무선 네트워크 기반에서 PKI 방식을 이용한 상호인증 프로토콜 설계

박재성* · 한승조[1*]

*조선대학교 정보통신공학과

Design of a Realtime Interactive Authentication Method using PKI in the Wireless Network

Jea-seong Park* · Seung-jo Han[1*]

*Dept. of Information and Communication Engineering, Chosun University

[1*]Corresponding author (Email: sjbhan@chosun.ac.kr)

요 약

랜 위의 앞의 증명 방법에서 많은 드러나 있는 문제점이 있었다. 특히 열려 있는 시스템 증명 방법,함께 나눠 진 주요 방법 ,Mac Based 증명 방법은 매우 보안이 필요하는 무선 네트워크에 사용하기 어렵다. 그렇게 지금 많은 연구를 행하여 802.1x와 적용되고 있는 PKI 사용자 증명 방법이었다 . 그러나 EAP은 PKI를 처음 사용하여 CRL이라고 불리는 사용된 없어 진 인증서가 문제 분배 포인트에 대해 가지고 있이 있었다. 이것을 향상시키기 위해 이 논문에서 일어나는 문제 바로 CRL와 OSCP 서버를 사용하지 않기 위해 CA을 사용할 CVS을 적용했다.

ABSTRACT

There were many exposed problems in previous authentication method on LAN. Especially Open System Authentication Method, Shared Key Method, Mac Based Authentication Method are very hard to use in wireless network that needs security. So now, many researches have been performed about 802.1x and user authentication method applying PKI. But certificate verification protocol has been used abolished list called CRL since it's first usage of PKI, there were still has a problem about distribution point. In this paper, I applied CVS to use CA direct not to use CRL and OSCP server in order to improve this problems.

키워드

EAP-TLS, PKI, 실시간 인증시스템

Ⅰ. 서 론

무선 LAN은 전파라는 전송매체를 사용함으로써 매체의 특성상 보안에 대한 취약성을 내포하고 있다. 물리적으로 접근이 어려운 유선과는 달리 무선 구간은 접근이 용이하므로 데이터를 암호화 함으로써 기밀성을 유지하고 인증 된 사용자에게만 네트워크 접속을 허용해야한다[2]. IEEE 802.11b에서는 이러한 사용자 인증 및 기밀성을 위하여 SSID(Service Set Identifier), MAC(Media Access Control) 주소, 그리고 WEP(Wired Equivalent Privacy)키를 이용하고 있다[2]. 하지만 IEEE 802.11b 보안 메커니즘에는 이미 많은 취약점들이 알려져 있다[3]. 이러한 취약점들을 보완하고자 고안된 것이 IEEE 802.1x EAP(Extensible Authentication Protocol)이다[4]. 여기서는 네트워크에 접속을 허용하기위해 여러 가지 인증유형들을 제공하고 있으며, 이러한 인증 유형들에는 EAP-MD5, EAP-TLS, EAP-TTLS등이 대표적이지만, 이 또한 상호 인증과 실시간 인증에 있어서 문제점을 가지고 있다.

이와 더불어 최근 인터넷 환경에서 제공되는

응용서비스에 암호화 기술을 이용한 보안시스템이 많이 등장하고 있다. 현재 보안 기능을 일관성 있게 제공해 주는 기술로 PKI(public key infrastructure)를 들 수 있다. PKI를 이용한 서비스들은 서로 통신하는 상대방을 인증하거나 또는 향후 거래 사실의 부인을 방지하기 위하여 인증기관(CA : Certification Authority)에서 발급한 인증서를 이용하는데 사용자는 수신한 인증서를 이용하기 전에는 반드시 인증서의 진위를 검증해야 한다. 인증서 소유자가 인증서를 분실하였거나 인증서의 비밀키를 잊어버렸을 경우 등의 이유로 인증서 유효기간 내에 CA에게 인증서 폐지신청을 할 수도 있기 때문에 반드시 인증서를 발급한 CA에게 인증서 폐지신청을 할 수도 있기 때문에 반드시 인증서를 발급한 CA에게 문의하여 인증서의 진위를 검증해야 한다. 그 동안 주로 이용되고 있는 인증서 검증 방법에는 인증서를 발급한 CA로부터 인증서 폐지목록(CRL : Certificate Revocation List)을 다운로드 하여 자신이 직접 검증하는 방법과 인증서 검증을 대신해주는 온라인 인증서 상태 검증 프로토콜(OCSP : Online Certificate Status Protocol) 서버를 이용하는 방법이 있다[5, 6].

