VPN 보안 게이트웨이 모델 구현

문두현*, 최현석*, 박세현*, 송오영*
*중앙대학교, 전자전기공학부

A Implementation of Security VPN Gateway Model.

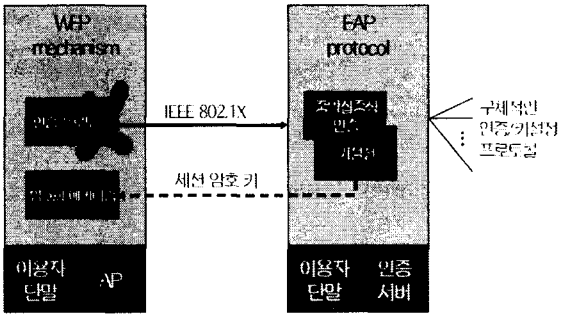
Du Hyun Mun*, Hyun Suk Choi. Se Hyun Park*, Oh Young Song*
School of Electrical & Electronics Engineering Chung Ang Univ.

요 약

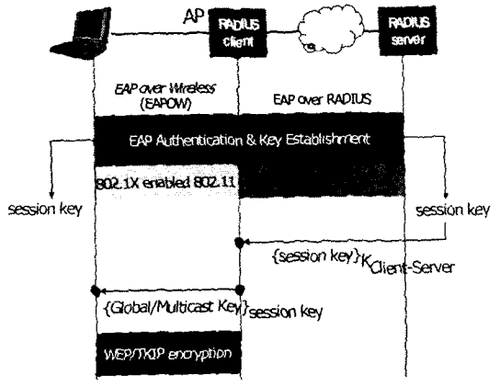
본 논문에서는 Security 보안 게이트웨이를 이용하여 VPN 기반 보안 터널링을 생성하여 기존의 단말의 안전한 데이터 전송을 보장하고 Rogue AP에 의한 사용자의 정보 누출 가능성을 최소화 할 수 있는 보안 게이트웨이를 구현하였다. 무선랜 방식은 기존의 유선랜에 비해 사용하기 편리하다는 장점이 있지만 수신 장비만 있으면 누구나 데이터를 수신할 수 있는것처럼 보안에 취약한 단점이 있다. 기존의 무선랜 보안 모델은 802.1X 와 RADIUS 서버를 이용하여 장비 업체별 상이한 솔루션으로 호환이 불가능하고 Rogue AP에 의한 위협이 있다. 본 논문에서 구현한 보안 게이트웨이는 2계층과 3계층에 보안 모델을 도입하여 데이터 전송을 안전하게 할 수 있다.

I. 서론

초고속 인터넷에 대한 사용자들의 요구가 커지면서 초고속 인터넷이 가능한 무선랜의 중요도가 높아지고 있다. 하지만 유선랜에 비해 무선랜은 보안적 위협이 많다. 하지만 무선랜 시스템의 보안기술 개발이 활발하게 전개되면서 무선랜 사용자들에게 안전한 통신을 제공할 수 있을거라는 기대감과 함께 사용자도 점차적으로 증가해가고 있는 추세이다. 기존의 무선랜 보안 모델은 802.1X(Port based Network Access Control)과 RADIUS 서버를 이용하여 버안 모델을 제시하고 있는데 이것은 사용자 기반 인증과 Dynamic WEP을 이용하여 데이터의 무결성을 보장한다는 이점이 있는 반면 장비 업체별 상이한 솔루션으로 인한 호환성의 결여와 Rogue AP에 의한 정보 누출 가능성이 심각한 것으로 알려져 있다. 이러한 단점을 보완하기 위해서 본 논문에서 구현한 보안 게이트 웨이는 Rogue AP에 의한 사용자 정보 누출을 방지하고, 접근 정책에 의한 중앙 집중 관리, AP(모니터링 및 관리의 편리성, 무선랜의 외부 공격에 대한 보호 용도의 Firewall 기능을 중심으로 구현하였다. 단말 클라이언트 프로그램에 802.1X 기반 인증 기능과 L2L Security 기능을 포함시키고 보안 게이트웨이 프로그램에서는 SNMP (Simple Network Management Protocol)기반 AP 관리 기능과 EAP-TTLS 중계기능, 접근 정책에 의한 중앙관리 기능과 L2L Security 기능을 추가하여 기존 무선랜의 보안적 취약점을 보완 할 수 있다. 이것은 기존의 무선랜 사용방식의 보안적 취약점을 하드웨어적으로 극복하는 것으로 소프트웨어적으로 적용할 수 있는 엑세스 포인트 설정이나, 인증, IDS 또는 암호화와 같은 방법 보다 VPN 네트워크상의 사용자 증가로 인한 트래픽의 증가를 하드웨어적으로 극복할 수 있는 방법이라 할 수 있다.



