라디우스 인증 서버를 이용한 Rogue AP 차단 시스템 설계

**김동필° *강철범 *김상욱

**경북대학교 정보보호학과

*경북대학교 컴퓨터 과학과

{dpkimO, cbkang, swkim}@woorisol.knu.k

Rogue AP Protection System Based On Radius Authentication Serve

Dong-Phil Kim° Chul-Bum Kang, Sang-Wook Kim

Dept. of Computer Science, Kyungpook National University

요 약

최근 무선 네트워크 장비의 가격이 하락함에 따라 낮은 전송 속도를 가지는 이동 통신 시스템의 대안으로 무선랜 시스템의 수요가 증가 하고 있다. 그러나 무선랜은 특성상 해킹와 침투에 취약한 약점을 안고 있다. 무선랜 환경에서 유선 네트워크와 무선 네트워크를 매개해주는 액세스 포인트는 내부 네트워크안에서만 접속이 이루어진다. 이러한 취약점을 이용하여 공격자는 위장 액세스 포인트를 설치하여 내부 망으로 침투할 수 있게 된다. 본 논문에서는 무선 구간 모니터링을 하여 위장 액세스 포인트를 탐지하고 AAA서버인 라디우스 인증 서버를 사용하여 위장 액세스 포인트를 차단하는 시스템을 제안한다.

1. 서 론

무선랜 서비스가 상용화됨에 따라 이동 통신보다 속도면에서 우위를 가지는 무선랜의 수요가 증가하고 있다. 현재 무선랜 기술에서 주요 쟁점은 전송속도와 보안에 있다. 특히 보안 문제는 무선랜 기술의 보급과 사용에 커다란 장애요소이다.

무선랜은 특성상 해킹과 침투에 취약한 약점을 안고 있다. 무선랜의 기지국 역할을 하는 액세스 포인트(AP)는 유선 네트워크와 무선 네트워크를 매개해주는 역할을 하게 된다. 이 AP를 통한 접속은 비록 사용자가 네트워크의 외부에서 접속하는 것 같아 보이지만 실제로는 내부 네트워크(LAN)안에서만 접근이 이루어진다. 따라서 외부망(WAN)과 내부망(LAN)사이의 보안 문제를 해결하는 기존 유선망의 보안 기술인 침입탐지시스템이나 방화벽등으로는 무선랜의 보안 취약점을 해결할 수 없다.

이미 학교 같은 곳에서 무선랜 AP를 통한 학내 시스템의 분산 거부 공격(DDoS)이나 바이러스 침투 등의 사례가 보고 되고 있는 실정이다. 이렇게 무선랜의 취약점을 통해 내부망으로 침투가 이뤄지거나 자료가 유출되는 경우에는 물리적인 침입의 흔적이 남지 않기 때문에 피해를 당해도 공격자를 추적하기가 매우 힘들다[1].

이러한 취약성을 이용하여 공격자는 위장 액세스 포인트(Rogue AP)를 내부망에 설치하여 강한 신호강도를 사용함으로써 인가된 단말기를 이용하는 사용자의 정보를 취득하여 불법적인 네트워크 자원의 사용을 허용하게 함과 동시에 위장 액세스 포인트의 접속을 통하여 내부 주요 서버에 직접 접근하게 되는 치명적인 약점을 가지게 된다. 이러한 고역에 대해 각 액세스 포인트 제조벤더에서는 액세스 포인트 단에 MAC 필터링 기능을 제공함으로써 인가되지 않은 단말의 접근을 차단하고 있다. 그러나 MAC 주소는 윈도우의 경우에 간단한 레지스트리 편집기로, 유닉스의 경우에는 루트 쉘의 간단한 명령어로 수정이 가능하다. 또한 액세스 포인트를 연결 할 수 있는 포트만 있다면 어디서든 설치가 가능하게 되어, 쉽게 악용될 수 있게 된다.[2]

이러한 위장 액세스 포인트를 사용하여 공격자는 내부망으로 침투하게 되고 또 다른 보안상의 허점을 두게 된다. 따라서 본 논문은 무선 구간을 실시간 모니터링하여 위장 액세스 포인트를 탐지하고, 라디우스 인증서버를 사용하여 위장 액세스 포인트를 차단하는 시스템을 설계한다.

