

IEEE 802.11 무선 LAN 보안 취약점 분석 및 보안 시스템 설계

박종근^o, 이극
한남대학교 컴퓨터공학과

Design of Security System and Analysis Security Vulnerability On IEEE 802.11 Wireless LAN

ChongKun Pak, LeeGeuk
Dept. of Computer Engineering, Hannam Univ.

요 약

현재의 802.11 무선 LAN은 54Mbps 속도와 유선 네트워크 정도의 품질을 갖추고 있다. 무선의 편리함으로 인해 많은 사설망에서 사용되고 있으며 핫스팟 서비스도 점차 증가되는 추세여서 이에 따른 보안의 중요성도 점점 커져가고 있다. 본 논문에서는 무선 LAN 환경에서의 보안 취약성을 분석하고 이에 대처할 수 있는 방안에 대하여 논의하며 최종적으로 무선 LAN 환경에 적합한 보안 시스템을 설계하고 구현하였다.

1. 서론

무선 LAN은 기존의 유선 케이블로 연결되어 있는 네트워크 망의 인프라를 이용하는 대신 무선 전파를 매체로 하여 무선 네트워크 내의 정보처리 기기간의 데이터 교환을 장소에 구애 받지 않고 실현 할 수 있는 시스템이다. 현재의 무선 LAN은 미국 전기전자 공학회(IEEE)의 802.11 표준에 따르는 것으로 관공서, 학교, 기업 등의 사설망 뿐만 아니라 개인이 이용할 수 있는 공중 무선 LAN 서비스인 핫스팟이 등이 있다. 무선 LAN은 무선 AP(Access Point)와 무선 클라이언트 사이의 무선 통신에 의하여 데이터 교환을 한다. 이러한 무선 LAN의 통신 구간은 개방되어 있어 네트워크의 최대 관심사인 보안에 있어서는 유선 LAN에 비하여 매우 취약하다. 유선 LAN은 전송 신호가

호가 유선이라는 한정된 물리 매체에서만 존재하므로 강력한 물리-접근 제어로 보호할 수 있다. 하지만 무선 LAN의 전송 매체는 전파이므로 수신기가 영역 내에 있으면 누구라도 접근할 수 있도록 설계되어 있으므로 네트워크 스니핑에 완전히 노출되어 있다.

본 논문은 802.11 무선 LAN이 가지는 보안 취약점에 대하여 연구 분석한 자료를 토대로 무선 LAN 환경에 적합한 보안 시스템에 대하여 논의한다.

2. 관련연구

2.1 MAC 필터링

MAC 필터링이란 MAC 주소를 이용하여 합법적인 클라이언트와 비합법적인 클라이언트를 구별하는 방법이다. 이것은 AP에 직접 설정하거나 RADUIS에

설정하여 최소한의 보안을 구현할 수 있다. 무선 LAN에서의 MAC 주소는 클라이언트의 무선 LAN 카드에 설정되어 있는 48비트의 하드웨어 주소를 말한다. 이것은 초기 제조과정에서 부여된 것으로 기본적으로 MAC 주소는 변경이 불가능하다. AP는 네트워크에 접속할 수 있는 MAC 주소의 허용리스트를 관리한다. 보안의 관점에서 보면 MAC 필터링은 OSI 모델의 2계층에서 발생한다. 때문에 2계층에서 필터링 되면 나머지는 더 이상 처리되지 않는다.

