무선망 위협 관리 시스템(W-TMS : Wireless Threat Management System) 설계에 관한 연구

서종원, 이형우
한신대학교 소프트웨어학과
seo0207@hs.ac.kr, hwlee@hs.ac.kr

Design of Wireless Threat Management System

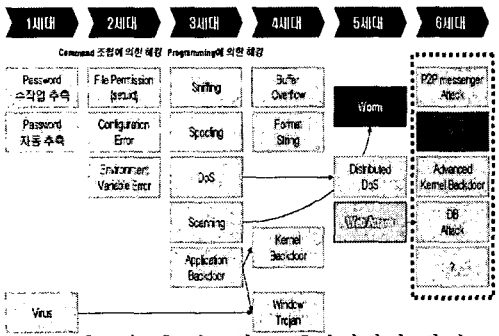
Jong-Won Seo, Hyung-Woo Lee
Div. of Com., Info., and Software, Hanshin University

요 약

무선 네트워크의 가장 큰 이점은 이동성에 있다. 따라서 사용자들은 네트워크에 접속하면서 자유롭게 로밍(이동)할 수 있다. 그 이동성의 전제는 물리적인 매체 없이 네트워크에 접속이 가능하다는 것이다. 그러나 이러한 이점에도 불구하고 유선 네트워크에서의 기초적인 물리적 보안기반 구조를 무선 네트워크에서는 제공하고 있지 않다는 것이다. 하지만 무선 네트워크가 기존 유선 네트워크에 비해 대역폭이 적다는 이유로 성능감소를 우려하는 사용자들은 보안 알고리즘 적용을 꺼려왔고 쉽게 해킹의 대상이 되어 왔다. 이에 본 논문에서는 특정 네트워크에 국한되지 않으면서도 유연성을 제공하는 W-TMS(Wireless Threat Management System) 시스템을 설계하여 기존 무선 네트워크 환경에서 보안 취약성을 보완하면서 안전성을 강화할 수 있는 무선망 보안 시스템을 제안한다.

1. 서론

지난 10년 동안 인터넷은 빠른 속도로 모든 분야에 확산되어 왔으며 이와 비슷한 현상으로 최근 몇 년 동안 무선 네트워크의 확산 역시 빠른 속도로 보급되고 있는 추세이다. 그러나 처음 무선 네트워크가 상업적으로 이용되면서 사람들은 보안에 대해 크게 신경을 쓰지 않은 상태에서 네트워크를 구축하였다.



[그림 1] 네트워크 공격기법의 발전

그 결과 무선 네트워크 침입의 형태와 기술은 시간과 비례하여 그 다양성이 점차 증가되고 있으며 공격 시도 및 침입에 성공하는 공격의 횟수도 증가하고 있다.

[그림1]에서 보면 현재 네트워크 공격 기법은 5세대와 6세대의 중간 시점에 와있다. 6세대의 네트워크 공격기법 중에 본 연구에서는 Wireless Attack에 중점을 두고 무선 공격에 대응 할 수 있는 무선망 위협 관리 시스템을 제안한다.

2. 관련 연구

2.1 무선 네트워크 공격기법

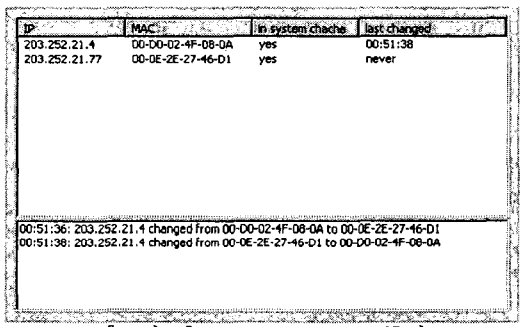
무선 네트워크 공격기법에는 스니핑(Sniffing)을 이용한 공격, 스프핑(Spoofing)을 이용한 공격, 서비스 거부(Denial of Service)공격등 여러 가지 공격기법이 있다.

2.1.1 스니핑(Sniffing)을 이용한 공격기법

이는 공격할 대상을 예비조사하고, 패스워드를 빼낼 수 있으며, 암호화되지 않은 데이터를 캡처하는데 사용된다. 대부분의 공격자들은 무선 네트워크 행위를 모니터링하기 위해서 스니핑 도구들을 사용하며, 네트워크를 모니터링 함으로써 스푸핑과 하이재킹, 플러딩과 같은 공격의 기초가 된다.