< 그림 1. 802.1x >

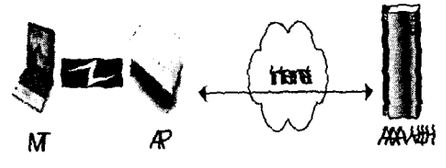


< 그림 2. 802.1x 인증 과정 >

II. 기존 무선랜 보안 모델의 문제점

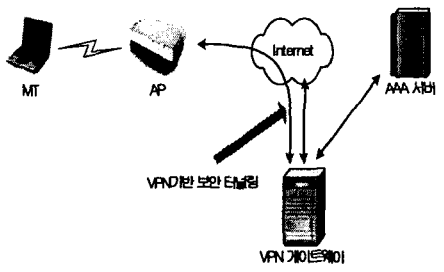
기존의 무선랜 보안 방식은 크게 접근제어와 정보보호 두가지 방식의 보안 매커니즘으로 나눌수 있다. 하나는 서비스 집합의 SSID (Service Set Identifier)를 이용한 방식이고 다른 하나는 WEP (Wired Equivalent Privacy) 이다. SSID는 도메인 이름으로 처리하는 기능으로 접근제어의 기본적인 수준을 제공한다. SSID는 보통 유선랜 장치들에 대한 네트워크 이름이며, 네트워크를 세그먼트로 분리하여 사용할 때 활용된다. 그러나 이러한 방식은 외부의 무선랜 장비에서 SSID의 이름만 일치 시켜주면 해당 사이트로부터 전송되는 전파를 캡춰하여 도청이 가능하다는 취약점이 있다. 두 번째 방식인 WEP은 대칭 암호화 알고리즘을 사용하여 자료의 암호화 복호화를 처리한다. WEP의 주요 목적은 접근제어와 정보보호 기능을 제공하는 것이다. 과거에는 40 bit 의 키를 사용하여 암복호화 알고리즘에 사용했으나 현재는 키 자체의 취약점이 드러나 104bit 키를 사용하는 추세이다. WEP의 단점으로는 많은 시스템들이 넓게 분포되어 있을 때 디폴트 키들을 악의적으로 사용하고자 하는 시스템이 있을 때 고정된 키로 인해 여러 보안적 문제점이 발생할수 있다는 것이다. 또 단방향 키 분배 시스템은 단말의 수가 증가할 수록키 관리 및 운영의 어려움이 따른다는 단점이 있다. 무선랜의 기존 인증 방식은 클라이언트가 인증 시스템에 의해 인증을 받지 못하면 무선랜의 서브시스템과 연결될 수 없다. IEEE 802.11b 표준은 공개 인증 방식과 공유키 인증 방식의 인증 메카니즘을 제공한다. 이런 인증 방식은 암호화 되지 않은 평문 형식으로 이루어고 WEP키를 사용한다 하더라도 WEP 키의 분실로 인한 잘못된 사용자의 보안 위협과 정당한 사용자의 WEP 키 사용상의 문제점이 발생할 수 있다. Access Point의 문제점으로는 IEEE 802.b의 공유키 인증체계는 단방향의 인증 방식을 사용하기 때문에 엑세스 포인트는 한 사용자를 인증할 수 있지만, 사용자는 엑세스 포인트를 인증할 수 없다. 올바르게 설정되지 못한 엑세스포인트가 무선랜 구간에 설치되어 있는 경우 합법적인 사용자의 하이재킹에 의해 서비스 거부공격이 발생할 수 있다. 이런한 문제점을 해결할 수 있는 방법은 클라이언트와 인증서버간의 상호 인증방식을 사용하여 양측간의 합법성을 증명하는 것이다. 클라이언트와 인증서버간의 통신은 엑세스포인트를 사용하기 때문에, 엑세스 포인트는 상호 인증 방식을 지원해야만 한다. 상호인증 체계 방식은 잘못 설정되어 설치된 엑세스 포인트를 고립시키거나 탐지한다. 이러한 문제들 말고도 기존의 무선랜 방식은 무선랜 하드웨어 분실시 MAC Address 및 WEP 키의 분실로 인해 악의적인 사용자가 정상적인 사용자를 위장하여 서버에 접근할 수 있다는 문제도 발생할 수 있다. 이러한 문제를 보완하기 위해서는 장비의 독립적인 인증 방식이 필요하고 또한 인증 방식에 근거한 동적인 WEP 키가 사용되어야 한다. 또 불법적인 AP에 의한 사용자에 대한 DDoS 공격을 막기위해서 AP의 지속적인 관리가 필요하다. 또 예방책으로서 상호인증방식과, 동적 WEP키를 생성하여 사용하고 WEP키에 근거한 세션방식의 사용과 사용자에 대한 WEP 세션키의 시간종료 값을 정의하고 이를 시행하기 위한 타이머가 구현외어야 한다. 본 논문에서는 이러한 문제점과 개선점을 반영하여 VPN Gateway를 구현했다.