이러한 무선 LAN을 이용하려는 클라이언트는 인증서버가 필요하며 인증서버의 인증서를 검증하기 위하여 네트워크로부터 CRL을 전송받거나 OCSP와 같은 인증서 검증서버에 접속해야 하는데 포트기반 접근제어방식을 이용하는 IEEE 802.1x에서는 클라이언트가 인증서버로부터 인증을 받기 전에는 인증서버 외의 네트워크 자원에 접속할 수 없다. 따라서 클라이언트가 인증서버를 실시간으로 인증할 수 없는 문제가 발생한다.

본 논문에서는 IEEE 802.1x기반의 EAP 인증의 문제점인 상호 인증과 실시간 인증의 문제점을 해결하고, 인증서의 유효성 검증을 빠르고 정확히 할 수 있으며 특정 검증 서버에 부하를 집중시키지 않음으로써 검증시스템의 안정화를 이룰 수 있는 보안 시스템을 설계하고자 한다.

II. IEEE 802.11b 보안의 취약점

IEEE 802.11b 표준에서 사용자 인증은 MAC(Media Access Control) 주소를 이용하여 암호화되지 않은 상태로 수행된다. 각 AP는 인가된 단말의 MAC주소 리스트를 가지고 있고 접속을 요청하는 단말의 MAC 주소를 자신의 리스트와 검사하여 유효한 사용자인지를 판별한다. 하지만 이와 같은 MAC 주소 인증 방식에서 누군가 네트워크를 도청하고 있다면 브로드 캐스트 되는 MAC주소를 금방 알아챌 수 있다. 기존의 무선 LAN은 보안 문제뿐만 아니라 확장성에도 문제가 있다. 사용자 장치의 MAC주소는 무선 LAN의 각 AP에 저장되어 있어야 하는데 이는 관리상의 불편함이 있을 뿐만 아니라, 만일 관리상의 실수가 생긴다면 심각한 보안 사고를 초래할 수 있다. WEP은 원래 유선랜과 같은 수준의 보안성을 제공하고자 만들어졌으나 근래 여러 보고서에 의하면 WEP 프로토콜은 크랙이 쉽고 무선 데이터 정보 전송 시 위험성이 심각하다고 알려져 있다[4]. WEP 알고리즘은 암호키가 상수이고 IV가 너무 작다. 24bit 길이의 IV는 재사용이 가능해서 동일한 의사 난수 키 스트림(Key Sequence)을 생성시키기 쉽다. 따라서 IV의 크기가 작은 점을 이용하여 <IV, 키 스트림>을 저장한 실시간 공격 가능성이 많은 것도 WEP의 단점이 된다[7]

III. EAP의 인증 방식의 취약점

EAP의 인증 방법을 설명하면 다음과 같다.

첫 번째로 EAP-MD5는 무선 네트워크에서 가장 기본적인 인증을 하는 방법이다. 저장된 패스워드를 사용하는 방식으로 인증 방식은 사용자와 서버사이에 상호인증이 없이 무조건 신뢰하는 방식이다.

두 번째로 EAP-TLS는 사용자와 서버중 한 개의 인증서를 이용하여 상호 인증하고, 그 결과에 의해 쌍방 간에 공유하는 세션 키를 생성하여 인증하는 방식이다. 이런 인증 방식의 특징은 안전한 터널을 통하여 세션 키를 가지고 동적인 WEP 키를 생성하여 안전한 인증을 하는 방식이다..

세 번째로는 EAP-TTLS와 PEAP로 이 두 인증 방식은 서로 비슷하다. 사용자와 서버 모두 인증서가 사용하는 가장 확실한 인증 방법이지만 모든 사용자가 인증서를 가지고 있어야 하기 때문에 비용이 많이 들어간다는 문제점을 가지고 있다.