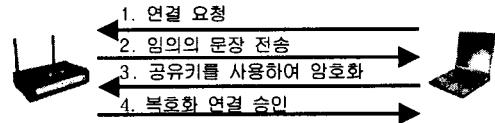
2.2 WEP

무선 LAN은 전파 매체를 이용하여 통신을 하므로 스니핑에 취약하다. 이 문제를 해결하기 위해서는 802.11은 WEP(Wired Equivalent Privacy)을 통하여 두 가지 보안기능(비밀, 승인)을 제공한다. WEP기능은 전송 정보를 암호화하여 보내고, 암호 키를 가진 수신기만이 전송정보를 해독할 수 있다. WEP은 암호화 없음, 40비트 암호화, 128비트 암호화의 형태로 보안 기능을 제공한다. 40비트 암호화 또는 128비트 암호화는 RC4 알고리즘에 의하여 클라이언트와 AP 사이에 전송되는 데이터를 암호화 하는 것을 말한다. WEP에서 사용하는 RC4 알고리즘은 RSA에서 만든 것으로 공유키로 임의의 문자열을 스트림 암호화를 사용하여 만든다. 송신자는 스트림 키와 평문을 XOR 연산하여 암호문을 만든다. 수신자는 공유키와 스트림 키를 가지고 있으므로 암호화된 문장을 역순으로 해독하여 평문을 얻는다.

2.3 WEP 인증 절차

WEP을 이용하여 인증하는 과정은 [그림 1]과 같다. 인증을 요구하는 클라이언트가 WEP를 사용하는 AP 인 연결 요청을 보낸다. AP는 요청을 받고 임의의 문장을 클라이언트에게 보낸다. 임의의 문장을 받은 클라이언트는 공유키를 이용하여 RC4 암호화를 수행한 후 암호문을 AP에게 보낸다. AP는 암호문을 자신의 공유키로 복호화 하여 원래의 문장과 비교한다. 만약 두 문장이 서로 일치하면 클라이언트의 공유키

와 AP의 공유키가 같은 것으로 인증에 성공하게 된다.



[그림 1] WEP 인증 절차

3. 무선 LAN 보안 취약점

3.1 MAC 필터링 취약점

국내의 경우 KT의 넷스팟 서비스에서도 단기간 사용 고객을 대상으로 MAC 필터링 인증 방식을 사용하고 있다. MAC 주소의 변경은 운영체제에서도 가능 하지만 구형의 무선 LAN 카드는 MAC 주소를 사용자가 임의로 지정할 수 있는 기능을 내장하는 경우도 있다. 공격자는 MAC 주소를 변경 하여 허가되지 않는 MAC 주소를 허용된 주소로 속일 수 있다.

3.2 WEP의 취약점

WEP은 초기 설계 당시부터의 문제점과 키 관리의 문제점등 많은 취약점을 가지고 있다. WEP을 사용하는 모든 사람들이 동일한 비밀 키를 공유한다. 이것은 WEP 키가 공격자에게 노출될 경우 보안에 커다란 문제점이 발생할 수 있음을 암시한다. AP를 통해 전송되는 무선 클라이언트들의 트래픽을 스니핑 하면 WEP 암호화된 자료를 수집할 수 있다. 이러한 자료를 토대로 수초 내에 WEP 키를 크랙 할 수 있으며 이미 AirSnort, WEPcrack 등의 공개 툴이 출시되어진 상태이다. WEP 키의 크랙이 가능한 이유는 현재 사용되는 모든 키가 정적인(static) 상태에 있기 때문이다. 다시 말해서 디바이스가 완벽히 재설정될 때 까지는 동일한 키가 사용된다는 것을 의미한다. 그러므로 공격자는 스니핑을 통해 수집된 암호화된 WEP 데이터를 바탕으로 WEP 키를 크랙할 수 있다.

3.4 무선 LAN 스니핑

무선 LAN에서의 스니핑은 전파의 범위 내에서 흐르는 무선 데이터를 수집하는 것을 말한다. 유선의 물리적인 연결과 다르게 수신기가 전파 범위에 있으면 스니핑이 가능하므로 무선 LAN은 스니핑에 매우 취약하다. 일반적으로 공격자는 무선 LAN 모니터링 툴인 NetStumbler, Ethereal, AiroPeek을 이용하여 네트워크를 스니핑한다. 스니핑은 유선네트워크와 마찬가지로 무선 LAN 카드를 “Promiscuous mode”로 설정하는 과정으로 이루어 진다. 그러나 유선과 다르게 모든 무선 LAN 카드가 “Promiscuous mode”를 지원하지는 않는다. “Promiscuous mode” 모드를 지원하는 무선 LAN 카드는 프리즘 2 칩셋을 사용한 경우이며 국내 모델의 경우 “삼성” 무선 LAN 카드가 “프리즘 2” 칩셋을 사용한다.