2.1.2 스푸핑(Spoofing)을 이용한 공격기법

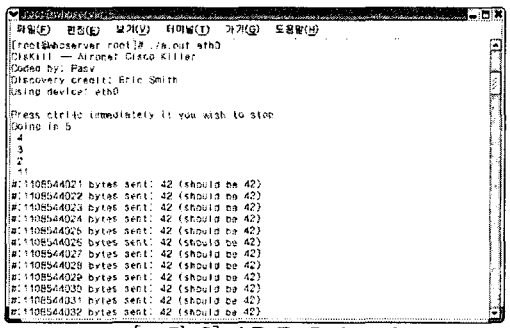
스푸핑 공격 [그림2]는 IP주소, 호스트 이름, MAC주소 등 여러 가지를 속일 수 있으며, 스푸핑은 이런 속임을 이용한 공격을 총칭한다.



[그림 2] MAC Spoofing 공격

2.1.3 서비스 거부(Denial of Service)공격

DoS공격[그림3]은 네트워크에서 사용가능한 자원을 모두 소모하게 하여 어떠한 접근도 할 수 없도록 네트워크를 마비시키는 공격이다. 예를 들자면, 무선 네트워크의 환경에서 여러 대의 장비들이 같은 주파수를 사용하려고 함으로 발생하는 주파수 충돌과 같은 것이 있다.

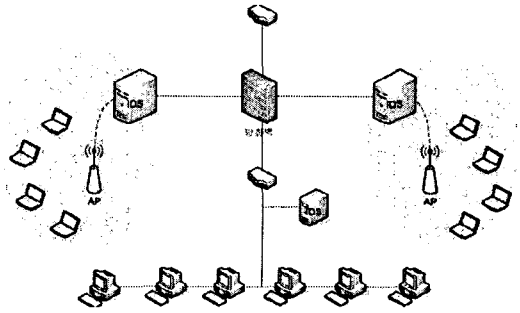


[그림 3] AP DoS Attack

2.2 Wireless-IDS

W-IDS 시스템[그림 4]의 특징은 컴퓨터 시스템과 네트워크 내의 여러 위치로부터 정보를 수집하여, 이들 중 보안 위반 징후와 관련된 정보를 분석하는 역할을 한다. 하지만 실시간으로 유입되는 패킷을 분석해야 하기 때문에 고성능의 처리능력을 필요로 하며, 저장의 한계를 극복해야 하고, 네트워크 트래픽 증가에 따른 별도의 하드웨어 및 소프트웨어가 필요하다. 또한 사고 대응 계획이 설계되고 기획되지 않으면, 보안성를 거의 제공하지 않는다. 그리고 이벤트를 감시하고 사고에 대응하기 위한 인적 요소 비용이 크게 소비된다.

이러한 문제점을 보완하기 위해 본 연구에서는 W-TMS을 제안한다.



[그림 4] 유무선-IDS구조도

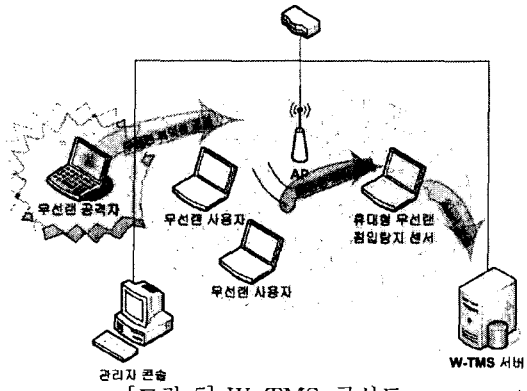
3. 제안한 W-TMS 시스템

위협관리시스템(TMS; Threat Management System)이란 바이러스, 해킹 등 아직 일어나지 않은 사이버 위협을 예측하고 기술과 정보를 상호 보완적으로 결합해 능동적으로 방어할 수 있는 시스템이다. 이처럼 TMS는 국내외 보안 트랜드, 네트워크 트래픽 및 공격 형태를 정밀하게 분석해 네트워크를 통한 사이버 공격에 대한 대응체계를 구축하고, 사이버 위협을 조기에 경보하고 피해를 최소화하기 위한 대응시스템이다.