마지막으로는 LEAP로 시스코 무선 네트워크 환경에서 주로 사용되는 인증 방식이다. 사용자와 서버의 인증을 모두 수행하는 상호 인증절차가 사용된다. 하지만 사용자는 서버가 주는 세션키를 무조건 믿어야 하고 서버가 주는 세션키를 받음으로 자신의 비밀키를 전송해 줘야한다는 문제점이 있다. 이것은 인증서버가 공격을 당했을 경우 서버를 통해 인증을 받는 여러 사용자의 비밀키를 공격자가 쉽게 가질 수 있다.[8]

IV 실시간 무선 LAN 보안 시스템 설계

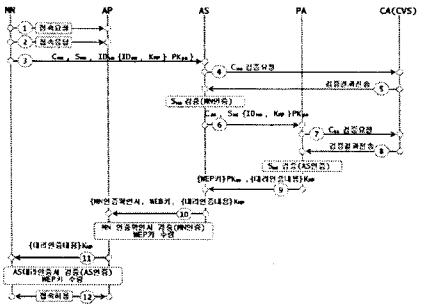
이제까지 기존 무선 LAN 보안 시스템에서 적용되었던 인증 유형과 인증서 검증방법의 문제점들을 분석하여 아래와 같이 보안적인 측면과 시스템 효율성에 관하여 개선할 점을 본 논문의 제안 목표로 정하였으며, 이러한 목적에 맞는 무선 LAN 보안 시스템을 설계하고자 한다.

A. 제안 시스템의 기본 조건

기존의 시스템에서의 문제점을 개선하기 위하

여 본 논문에서 제안한 무선 LAN 보안 시스템은 포트 기반의 접근제어 방식의 IEEE 802.1x 프레임워크상에서 공개키 기반구조의 암호시스템을 이용하고, 인증서 발급 및 관리를 담당하는 인증기관(CA)이 다중으로 설치되어 있는 환경을 제안 시스템의 기본 조건으로 가정후에 본 논문에서 구현하고자하는 무선 LAN 보안 시스템을 설계하고자 한다.

B. 제안 시스템의 인증 절차



<그림 1> 제안 시스템의 인증절차

단계 ① MN → AP : IEEE 802.11 접속요청
무선 단말기는 최적의 AP를 선택하여 접속을 요청한다.

단계 ② AP → MN : IEEE 802.11 접속응답
무선 네트워크에 접속하기위한 인증 과정의 시작을 알린다.

단계 ③ MN → AS : [Cmn, Smn, IDpa, {IDmn, KMP}PKpa]
CA가 MN에게 발급한 인증서(Cmn), MN의 개인키로 서명한 서명문(Smn), PA의 ID(IDpa)와 함께 MN의 ID(IDmn), MN와 PA 사이의 대칭키(KMP)를 PA의 공개키(PKpa)로 암호화하여 AP를 통하여 AS에 전송한다. 이와같이 MN에서 사전에 PA에 유선망을 통하여 PKI방식을 이용한 상호인증을 마쳤으며, 이에대한 MN과 PA사이에 사용가능한 대칭키를 PA의 공개키로 MN의 ID와 함께 암호화하여 기존의 EAP-TLS 방식에 추가하여 전송함으로써, 클라이언트에서는 한번의 데이터 전송만으로 인증서버와 상호인증이 가능하다.

단계 ④ AS → CVP : Cmn
CA가 MN에게 발급한 인증서의 유효성 검증을 위하여 CVP에 전송

단계 ⑤ CVP → AS : 검증결과 전송

단계 ⑥ AS → PA : [Cas, Sas, {IDmn, KMP}PKpa]
AS는 ⑤에서 전송받은 Smn에 대하여 검증을 완료함으로써 MN를 인증한다. 이후 AS자신을 인증하기 위하여 PA에게 CA가 AS에게 발급한 인증서, AS의 개인키로 서명문과 함께 MN의 ID, MN와 PA사이의 대칭키를 PA의 공개키로 암호화하여 전송한다. 기존의 EAP-TLS 방식에서는 클라이언트와 직접 인증과정을 거치는 단계에서 클라이언트에 인증서 확인을 위한 연산과, 유선망에 비하여 한정되고 보안에 취약한 무선망을 사용함으로써 인증시간의 지연과 무선망에 트래픽을 더욱 증가 시켰다. 따라서, 단계 ⑥에서와 같이 인증과정만을 클라이언트를 대신하여 처리해 줄 수있는 서버의 이용은 무선망을 이용하지 않고, 계산능력이 빠른 서버를 이용함으로써 인증에 걸리는 시간을 단축시킬 수 있다.

