화 함으로써 세션가로채기 공격(Session hijacking)이나 패킷 스니핑 공격[9]에 안전하다. 또한 제안한 기법인 경우 사용자의 ID 노출 위협이 없어졌으며, 무선 구간에 대한 암호화 과정을 적용하여 공중 무선망 데이터에 대한 안전성을 높일 수 있다.

6. 결 론

본 연구에서는 네스팟에서 사용되는 IEEE 802.1X EAP-MD5 기반 사용자 인증 단계에 대해 절차적으로 분석하였고 네스팟 서비스 이용과정에서 송수신되는 패킷을 직접 스니핑하여 분석하는 과정을 수행하였다. 분석 결과 일반 사용자 ID 값이 노출되어 전송되고 있으며, 네스팟 서버와 접속 장치간 상호인증 과정의 취약성을 발견하였다. 따라서 본 연구에서는 현재 널리 사용되고 있는 IEEE 802.1X EAP-MD5 기반 네스팟 사용자 인증 시스템의 취약점을 강화하기 위해 추가적으로 간략화된 일회용 세션키 공유 방식을 적용하여 상호인증 및 무선 구간의 암호화 기능을 제공하는 기법을 제시하였다. 제시한 기법은 상호인증 기능을 제공하며 기본 네스팟의 인증 취약점을 개선할 수 있을 것으로 기대되며, 앞으로 더욱 더 개선된 무선 사용자 인증 및 암호화 전송과정을 통한 보안 서비스 방안에 대한 연구가 필요하다.

참 고 문 헌

[1] KT 연구보고서, "The World's Largest Wireless LAN Hotspot Controls Access with RAD-Series Radius," KT, 2006.

[2] P. Dasgupta and T. Boyd, "Security in Wireless Network," Taylor & Francis, pp. 513-515, 2005.

[3] C. Hüseyin, "IEEE 802.1X, RADIUS and Dynamic VLAN Assignment," 2005. (http://inet-tr.org.tr/inetconf11/bildiri/107.pdf)

[4] M. Siyal and F. Ahmed, "Security Services and Issues in WLANs," Taylor & Francis, 2005.

[5] 임보혁, "IEEE 802.1x를 이용한 보안성 강화 및 공격 유형별 분석," 슈마 IT News, 2004. (http://blog.naver.com/airbag1?Redirect=Log&logNo=80000771366)

[6] ANSI/IEEE Std 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," ANSI/IEEE Std,

2003.
[7] X. Wang, D. Feng, X. Lai, H. Yu, "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD," Aug. 17, 2004. (http://support.reasonablesw.com/forums/94/ShowPost.aspx)
[8] P. Sridharan, "A Survey of the Attack on MD5," 2006. (https://drum.umd.edu/dspace/bitstream/1903/3689/1/umi-umd-3405.pdf)
[9] D. Welch, S. Lathrop, "Wireless Security Threat Taxonomy," Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society, pp. 76-83, 2003.
[10] 윤종호, 무선 랜 보안 프로토콜, 교학사, 2005.
[11] IEEE Std 802.11i - 2004 Part 11, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) SpecificationsAmendment 6: Medium Access Control (MAC) Security Enhancements -Description," IEEE Std, Retrieved on 2007. (http://standards.ieee.org/reading/ieee/std_public/description/lanman/802.11i-2004_desc.html)

이 형 우

1994년 고려대학교 전산과학과 1994년 졸업(학사)
1996년 고려대학교 대학원 전산 과학과 졸업(석사)
1999년 고려대학교 대학원 전산 과학과 졸업(박사)
1999년~2003년 2월 천안대학교 정보통신학부 조교수
2003년~현재 한신대학교 컴퓨터공학부 부교수
관심분야 : 정보보호, 네트워크 보안, 해킹/바이러스, 스테가노그래피, 컴퓨터 포렌식스