무선 네트워크 모니터링 및 통합 관리 시스템

김동필°**, 백병욱*, 김상욱*
*경북대학교 컴퓨터과학과
**경북대학교 정보보호학과
{dpkim°, bwback, swkim}@woorisol.knu.ac.kr

A Wireless Network Monitoring and Integrated Management System

D. Kim°**, B. Back*, S.Kim*
Computer Science Department, Kyungbook National University

요 약

최근 고속 무선 네트워크에 대한 사용자의 요구가 증가함에 따라, 낮은 전송속도를 가지는 이동통신 시스템의 대안으로 무선 네트워크 시스템이 부각되고 있다. 무선 네트워크 기술의 보안 취약점은 무선 네트워크 사용의 중요한 장애 요인이다. IEEE 802.1x, IEEE 802.11i에서는 인증과 데이터 프라이버시 제공을 위한 표준을 내고 있으나, 무선 네트워크 보안을 완벽하게 지원하지는 않는다. 본 논문에서는 무선 네트워크 환경의 트래픽을 모니터링하고, 통합 관리 서버를 통하여 여러 무선 네트워크를 통합적으로 관리하는 시스템을 설계하고 구현한다.

1. 서 론

본 논문은 무선 네트워크에 존재하는 이동 단말기의 정보를 모니터링하고, 통합 관리하는 시스템에 대하여 기술한다. 무선 네트워크 기술의 주요 쟁점은 전송속도와 보안에 있는데 특히 보안 문제는 무선 네트워크 기술의 보급과 사용에 커다란 장애요소이다. 무선 네트워크의 데이터는 전파를 통하여 브로드 캐스팅되므로 네트워크 도메인안에 있는 모든 단말기에 전달된다. 이것은 무선 네트워크 환경이 보안에 매우 취약하다는 것을 의미한다.

보안에 대한 이러한 문제를 해결하기 위하여 IEEE 802.1x 태스크 그룹에서는 포트 기반의 네트워크 접근 제어(Port-based Network Access Control)를 표준으로 발표하였다. 이것은 언컨트롤 포트(uncontrolled port)를 통하여 인증된 사용자만 컨트롤 포트(controlled port)를 통하여 서비스를 이용할 수 있는 개념이다. 그리고 802.11i 에서는 데이터 프라이버시를 위하여 TKIP, AES 등의 암호화 기술에 대한 표준화 논의가 활발히 진행되고 있다[1,2].

그러나 무선 네트워크 환경에서 802.1x, 802.11i는 결국 유선 수준의 보안성을 제공해 줄 뿐, 위장 액세스포인트(Rogue AP), 세션 하이잭킹, DOS 등의 공격에 대한 완벽한 보안성을 제공하지 못한다. 또한 유선 환경에서는 각 호스트가 일정하게 존재하지만, 무선 네트워크에서는 단말기가 수시로 변경될 수 있다.

그러므로 본 논문에서는 중앙의 통합 관리 서버를 통하여 여러 무선 네트워크에 존재하는 이동 단말기의 상태를 모니터링함으로써, 위장 액세스포인트의 설정 및 공격에 대한 징후를 탐지, 차단하는 관리 시스템에 대하여 설명한다.

제 2절에서는 무선 네트워크 보안에서의 고려사항에 대해 설명하고, 제3절에서는 모니터링 및 통합 관리 시스템을 설명한다. 제 4절에서는 결론과 향후 연구방향에 대하여 언급한다.

2. 무선 네트워크 보안에서의 고려사항

무선 네트워크의 보안은 802.1x나 802.11i 등의 표준 기술을 단일하게 적용하는 것으로 이루어지는 것이 아니며, 각 공격의 유형에 따라 여러 단계에서 대응방안을 모색하는 것이 필요하다. 이 절에서는 무선 네트워크에 존재하는 공격의 유형과 대응을 위한 보안 기술을 기술한다.