단계 ⑦ PA → CVP : Cas
CA가 AS에게 발급한 인증서의 유효성 검증을 위하여 CVP에 전송

단계 ⑧ CVP → PA : 검증결과 전송

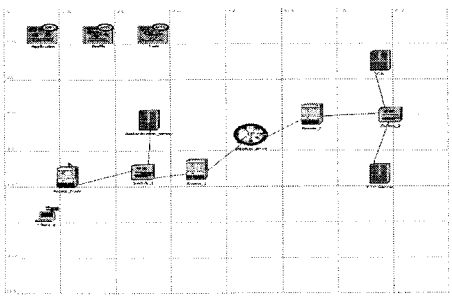
단계 ⑨ PA → AS : [{WEP키}PKas, {대리인증내용}KMP]
PA는 ⑧에서 전송받은 Sas에 대하여 검증을 완료함으로써 AS를 인증한다. 이후 WEP키는 AS의 공개키로 암호화한 정보와 AS 대리인증서를 MN과 PA의 대칭키로 암호화하여 AS에 전송한다.

단계 ⑩ AS → AP : [MN 인증확인서, WEP키, {대리인증내용}KMP]
⑥에서 MS의 인증완료에 따른 MN의 인증확인서, WEP키, AS 대리인증서를 AP에 전송한다.

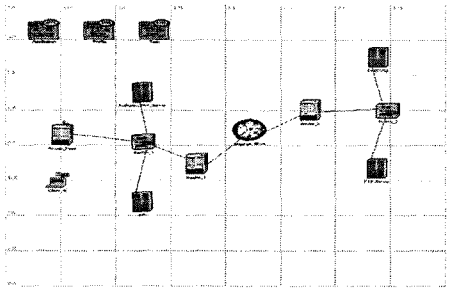
단계 ⑪ AP → MN : [{대리인증내용}KMP, WEP키]
수신한 MN 인증확인서를 검증한후 WEP키와 AS 대리인증서를 MN에 전송

단계 ⑫ MN : AS 대리인증서 검증하여 AS를 인증후 WEP키를 이용하여 무선 네트워크에 접속한다. 이와 같이 단 한번의 핸드쉐이크 과정을 거쳐 인증서버와 상호인증을 마치고 AP를 통하여 외부 네트워크에 접속이 가능하게 되었다.

V. 시뮬레이션

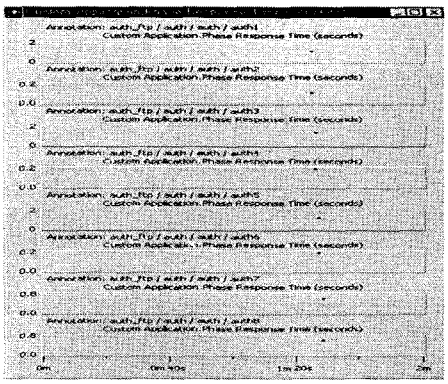


<그림 2> EAP-TLS 시뮬레이션 구성도

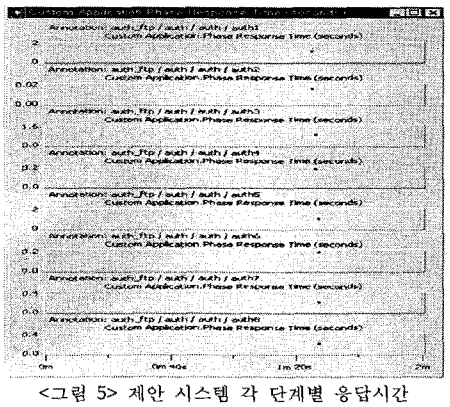


<그림 3> 제안 시스템 시뮬레이션 구성도

위 그림 같이 무선 네트워크를 Opnet 11.0 시뮬레이터를 이용하여 설계하였으며, 이를 이용하여 기존의 EAP-TLS 인증방식과 제안한 시스템과의 비교 분석을 하였다. 무선 LAN 환경은 위의 시뮬레이션 파라미터를 기반으로 시뮬레이션을 구성하였으며, 구성 모델은 Opnet 11.0에서 지원하는 무선 Network 표준 모델과 Ethernet 영역의 표준 모델을 사용하였으며, Application 영역에서는 시뮬레이션 파라미터 값을 적용하여 기존의 EAP-TLS 모델과 제안 시스템 모델을 시뮬레이션 하여 아래 그림과 같은 결과를 얻었다.