2. 관련 연구

위장 액세스 포인트(Rogue AP)

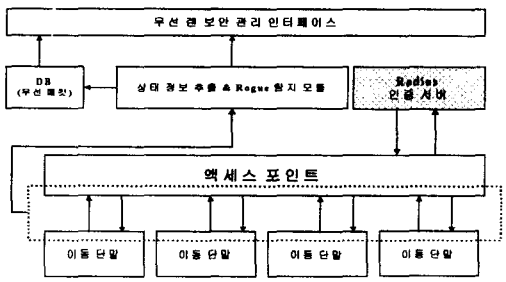
일반적으로 위장 액세스 포인트 공격은 두 가지의 형태로 나타날 수 있다. 첫번째는 내부망으로 접근 가능한 공격자가 개인적으로 사용할 수 있는 액세스 포인트를 구입하여 자신만이 사용할 수 있는 장소에 설치함으로써 내부망에 접근할 수 있는 백도어(back door)를 만들어 두는 것이다. 두 번째로, 액세스 포인트를 소프트웨어로 구성하여 강한 신호를 발생함으로써 이동 단말기가 인가된 액세스 포인트로 오인하여 접속하게 되고 사용자와 단말기의 정보를 가로 채어 인가된 단말기로 위장 함으로써 공격을 하는 것이다. 이러한 위장 액세스 포인트를 사용하여 공격자는 내부망으로 침투하게 되고 또 다른 보안상의 허점을 두게 된다.

라디우스 인증 서버(RADIUS Authentication Server)

라디우스 인증서버는 MAC주소를 인증하여 인가되지 않은 사용자의 네트워크 접근을 막는 방법이다. 일단 라디우스 서버에 사용자(Access Point) 의 MAC 주소를 등록하여 AP 사용자가 인증시에 허용 여부를 확인하는데 이용하는 방법이다. 또한 네트워크를 사용하고자 하는 이동 단말과 그 사용자들에 대하여 MAC 인증과 사용자 인증을 제공한다. 더욱이 802.1x 와 라디우스 인증 서버를 연동하여 사용할 수도 있다. 이는 무선랜 사용자에게 아이디와 암호를 주어 라디우스 서버의 인증을 받아야만 AP를 통해 무선랜을 이용하는 것이다. 802.1x는 MAC 주소 기반의 인증과 비교해 볼 때 컴퓨터 없이 이동하는 네트워크 사용자를 더 편리하게 한다. [3]

3. Radius 인증 서버를 이용한 Rogue AP 차단 시스템

3.1 시스템 구성



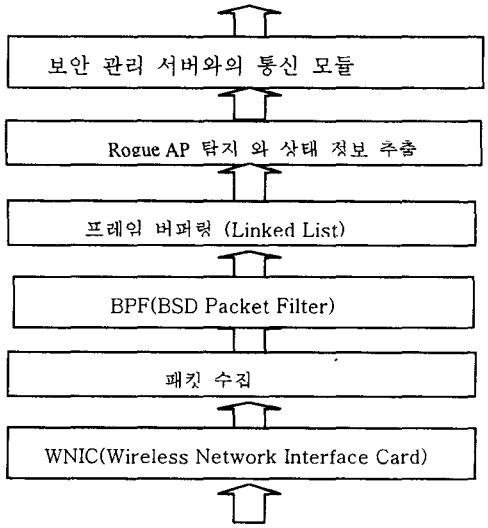
[그림 1]은 Rogue AP 차단 시스템의 구조도

본 시스템은 크게 보안 관리 인터페이스 , 무선 데이터저장 DB, 무선 구간 모니터링 에이전트, Radius 인증 서버로 나누어 진다.

보안 관리 인터페이스는 무선랜 보안 관리를 위해 무선망에서 사용되고 있는 장비를 등록하고, 현재 활성화되어 있는 액세스 포인트들의 정보와 탐지된 Rogue AP 를 디스플레이하는 관리자를 위한 툴이다. 무선 데이터 저장 DB는 무선 구간 모니터링 에이전트에서 수집한 현재 활성화된 액세스 포인트들의 정보와 Rogue AP 의 정보를 저장하는 데이터 베이스이다. 무선 구간 모니터링 에이전트는 무선 구간에서 전송되는 패킷들을 수집하고 Rogue AP 를 탐지한다. 또한 라디우스 인증 서버는 액세스 포인트나 이동 단말이 네트워크의 자원을 사용하고자 할 때 인증을 한다.