III. Security VPN Gateway



< 그림 3. 기존의 무선랜 모델 >

본 논문에서 구현한 VPN Gateway의 모델을은 다음의 구성도와 같다.



< 그림 4. 보안 게이트 모델 >

그림 1과 같이 기존의 무선랜 보안 모델에서는 AP와 AAA 서버 사이에 Internet을 사용함으로서 여러 가지 보안적 문제점을 발생시키는 반면에 구현된 보안 Gateway 모델은 AP 와 AAA 서버 사이에 VPN Gateway를 설치 하여 VPN 기반 보안 터널링을 생성하고 관리자가 VPN Gateway의 접근 정책을 관리하고 SNMP를 사용하여 Rogue AP를 실시간으로 모니터링 하는데 편의성을 제공하여 불법적인 AP의 침입을 사전에 막을 수 있고, 등록된 단말외에 트래픽이 있는 경우 전송 경로를 추적하고 연결을 끊음으로서 네트워크 상의 트래픽을 관리자가 스스로 조절할 수 있다. 그리고 Internet을 통한 AP의 불법적인 공격을 사전에 관리자가 관리함으로서 Firewall의 역할도 수행 할 수 있다. 단말은 AP에 Association 하고 DHCP를 통한 IP분배까지는 인증을 받지 않아도 가능하도록 구성하였고, Rogue AP에 의해 전송되는 트래픽인지 아닌지는 상관없이 인증 받지 않은 사용자의 트래픽은 차단하고 인증받은 사용자의 패킷은 통과 하게 구현함으로서 Rogue Ap에 의한 트래픽을 줄일 수 있다.

IV. 파일럿 시스템 구축

●단말과 보안 게이트웨이간 EAP-TTLS

●보안 게이트웨이와 RADIUS 서버간 EAP over RADIUS

●보안 게이트웨이를 통해 트래픽 제어

■ Wireless Firewall 개념으로 내부 인증 받은 단말의 트래픽만을 외부로 보낸다.

■ 단말은 AP에 Association하고 DHCP를 통한 IP 분배까지는 인증 받지 않아도 가능하도록 구성

■ Rogue AP에 의해 전송되는 트래픽인지 아닌지는 상관없이, 인증 받지 않은 사용자의 트래픽은 차단하고 인증 받은 사용자 패킷은 통과한다.

■ AP는 허브 기능만 수행 (기존의 AP로 사용가능)

■ AP 모니터링 기능 (SNMP를 이용)

■ 필요에 의한 L2L Security 제공

RADIUS 서버	- RADIUS 표준 지원 - EAP over RADIUS 지원
보안 게이트웨이	- 인증 프로토콜 : EAP-TTLS - 데이터 비밀성 : SSL 이용 - 사용자 DB 사용
Virtual AP	- 노트북 이용 - 네트웍 인터페이스 : 유무선랜 - 인증 프로토콜 : 802.1x, EAP-TTLS

< 표 1. 파일럿 시스템 스펙 >

V. 결론

기존 무선랜 보안 모델은 사용자 기반 인증 과 Dynamic 이용으로 데이터의 무결성을 보장한다는 장점이 있으나 Rogue AP에 의한 사용자의 정보 누출 가능성이라는 큰 보안적 문제점을 가지고 있는데 이 논문에서 구현한 Security VPN Gateway는 2계층과 3계층에 VPN 모델을 도입하여 단말의 안전한 데이터 전송을 보장하고 있다. 이러한 방법외에도 소프트웨어적으로 (엑세스 포인트 설정, 패치 & 업그레이드, 인증, 개인 방화병, 침입탐지 시스템, 암호화 보안 평기)가 있고, 다른 하드웨어 구현으로는 스마트 카드나 PKI, 생체 인식 등의 방법이 있다. Security VPN Gateway 구현 후에 지속적인 Test 결과 장점과 함께 단점도 도출 되었는데 단말의 개수에 비례해 보안 터널링을 유지가 계속 증가한다는 단점과 그런 보안 터널링 유지를 위한 Overhead가 문제점으로 발생하여 이에대한 연구가 더 필요하다. 또한 현재 Draft 상태인 802.1aa (Port-Based Network Access Control) 와 802.11i (Medium Access Contorl Security Enhancements) 와의 연동에 대한 연구가 필요하다.

참고문헌

[1] IEEE Standard for Local and metopolitan area networks - Port-Based Network Access Contorl . Standard 14.June 2001

[2]http://www2.rad.com/networks/1995/snmp/snmp.htm

[3] Aboba, B. and D.Simon , "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.

[4] Blunk, T. and J. Vollbrecht, "PPP Extensible Authentication Protocol ", RFC 2284, March 1998

[5] Dierks, T. and C. Allen, " The TLS Protocol Version 1.0", RFC 2246, November 1998.

[6] draft-ietf-pppext-eap-ttls-02[2].txt Basic Commerce&Industries, Inc. November 2002