무선랜 환경을 위한 패스워드 기반의 안전한 인증 프로토콜 연구

*김태섭, *오룡, **이형우, *조충호

고려대학교 *컴퓨터정보학과, **전자및정보공학부

*ree31206@korea.ac.kr, *orionpia@korea.ac.kr, **hwlee@korea.ac.kr, *chcho@korea.ac.kr

A study of Security Authentication Protocol based on the Password for Wireless LAN Environment

*Tae-Sup Kim, *Ryong Oh, **Hyong-Woo Lee, *Choong-Ho Cho

*Department of Computer and Information Science, Korea University

**Department of Electronics and Information Engineering, Korea University

요 약

최근에 공공장소에서의 보다 안정적이고 고속의 무선 인터넷 접속에 대한 욕구가 커지면서 무선랜에 대한 수요가 많아지고 있고, 유무선 사업자들은 무선랜 시장을 선점하기 위해서 서비스를 서두르고 있다. 무선랜의 보안문제는 크게 두 가지 측면에서 지적할 수 있는데, 첫 번째는 승인된 사용자에게만 접속을 허용하는 접속에 관한 보안이며, 다른 하나는 스니퍼 등을 이용해 무선랜을 통해 전송되는 내용 자체를 몰래 보는 도청 행위를 방어할 수 있는 보안이다. 특히 유선 네트워크와 달리 무선랜에서는 Access Point 만 설치되어 있는 곳이면 누구나 쉽게 Access Point 를 통해 네트워크를 이용할 수 있다. 이에 따라 무선랜에서 보다 중요성이 강조되는 보안문제는 접속에 관한 보안, 즉 사용자 인증이라 할 수 있다. 이와 같은 무선랜 환경에서 안전하게 사용자를 인증하고 서비스를 제공하기 위한 패스워드 기반의 사용자 인증 프로토콜을 제안한다.

1. 서론

인터넷 및 이동통신 기술의 발전과 함께 사무실 내에서 뿐만 아니라 자동차나 거리, 공항이나 지하철 역 등 다양한 환경에서 인터넷에 접속이 가능해지고 있다. 이러한 환경 구축은 PDA(Personal Digital Assistant) 나 휴대전화 등에서 인터넷 접속이 가능하게 되면서 실현되고 있는데, 이러한 가운데, 최근에는 우리에게 익숙한 이더넷 (Ethernet) 랜 기술을 사용하는 무선랜 (WLAN:Wireless Local Area Network) 서비스가 주목을 받고 있다.

무선랜은 무선랜 카드를 노트북이나 PDA 등에 장착하고 인터넷과의 접점이 되는 AP(Access Point)를 이용해 인터넷을 이용할 경우에 비해 속도가 빠르고, 장비의 비용이 10 배정도 저렴하기 때문에 무선인터넷 시장에서 경쟁력을 갖추고 있다고 보여지며, 향후 더 많은 이용이 예상되고 있다.

현재 무선랜 기술에서 주요 쟁점은 전송속도와 보안에 있다. 특히 보안 문제는 무선랜 기술의 보급과 사용에 커다란 장애 요소이다[1].

무선랜은 특성상 해킹과 침투에 취약한 약점을 안고 있다. 무선랜의 기지국 역할을 하는 AP 는 유선 네트워크와 무선 네트워크를 매개해주는 역할을 하게 된다. 이 AP 를 통한 접속은 비록 사용자가 네트워크의 외부에서 접속하는 것 같아 보이지만 실제로는 내부 네트워크(LAN:Local Area Network)안에서만 접근이 이루어 진다. 따라서 외부망(WAN:Wide Area Network)과 내부망(LAN)사이의 보안 문제를 해결하는 기존 유선망의 보안 기술인 침입탐지시스템이나 방화벽등으로는 무선랜의 보안 취약점을 해결하기 어렵다[2].

무선랜의 보안문제는 크게 두 가지 측면에서 지적할 수 있는데, 첫 번째는 승인된 사용자에게만 접속을 허용하는 접속에 관한 보안이며, 다른 하나는 스니퍼 등을 이용해 무선랜을 통해 전송되는 내용 자체를 몰래 보는 도청 행위를 방어할 수 있는 보안이다. 특히 유선 네트워크와 달리 무선랜에서는 AP(Access Point)만 설치되어 있는 곳이면 누구나 쉽게 AP 를 통해 네트워크를 이용할 수 있다. 이에 따라 무선랜에서 보다 중요성이 강조되는 보안문제는 접속에 관한 보안, 즉 사용자 인증이라 할 수 있다.

본 논문에서는 시간함수에 의해 생성되는 값(Nonce), 대칭키(Symetric key), 공개키(public key), 전자서명(Electronic Signature), 검증자(Authenticator)를 이용하여 보다 유연하고 안전한 인증을 위한 프로토콜을 설계한다.

2 장에서는 현재 사용되는 무선랜 인증 프로토콜에 대하여 살펴보며, 3 장에서는 인증 프로토콜들이 일반적으로 직면하고 있는 공격으로부터 안전하기 위하여 어떠한 요구사항들이 필요한지 알아보며, 4 장에서는 무선랜 환경에서 사용할 수 있는 패스워드 기반의 프로토콜을 제안하고, 5 장에서는 제안한 프로토콜의 보안에 대하여 평가하며, 6 장에서 결론을 맺는다.

2. 관련연구

2.1 EAP(Extensible Authentication Protocol)

IETF EAP WG 에서 표준화를 진행하고 있는 EAP 프로토콜