3.2 Rogue AP 탐지

본 논문에서 제안하는 Rogue AP 탐지 방법은 무선 구간을 실시간 모니터링하여, 현재 활성화된 액세스 포인트의 정보를 추출하고 , 추출된 정보를 이용하여 현재 사용이 인가된 액세스 포인트인지를 판별하게 된다. (그림 2)는 무선 구간 모니터링 에이전트의 구조도이다.



[그림 2] 무선 구간 모니터링 에이전트 구조와 동작

무선 구간 모니터링 에이전트는 두 개의 인터페이스를 가진다. 하나는 무선 네트워크의 신호 정보를 수집하는 무선 인터페이스이고 다른 하나는 수집된 정보를 보안 관리 인터페이스와 통신을 하기 위한 유선 인터페이스이다. 무선 구간 모니터링 에이전트는 다음과 같은 모듈로 구분된다.

프레임 수집, 패킷수집, BPF, 프레임 버퍼링, 정보 추출, 보안 관리 인터페이스와 통신 모듈로 나누어 진다.

802.11b MAC 프레임을 효율적으로 수집하기 위해서 BPF를 사용하는 pcap 라이브러리를 이용한다. 그 리고 802.11b MAC 프로토콜을 이용하는 모든 프레임을 수집하기 위해서는 무선랜 카드를 RFMON 모드로 전환을 하여야 한다. 무선랜 카드를 모니터링 모드로 전환한 후에는 다음과 같은 절차에 따라 무선랜의 인터페이스로부터 MAC 프레임을 획득한다.[2]

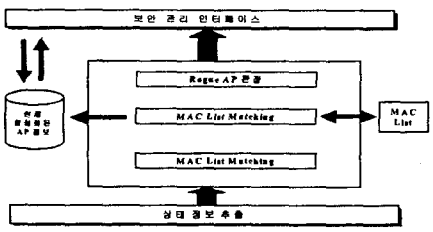
802.11b MAC 프레임을 수집한 후에는 정보를 추출하기 전에 버퍼링을 수행한다. 버퍼링 된 데이터는 액세스 포인트의 상태 정보, 보안 정보를 추출한다. 상태 정보는 현재 무선 네트워크에 존재하는 액세스 포인트와 스테이션의 정보를 나타낸다. 이것은 어떤 액세스 포인트와 어떤 스테이션의 연결 설정이 이루어져 있는지, 어떤 스테이션이 현재 연결되지 않고 존재하는지 파악할 수 있다.

액세스 포인트에 대한 정보는 Beacon 프레임과 Association Response 프레임을 통해서 획득할 수 있다. Beacon 프레임은 액세스 포인트가 스테이션에 접속 할 수 있도록 자신의 존재와 정보를 주기적으로 브로드 캐스팅하는 프레임이다. 그리고 Association Response 프레임은 인증된 스테이션이 액세스 포인트와의 연결 설정이 이루어질 때 액세스 포인트에서 스테이션으로 전달되는 프레임이

다. 이 두 프레임을 통해서 현재 액세스 포인트의 정보와 액세스 포인트와 연결되어 있는 스테이션의 정보를 확인할 수 있다.

스테이션이 액세스 포인트와 연결 설정에 관여 하는 프레임은 Probe Request 프레임, Authentication 프레임, Association Response 프레임이다. 이 가운데 Probe Request 프레임은 스테이션이 액세스 포인트와 연결을 이루기 전에 액세스 포인트를 확인하기 위해 이용된다. 따라서 , 이것은 스테이션의 존재를 확인할 수 있는 단서가 된다. [2]