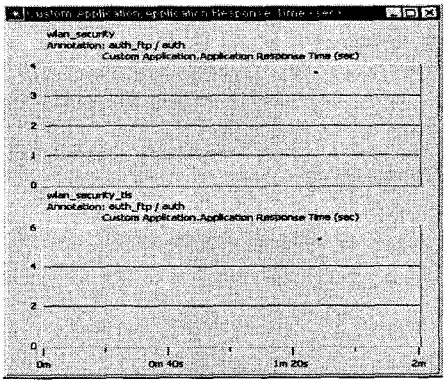


<그림 4> EAP-TLS 각 단계별 응답시간



<그림 5> 제안 시스템 각 단계별 응답시간

위 그림은 EAP-TLS의 인증에 걸리는 시간을 각 단계별로 나누어서 시뮬레이션 한 결과를 나타내고 있다. 제안 시스템과 비교하기 위하여 4Way 핸드쉐이크 단계는 간략화하여 마지막 MN↔AP, MN↔AP의 구간에서 나타내었다. 위 시뮬레이션 결과에서 보듯이 MN→AS구간과 AS→AP 단계에서 1sec 이상의 시간이 지연됨을 볼 수 있다. 이는 MN과 AS에서 상호인증에 필요한 데이터를 주고받는데 필요한 시간을 나타내고 있다. 이는 MN과 AS사이에 무선망이 존재하며, 정보의 처리량의 제한된 모바일기기가 인증서를 처리하는 과정에서 응답시간이 현저히 증가함을 알 수 있다. 따라서 본 논문에서는 클라이언트 측에서 사용되는 모바일 기기의 처리량과 인증시 속도가 느린 무선망을 사용함으로써 발생되는 지연시간을 줄여보고자 대리인증서버를 사용한 상호인증 시스템을 제안하여 시뮬레이션 결과를 얻었다.



<그림 6> 제안 시스템과 EAP-TLS의 인증 응답시간

. 기존의 EAP-TLS방식에 비하여 1.6sec 정도 단축된 인증시간을 위 시뮬레이션 결과에서 확인할 수 있다. 이는 제안한 인증 시스템에서 추가된 대리인증서버가 무선 클라이언트를 대신하여 인증서버를 인증함으로써 인증시간은 단축 되었다. 이와 더불어 새롭게 추가된 대리인증서버 때문에 발생되는 유선망에서의 트래픽과 로컬망에서의 추가된 대리인증서버로 인한 망 구축비용의 증가는 무선망을 구축하려는 사업자측면에서는 부담이 될 수 있다.

하지만, 향후 무선망을 사용하는 사용자들이 급속도로 증가한다면 보안에 대한 요구사항이 늘어날 것이고, 또한 다양한 무선 단말들이 사용될 기존의 인증 시스템으로는 많은 가입자를 수용할 경우 무선망에서의 트래픽은 제안시스템에서보다 현저히 증가된다. 그리고, 단말 또한 소형 무선단말의 경우 인증을 위한 지연시간은 더욱더 증가될 것이다.

따라서, 위 시뮬레이션 결과에서와 같이 본 논문에서 제안한 시스템을 이용한다면 한정된 무선

망에서 단말의 인증에 관련된 트래픽을 줄여줌으로써 같은 무선 네트워크를 이용하는 다른 단말이 인터넷을 사용함에 있어서 여유를 줄 수 있다. 이렇게 무선망에서 줄어든 트래픽을 유선망에서 대역폭을 좀 더 확보한다면 오히려 보다 적은 비용으로 무선 가입자를 확보 할 수 있을 것이며, 대리인증서버의 사용으로 인하여 인증서 처리에 대한 부담이 줄어들어 다양한 무선 단말이 무선망을 사용가능하다면 대리인증서버의 추가는 많은 가입자를 확보할 수 있는 방법이 될 수 있다.