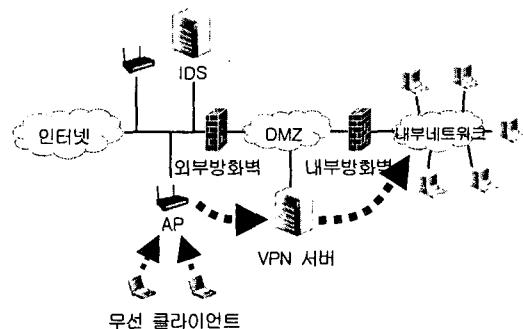
4. 무선 LAN 보안 시스템

4.1 시스템 구성 및 설계

본 논문에서 구현하고자 하는 무선 LAN 보안 시스템은 기존의 유선 네트워크 환경에서 갖추어진 보안 시스템에 무선 LAN 환경에 적합한 보안 능력을 추가할 수 있도록 설계하였다. 강력한 무선 LAN 보안 환경을 구축하기 위해서 AP를 방화벽 밖에 설치하였으며 무선 LAN 구간과 기존의 유선 네트워크 구간을 연결하기 위해서는 VPN 사용하도록 하였다. 이와 같이 무선 LAN 구간과 유선 네트워크 구간을 분리하면 공격자는 WEP 키를 해독하거나 MAC 주소를 스포핑하는 등의 보안 대책을 우회하여 AP에 접속했다 하더라도 내부 네트워크에는 접근할 수 없게 된다. VPN을 사용함으로써 내부네트워크로 전달되는 모든 트래픽은 강력한 암호화가 이루어 지며 허락되지 않은 사용자의 접근을 원천적으로 차단할 수 있다. 본 논문에서 구현한 보안 시스템은 [그림 2]와 같다.

AP는 무선 LAN을 이용하기 위한 필수 접속 점이지만 공격자가 내부 네트워크로 접근할 수 있는 최

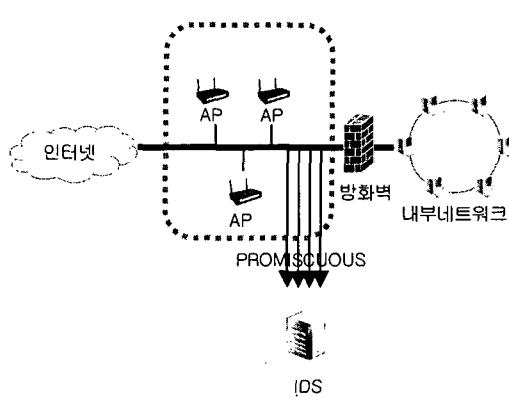
적의 경로 이기도 하다. 일반적으로 무선 LAN을 설치 할 때 네트워크 관리자가 가장 고려 해야 할 부분 중 하나가 AP의 위치 선정이다. 네트워크 사용자의 편의성의 위해 설치한 무선 AP 가 방화벽 안쪽에 설치 되었을 경우 해커에게 내부 네트워크를 그대로 넘겨 주는 것과 다를 바 없다. 보안을 위해서라면 AP는 방화벽 외부에 설치되어야 한다.



[그림 2] 무선 LAN 보안 시스템

4.2 무선 LAN 기반 침입탐지시스템

무선 LAN 기반 침입탐지시스템은 기존의 유선 네트워크 기반 침입탐지시스템에 무선 LAN에서의 침입이 의심되는 감사자료를 포함한 탐지 모듈을 추가 적용시킨다. 무선 LAN 기반 침입탐지시스템 [그림 3]와 같이 무선 LAN 구간에 설치한다. 기본적인 동작은 침입탐지시스템과 같이 네트워크에 지나가는 모든 패킷을 감시하기 위하여 네트워크 인터페이스 카드를 “Promiscuous Mode”로 변경하고 AP로부터 전송되는 패킷을 감시한다. 무선 LAN 기반 침입탐지시스템에는 기존의 네트워크 침입탐지시스템이 가지는 감사자료와 무선 환경에서 일어날 수 있는 공격에 대한 감사자료를 포함하고 있으므로 AP에 연결된 공격자의 악의적인 행동을 모두 차단할 수 있다. 앞에서 논의 했듯이 무선 LAN 구간에서 내부 네트워크로의 연결은 VPN이 담당하므로 무선 LAN 기반 침입탐지시스템은 무선 구간에서 일어날 수 있는 공격에 초점을 맞추어 설계하였다.