2.1 무선 네트워크의 취약성

▪ 스니핑(sniffing), 가로채기 및 도청

무선 네트워크에서 모든 패킷들은 공중으로 브로드 캐스트된다. 만약, 이러한 패킷들이 802.11에서 제공되는 WEP(Wired Equivalent Privacy) 프로토콜을 이용하지 않는다면, 공격자에 의하여 도청될 수 있다. 또한 WEP를 사용하더라도 적은 키 사이즈로 인해 Airsnort, WEPCrack 등의 툴을 통하여 해독이 가능하다.[3]

▪ 위장 액세스 포인트(Rogue AP)

공격자는 기존의 여러 스니핑 도구를 사용하여 유선 네트워크와 무선 네트워크 사이의 브리지 역할을 하는 액세스 포인트의 MAC/IP를 스니핑하여 위장 액세스 포인트를 설정할 수 있다. 위장 액세스 포인트는 인가된 이동 단말기들의 정보를 가로채어 인가된 단말기로 위장할 수 있다. 이러한 위장 액세스 포인트는 중간자 공격

(Man-In-the-Middle)과 세션 하이잭킹(Session-Hi-jacking)에 이용된다.

▪ 서비스 거부 공격(DOS)

무선 네트워크에서 존재하는 DOS 공격에는 여러 가지 유형이 있다. 일반적으로 네트워크를 이용하고 있는 단말기에 디스어소시에이션(disassociation) 메시지를 주기적으로 전송해서 합법적인 단말이 서비스를 이용할 수 없도록 한다. 또는 액세스 포인트가 수용할 수 없을 정도의 어소시에이션(association) 메시지를 보내어 액세스 포인트의 동작을 방해함으로써 합법적인 사용자의 네트워크 이용을 어렵게 한다.[4]

2.2 무선 네트워크 보안 기술

무선 네트워크는 표준 보안 기술에 따른 단일한 보안 기술보다는 여러 단계에서의 보안 기술이 요구된다. 다음은 각 단계에서 해 줄 수 있는 보안 기술을 설명한다.

▪ 액세스 포인트

가장 기본적인 보안 단계로써 모든 액세스 포인트는 인가된 MAC 주소를 사용하는 이동 단말기들만이 액세스 포인트와 네트워크를 사용할 수 있는 협상을 한다. 이러한 기능은 소규모의 무선 네트워크에서는 유용하지만, 대규모의 무선 네트워크를 사용하는 지역에서는 MAC 주소의 변조나 위조 같은 문제로 보안에 취약점을 가지고 있다. 그러나, 액세스 포인트 단계에서 MAC 주소를 필터링할 수 있는 기능을 가지도록 하여야 한다.

▪ 네트워크 상태 감시

무선 네트워크에서 무선 구간은 데이터의 공개성과 단말기의 이동성으로 인하여 해킹의 위험성이 크다. 액세스 포인트는 SSID를 공중망으로 브로드캐스팅하고, 무선랜 카드에 입력되어 있는 MAC 주소는 ad hoc 네트워크 방식을 통하여 위조되어 질 수 있다. 따라서 실시간으로 네트워크의 상태 모니터링을 통하여 감시하여야 한다.

▪ 인증과 데이터 프라이버시

MAC 기반의 접근 통제에 대한 보안 취약성으로 인하여 IEEE 802.1x 포트 기반의 네트워크 접근 제어와 IEEE 802.11i의 무선 네트워크 보안 표준에 따른 보안 기술이 적용되어야 한다. IEEE 802.1x는 EAP 프로토콜을 이용하여 third-party의 RADIUS서버를 통하여 인증된 단말에만 네트워크 자원에 대한 접근제어를 할 수 있다. 802.11i는 MAC Layer에서 데이터 프라이버시를 제공하기 위하여 암호화에 이용되는 보안 표준이다.[1,2,6]