TMS 시스템의 가장 큰 특징으로는 단순히 외부 위협의 통계를 보여주는 것이 아니라 이를 종합적으로 분석해 대응책을 마련할 수 있기 때문에 보다 효과적인 보안 대응이 가능하다는 점이다.

따라서 TMS 시스템에서는 각종 위협 및 공격에

대해 맞춤형 경고를 제공 할 수 있다.

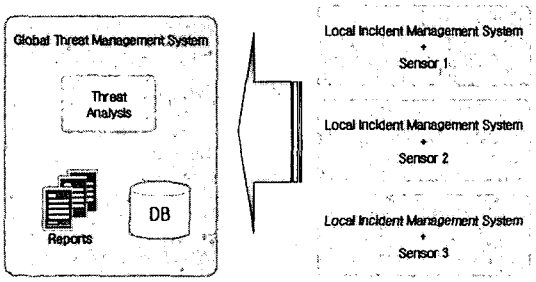


[그림 5] W-TMS 구성도

W-TMS의 특징은 W-IDS의 지역적인 무선망의 Incident 모니터링에서 벗어나 휴대형 무선 랜 침입탐지 센서를 이용해 전역적으로 모든 무선망의 Incident들을 취합하여 예측된 위협을 효과적으로 사전에 방어함으로써 보호해야할 무선망에 가해지는 공격으로부터 충격을 완화시키고 가용성의 본질을 훼손되지 않게 하는 것이 특징이다.

3.1 핵심 모듈 구조

W-TMS는 예측성, 적시성, 신뢰성, 적합성에 맞게 구성되어야 한다. 따라서 위협관리 시스템은 외부로부터 가해질 다양한 형태의 공격 등 위협에 관한 국내외 각종 정보들과 실제 위협관리 시스템의 보호대상 인프라에 미치는 영향을 토대로 상호연관성 분석 기법을 적용하여 현재 그리고 앞으로 다가올 위협을 예측할 수 있어야 한다. 이를 위해 본 연구에서는 아래와 같은 W-TMS 핵심 모듈 구조를 제안한다.



[그림 6] W-TMS 시스템 구조

3.1.1 Global Threat Management System

Global Threat Management System은 잠재적인 위협, 활성화된 위협, 상승하는 위협, 감소하는 위협 등으로 분류해 단계별로 적절한 대응에 필요한 의사결정을 지원하기 위해 기술과 정보를 제공하는 역할을 담당한다.

Global Threat Management System의 모듈 구조는 Threat Analysis, Reports, DB로 구성되어 있다.

Threat Analysis는 휴대형 무선 침입 탐지 센서로부터 보내어진 이상 트래픽 정보를 분석하여 TMS 관리자 콘솔로 Alert를 전송한다.

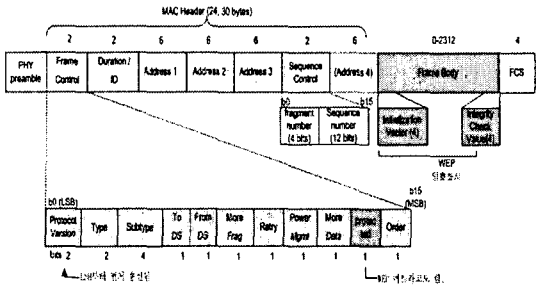
Report는 TMS 관리자 콘솔로부터 Report 생성 요청을 받을시 Threat Analysis에 의해 분석된 정보를 가지고 TMS 관리자 콘솔에서 원하는 정보를 생성한다.

DB는 휴대형 무선 침입 탐지 센서로부터 이상 트래픽에 대한 데이터를 저장한다.

3.1.1 Local Incident Management System

W-TMS는 잠재적인 위협이나 활성화된 위협을 인식하는 것에서부터 시작한다. 동일한 무선 위협으로 인해 다양한 환경에서 동일한 위험(Risk)을 갖는 것은 아니지만 Local Incident Management System는 다양한 무선 환경에서의 위협을 탐지해 다가올 위협 또는 잠재적인 위협, 새롭게 활성화된 위협, 상승하는 위협, 감소하는 위협 등으로 위협을 분류하고, 위협의 위험도(Severity), 영향도(Impact)등에 따라 현재 상황에서 집중 처리해야할 위협들을 결정하고, 분석할 수 있는 데이터를 제공한다.