Rogue AP 탐지 정보는 상태 정보로부터 Beacon 프레임에서 추출된 현재 액세스 포인트의 정보를 이용하게 된다. Beacon 프레임에는 현재 활성화 된 액세스 포인트의 세부 정보, 즉 SSID CHANNEL, ESS 모드, MAC 등의 정보가 포함되어 있다. 또한 액세스 포인트를 처음 사용할 경우 보안 관리자에게 액세스 포인트의 MAC, SSID 를 등록을 하게 되고, 이 등록된 액세스 포인트 리스트와 매칭을 통하여 Rogue AP 유무를 판별하게 된다. Beacon 프레임으로부터 받아온 액세스 포인트의 정보가 MAC 리스트와 일치한다면 , 인가된 액세스 포인트로 간주하고 DB에 로그를 저장한다. 만약, 그렇지 않을 경우 보안 관리 인터페이스로 보내어 관리자에게 보고 하게 되고, 세부 정보를 로깅하게 된다. (그림 2)는 Rogue AP탐지 모듈의 구조도 이다.



[그림 3] Rogue AP 탐지 모듈

3.3 Rogue AP 차단

본 시스템에서 라디우스 인증 서버로부터 네트워크를 사용하기 전에 액세스 포인트와 이동 단말기의 사용자에 대한 인증을 받게 된다. 일반적으로 라디우스 인증 서버는 client, client.conf, radiused.conf, users 이렇게 총 4가지의 설정 파일이 존재한다.

client - Radius 와 연동할 AP의 IP 주소와 secret 공개키를 설정

client.conf - client 등록 AP 와 동일한IP, secret 과 ssid에 해당하는 shortname 을 추가 등록,

radiused.conf - RADIUS 의 인증 방법, DB 연동 등 대부분의 설정이 여기에서 이루어지며, TLS을 지원하기 위해서 TLS 해당 부분의 주석을 풀고 인증서가 위치한 부분의 경로와 일치.

Users - 실제 인증하게 될 이동 단말 사용자들을 등록

위의 4가지의 파일중 client, client.conf, users 들은 실제 액세스 포인트와 이동 단말 사용자들의 인증에 관여 하는 파일이다[4]. 특히 client 와 client.conf 실제 사용하고자 하는 액세스 포인트의 정보를 담고 있고, users는 실제 사용하고자 하는 이동 단말기들의 정보가 담겨 져 있다. 액세스 포인트와 이동 단말기를 처음 사용하고자 할 경우 보안 관리 인터페이스로부터 등록을 받고 등록된 정보는 라디우스 인증서버로 보내어 지게 된다. 이러한 정보들은 인증 서버의client ,client.conf,users 파일에 저장 되고 , 노드들을 인증하게 된다. 인증되지 않은 액세스 포인트는 위장 액세스 포인트 간주되고 차단된다.

4. 결론

무선랜 환경에서 보안 문제에 대한 많은 연구가 진행되고 있다. 그러나 시스템 차원에서 이루어지는 보안 문제에 대해서는 연구가 아직 미비한 실정이다. 특히 Rogue AP 공격을 통한 내부망의 침투는 많은 심각한 문제를 안고 있다. 따라서 본 논문에서는 무선 구간 모니터링 에이전트를 통하여 실시간 모니터링을 하여 , 현재 활성화 되어 있는 액세스 포인트들의 상태 정보와 Rogue AP를 탐지한다. 또한 라디우스 인증 서버를 이용하여 Rogue AP의 네트워크 사용을 차단하는 시스템을 제안하였다. 무선 구간 모니터링 에이전트는 현재 활성화되어 있는 액세스 포인트의 정보를 파악할 수 있고, 그 상태를 분석 할 수 있게 된다. 또한 위장 액세스 포인트를 탐지 할 수 있게 된다. 더욱이 현재 많이 사용하고 있는 라디우스 인증서버를 사용하여 Rogue AP의 네트워크 접근을 원천 봉쇄하게 된다.

참고 문헌

[1] http://news.empas.com/show.tsp/20030708n01065/?s =1133&e=1310

[2] 김동필, 백병욱, 김상욱," 무선랜 보안 관리를 위한 정보 수집 에이전트 설계 및 구현", 한국 정보보호학회 동계학술대회논문집 Vol.13,No.2, 2003,pp 585-590

[3] Keung Hee Oh's Access Control of Wireless LAN Access Point Based on IEEE 802.1X 2002 CISC

[4] C.Ringney,A Rubens,W. Simpson,s. Willens, RFC 2058 Remote Authentication Dial In User Service(RADIUS) January 1997