▪ 침입 탐지

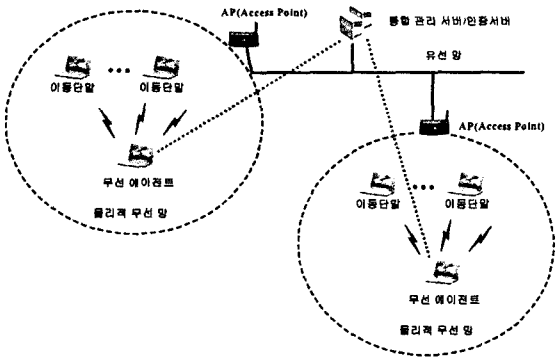
중간자 공격이나 세션 하이잭킹에 이용될 수 있는 위장 액세스 포인트를 탐지하여 공격의 징후를 판단한다. 또는 어소시에이션(association) 패킷이 필요 이상으로 발생하는 것과 같은 공격의 징후를 네트워크 모니터링을 통하여 파악한다

3. 무선 네트워크 모니터링 및 통합 관리 시스템

무선 네트워크 모니터링 및 통합 관리 시스템은 제 2절에서 설명한 단계별 접근 중에서 네트워크 상태 감시와 침입 탐지가 중심이다. 또한 액세스 포인트를 중심으로 이루어진 소규모 무선 네트워크를 통합된 서버에서 관리할 수 있도록 한다.

3.1 전체 환경과 구성

무선 네트워크 모니터링 및 통합 관리 시스템은 무선 구간에 존재하는 각 노드들의 정보를 중앙 집중화된 서버에서 통합 관리한다. 또한 액세스 포인트를 중심으로 이루어지는 소규모 무선 네트워크 환경을 실시간으로 모니터링하여 무선 구간에서 이루어지는 불법적인 행위를 차단한다. [그림 1]은 본 논문에서 제안하는 무선 네트워크 모니터링 및 통합 관리 시스템의 전체 구성이다.



[그림 1] 무선 네트워크 모니터링 및 통합 관리 시스템 개요

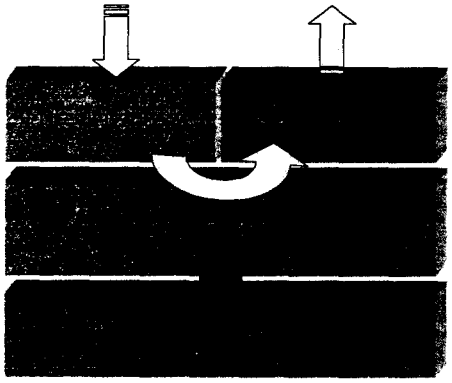
[그림 1]에서 무선 에이전트는 액세스 포인트를 중심으로 이루어지는 물리적인 소규모 무선 네트워크에서 이동되는 모든 패킷들의 트래픽을 실시간으로 모니터링한다. 모니터링한 트래픽을 분석하여, 통합 서버에서 요청하는 자료에 대한 서비스를 제공한다.

3.2 무선 에이전트

무선 에이전트의 구조는 [그림 2]와 같다. 물리적 무선 네트워크의 트래픽을 수집하는 모듈, 수집된 트래픽을 통하여 침입의 징후를 탐지하는 모듈, 탐지된 결과나 현재 무선 네트워크의 상태를 통합 서버로 전송하는 모듈, 로깅과 데이터를 저장하는 모듈로 구분된다. 이 모듈은 다음과 같은 기능을 수행한다.

- 물리적 무선망의 트래픽을 수집
- 위장 액세스포인트와 같은 불법적인 사용을 탐지, 통합 서버에 경고하는 기능
- 현재 무선 네트워크에 이용되고 있는 액세스포인트,