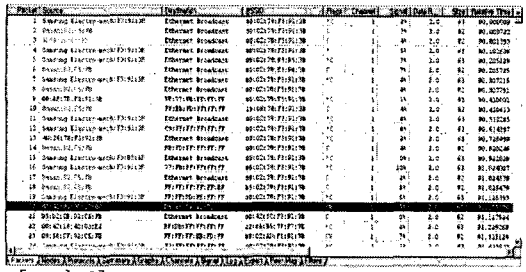
다음은 [그림 7]은 IEEE 802.11 무선 LAN MAC 프레임의 기본 형식이다.



[그림 7] IEEE 802.11 무선 LAN MAC 프레임의 기본 형식

각 프레임은 2바이트 길이의 프레임제어 영역으로부터 시작한다. 그러므로 프레임제어 영역의 정

보를 캡처하여 무선데이터의 기본 정보 및 위협 여부를 파악 할 수 있는 가공된 데이터를 만들 수 있고 그 정보는 소프트웨어 적으로 구현된 Local Incident Management System에 의해 모니터링 되고 Golbal Threat Management System으로 전송되어 진다.



[그림 8] IEEE 802.11 Beacons, Data, Management 프레임 모니터링 프로토타입

3.2 시스템 개발 환경

3.1.1 Global Threat Management System 개발 환경

개발 환경	개발 도구
운영 체제	Windows 2003
개발 언어	.NET C#
Database	MS SQL Server 2005
리포팅	Crystal Report

[표 1] Global Threat Management System 개발 환경

3.1.2 Local Incident Management System 개발 환경

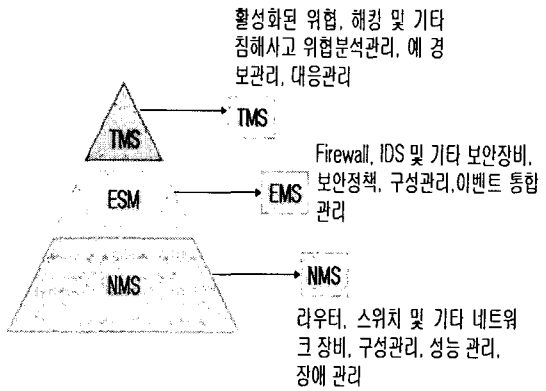
개발 환경	개발 도구	
운영 체제	Windows XP	
개발 언어	C++	
무선랜 카드	무선 랜카드 종류	Atheros Chipset(PCMCIA type)
	디비이스 드라이버	The WildPackets Atheros Wireless Driver v4.2
	지원하는 하드웨어 리스트	http://www.wildpackets.com/support/product_support/airopeek/hardware

[표 1] Local Incident Management System 개발 환경

4. 결 론

본 연구에서 제시한 W-TMS는 보안을 위한 새로운 방향성을 가지고 접근한다. 첫째는 기술과 정보를 융합시켜 단위 솔루션이 갖는 한계를 극복하는 것이고, 둘째는 관리의 방향이 무선망이 아닌 무선망의 위협으로 보다 능동적인 방향을 향하고 있다.

W-TMS는 필요에 따라 자동화되고 능동적인 대응 수단을 제공하기도 하지만, 많은 제로 데이 위협의 경우 사람이 막아야 하는 현실을 고려하고 있다. 또한 W-TMS의 관리 대상은 위협 그 자체로, 무선망 자신이나 보안 시스템으로 보는 NMS나 EMS와 분명히 다른 방향성을 가지고 있다.



[그림 9] NMS, ESM과 TMS

그러므로 전역적으로 무선 트래픽을 탐지 할 수 있는 W-TMS와 기존의 보안 시스템과의 상호 보완적인 구축으로 더욱더 강력한 무선 보안 환경을 구축 할 수 있게 되었다.

참 고 문 헌

[1] Jay Beale, "스노트 2.0 마술 상자" chapter 1 침입 탐지 시스템, 2003

[2] 김동욱, "위협관리, 보안의 새로운 방향 제시" 정보보호 기술 연구소장

[3] Kevin Beaver, Peter T.Davis "Hacking Wireless Networks For DUMMIES"

[4] Symantec DeepSight Threat Management System

[5] www.airopeek.com

[6] www.securityfocus.com