[그림 3] 무선 LAN 기반 침입탐지시스템

4.4 무선 LAN 스니핑 차단 모듈 설계

무선 LAN 카드는 제조회사마다 다른 종류의 칩셋을 사용한다. 공격자가 가장 많이 사용하는 것으로 “Hermes”와 “Prism2” 칩셋이 있다. “Hermes” 칩셋을 사용한 무선 LAN 카드는 전파의 범위에 있는 모든 AP를 동시에 보는 기능을 제공하며 WEP의 설정 여부를 파악할 수 있는 기능을 가지고 있다.

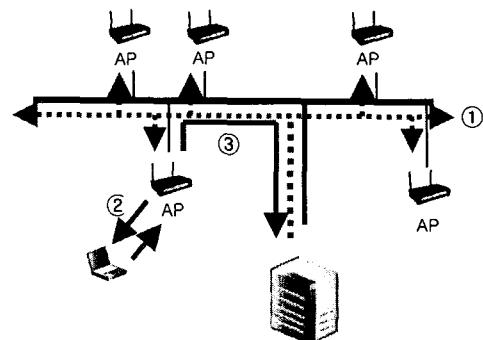
“Prism2” 칩셋을 사용한 무선 LAN 카드는 WEP의 설정 여부를 파악하지는 못하지만 네트워크의 모든 패킷을 볼 수 있는 “Promiscuous mode”를 지원한다. “Prism2” 칩셋을 사용한 무선 LAN 카드는 전파구간의 모든 트래픽을 받아 들인다. 이러한 무선 클라이언트를 탐지하기 위해서 PING(ICMP Echo Request)를 이용한다. IDS에 추가하는 무선 LAN 스니핑 탐지 모듈은 [그림 4]와 같다.

네트워크 상에 존재하지 않는 MAC 주소를 사용하여 Ping(ICMP Echo Request)를 보낸다.

AP는 존재하지 않는 MAC 주소를 사용한 Ping을 무선 클라이언트들에게 브로드캐스트 한다.

만약 IDS가 Ping reply((ICMP Echo Reply)를 받게 되면, 해당 무선 클라이언트는 “Promiscuous mode”이며 네트워크를 스니핑하고 있는 것이다.

이와 같이 존재하지 않는 MAC 주소를 사용하면 정상적인 무선 클라이언트는 Ping(ICMP Echo Request)를



[그림 4] 무선 LAN 환경에서의 스니핑 탐지
받을 수 없으며 스니핑 하고 있는 무선 클라이언트를 파악할 수 있다.

4. 구현 및 고찰

본 시스템은 보안 시스템이 적용된 유선 네트워크 환경에서 구현되었으며 기존의 침입차단시스템을 무선 LAN 환경에 맞도록 재구성하였다. 현재 본 시스템은 사설망을 기준으로 구현되었으나 향후 핫스팟과 같은 공중망에서도 응용 될 수 있을 것으로 예상된다.

5. 결론

본 논문에서는 VPN을 이용하여 무선 LAN과 내부 네트워크를 분리 하였으며 무선 LAN 기반의 침입탐지 시스템을 이용하여 무선 구간에서의 보안을 구현하였다.

[참고문헌]

- [1] “Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specifications: “IEEE Draft 802.11i/D3.0, November 2002.
- [2] IEEE, Draft P802.1X/D11, “Standard for Port based Network Access Control.” IEEE, Mar, 2001
- [3] <http://www.interlinknetworks.com/references>
- [4] IEEE, Standard for Local and Metropolitan Area Networks-Port-Based Network Access control, IEEE Std 802.1X, June 2001.