무선 단말의 정보를 통합 서버에 알려주는 기능
- 로깅 기능
- 그 외, 통합 서버가 요청하는 트래픽 정보에 대한 서비스 기능

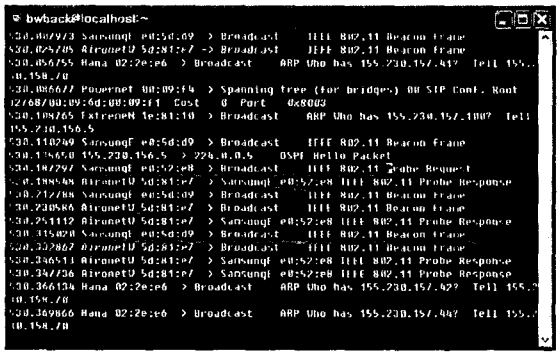


[그림 2] 무선 에이전트의 구조

위장 액세스포인트는 제 2 절에서 살펴본 바와 같이 무선 네트워크에 존재하는 단말로부터 네트워크 접속에 필요한 정보를 가로채는 기능을 가진다. 일반적으로 무선 네트워크에 존재하는 액세스 포인트는 고정적으로 운용되며, 단말 또한 액세스포인트보다는 유동적이나, 대체로 고정적으로 이용된다. 그러므로 통합 관리 서버에 무선 네트워크에서 가용한 이동 단말과 액세스포인트를 등록하고, 이 목록과의 비교를 통해 위장 액세스 포인트를 찾거나, ad-hoc으로 불법적인 기능을 수행하는 단말을 탐지한다.

무선 에이전트는 네트워크 인터페이스를 RFMON모드로 전환하여 물리적 영역에 존재하는 모든 트래픽을 모니터링할 수 있다. 이것은 실제 단말이 액세스 포인트에 접속할 때, 주고받는 Beacon 프레임, Probe Request, Probe Response 패킷까지도 포함한다. 이러한 raw 패킷을 통하여 단말이 이용하고 있는 자원, 상태, 액세스포인트와의 연결 상태 등의 자료를 수집할 수 있다.

[그림 3]은 Beacon 프레임과 Probe Request, Probe Response 패킷이 전달되는 모습을 보인다.



[그림 3] 무선 네트워크 raw 패킷 화면

3.3 통합 관리 서버

통합 관리 서버는 RADIUS 인증서버와 동시에 운용된다. 인증과 데이터 프라이버시를 위해서는 RADIUS 인증서버를 이용하고, 실제 통합 관리서버는 여러 무선 에이전트로부터 필요한 정보를 수집하고, 필요한 조치를 수행한다. 통합 관리 서버는 다음과 같은 기능을 가진다.

- 각 무선 에이전트별로 존재하는 무선 단말에 대한 모니터링 기능
- 특정 시간 내의 무선 네트워크의 트래픽 디스플레이 기능
- 무선 에이전트의 경고 메시지를 받으면, 관리자에게 전달하는 기능
- 위장 액세스포인트나 DOS 공격과 같은 공격에 대한 차단 기능

무선 에이전트로부터 전송받은 데이터나 경고를 바탕으로 통합 관리 서버는 이용되고 있는 액세스포인트에 필요한 정책을 적용할 수 있다. 특정 단말의 접근 차단이나, 특정 패킷을 누락시키는 등의 조치를 해당 액세스 포인트에 전달함으로써 여러 무선네트워크를 통합적으로 관리한다.

5. 결론

본 논문에서는 무선 네트워크에서 발생할 수 있는 보안적 문제를 통합적으로 관리하고 모니터링할 수 있는 시스템에 대한 모델을 제시하였다.

이 시스템은 IEEE에서 제시하는 보안 표준기술과 함께 액세스 포인트와 이동 단말기 사이의 무선 구간에 대한 통합적인 보안 기술을 제공해 줄 수 있다.

참고 문헌

[1] IEEE Std 802.1x, "Port-based Network Access Control," 2001

[2] IEEE Std 802.11i/D2.0, "Draft Supplement to STANDARD FOR Telecommunications and Information Exchange Between System-LAN/MAN Specific Requirements - Part11:Wireless Medium Access Control and physical layer specifications : Specification for Enhanced Security," March 2002

[3] B. Christian, B. Tony, O. Eric and P. Jeffrey, HACK PROOFING YOUR WIRELESS NETWORK, SYNGRESS, 2002

[4] Aranesh Mishra and William A. Arbaugh, "An Initial Security of the IEEE 802.1x Standard", 6 Feb 2002

[5] IEEE. Lan man standard of the ieee computer society. wireless Lan medium access control (mac) and physical layer(phy) specification. IEEE Standard 802.11, 1997

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