또한 무선망에서 접속을 시도하는 클라이언트는 최종적으로 한번의 핸드쉐이크 과정을 거쳐 인증서버와 상호인증을 완료함과 동시에 기존의 CRL방식의 인증서 검증방식이 아닌 CVS를 사용함으로써 실시간 인증을 동시에 수행 가능한 시스템을 본 논문에서 제안하였다. 이는 향후 인증과 관련하여 실시간 인증의 중요서은 더욱더 커질 것이므로 이에 대한 대비 또한 함께 이루어질 수 있다.

Ⅶ. 결 론

무선랜에서 인증서의 유효성을 검증하기 위해 CRL을 이용할 경우 시간차 문제 때문에 실시간으로 그 유효성을 검증할 수 없으며 OCSP를 이용할 경우 규모가 큰 보인시스템에서는 인증서버로부터 승인받기 전에는 유선랜으로 접근이 허용되지 않기 때문에 인증서버를 실시간으로 인증할 수 없다. 그리고, 기존의 인증 방식의 문제점을 해결하기 위하여 IEEE 802.1x를 이용한 PKI 인증방식이 많이 사용되고 있다. 하지만 이러한 인증방식 또한 상호인증과 관련하여 현재까지 EAP-TLS를 제외하고는 인증 요청자와 인증서버 사이에 공인 인증서를 사용하는 인증 프로토콜은 없는 실정이다.

이러한 이유 때문에 본 논문에서는 인증 경로 검사와 인증서 검증을 CA와 직접 접속하여 처리하는 CVS를 이용하였다. 이에 따라 인증서 폐지 정보를 실시간으로 파악할 수 있어 인증서 유효성 검증 결과 값의 현재성을 얻을 수 있었고 각 CVS에 인증서 유효성 검증 업무를 분산시킴으로써 다중 CA 환경에서 특정 검증기관에 부하가 집중되는 것을 막을 수 있다. EAP-TLS의 경우 상호 인증도 가능하고 공인 인증서를 사용함으로써 공인된 인증방식이라 할 수 있지만, 인증상태에 대한 현재성에 있어서는 아직 명확히 해결되지 못하는 문제점이 있다.

따라서 본 논문에서 제안하는 방식인 대리 인증 서버를 이용함으로써 인증, 안전성, 효율성 측면에서 기존 시스템의 문제점이 개선 되었음을 분석하였고, Opnet 11.0를 이용한 시뮬레이션 결과에서 볼 수 있듯이 성능 또한 기존의 EAP-TLS의 인증 대기 시간보다 1.6sec 이상 시간을 단축시켰음을 볼 수 있다. 향후 무선 LAN이 전국에 보급되어 많은 사람들이 무선 인터넷을 안전하게 사용될 것은 분명한 사실이다. 하지만 보안이 허술한 현재의 무선 인터넷의 문제점을 극복하고 많은 사람이 안전하게 무선망에 접속할 때 보다 빠르고 안전한 인증방식의 필요성은 대단히 중요하다고 볼 수 있다. 이에 본 논문에서는 향후 무선 LAN 사용자가 많아지고, 보안에 대한 인식이 보편화 되었을 때, 효과적으로 적용이 가능한 인증 프로토콜 설계에 있어서 많은 참고 사항이 될 것이다.

참고문헌

[1] S. Rommer, " Security Issue in Public Access WLAN Architectures," Ericsson Telecom Report, March, 2002

[2] "IEEE 802.11b Wireless LAN Medium Access Control (MAC) Physical Layer (PHY) Specification", IEEE Standard 802.11b, 1999.

[3] W. A. Arbaugh, "Your 802.11 Wireless Network has No Clothes", University of Maryland, Mar. 2001

[4] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", IETF RFC 2284, Mar. 1998.

[5] R. Housley, W. Ford, W. Pork, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", IETF RFC 3280, Apr. 2002

[6] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "X.509 Public Key Infrastructure : Online Certificate Status Protocol - OCSP", IETF RFC 2560, Jun. 1999.

[7] R. Rivest, "The MD5 Message-Digest Algorithm," IETF RFC 1321, April. 1992.

[8] C. Rigney, "Remote Authentication Dial In User Service(RADIUS)," IETF RFC 2865, June. 2000.