무선 랜 환경에서의 비정상 트래픽 차단기법에 관한 연구

서종원, 최창원, 이형우
한신대학교 컴퓨터정보소프트웨어학부
seo0207@hs.ac.kr, won@hs.ac.kr, hwlee@hs.ac.kr

A Study on Anomaly Traffic Detection & Prevention Schemes in Wireless LAN

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

요 약

인터넷 사용자들의 무선 네트워크의 활용빈도가 점차 높아지고 무선 네트워크의 보안시스템도 요구되면서 무선 네트워크의 안정적이고 원활한 활용과 사용자의 정보 노출의 위험을 줄이고자 유무선 통합형 IDS/IPS도 개발되고 있는 단계다. 본 논문에서는 무선랜 환경을 지원하는 유무선 IPS시스템을 구현하고, 비정상적인 트래픽 탐지의 효율성을 높여 IPS 시스템의 성능향상에 기여정도를 파악 및 분석하였다. 본 논문에서 구축한 IPS시스템은 하이브리드 형태로 구현하였으며 Snort-inline[11]과 Snort-wireless[12] 모듈을 사용하여 무선 랜 이상탐지 기능을 구현하였다. 네트워크 모니터링 시스템으로 네트워크의 트래픽 상황을 파악하여 비정상적인 트래픽이 증가되었을 경우, 제안한 IPS시스템에서 비정상 트래픽의 탐지 및 차단 기능을 기존 IPS와 성능을 비교/분석하였다.[1)]

I. 서론

인터넷의 발전과 보급이 급속도로 활성화되면서 네트워크를 통한 공격과 침입은 더욱 빠른 속도로 지능화되어 이루어지고 있다. 인터넷 사용의 쉬움과 편리함을 이용하여 개인 혹은 기업의 컴퓨터에 불법적인 침입으로 정보를 빼내어가거나, 각종 웜들의 전파를 통하여 정상적인 인터넷 사용자들과 인터넷 서비스를 제공하는 서버나 전체 네트워크를 마비시키는 경우가 빈번하게 발생되면서 사이버 범죄의 발전을 초래하였다. MS사의 Windows Server들을 공격한 코드레드 웜이나, 1.25대란의 주범이었던 SQL-Server의 보안상 허점을 이용한 웜, 그리고 NT계열의 Windows가 부팅 후 RPC오류로 인한 시스템 재부팅 등 보안상의 허점을 이용한 공격들을 예로 들 수 있다[1,2].

또한 네트워크의 공격들로 인한 피해는 점차적으로 증가하고 있다. 그림을 통해 나타난 공격들은 현재 대부분 패치가 되어있지만, 어떤 방법으로 어느 곳에서 변형된 웜이나 바이러스성 코드들이 다시 발생할지는 모르는 일이다. 그렇기 때문에 개인의 정보보호 및 단체의 보안을 위한 네트워크의 보호와 침입에 대한 즉각적인 대처가 필요하다. 이러한 현실에 능동적인 대처를 위해 개발된 것이 침입방지 시스템(Intrusion Prevention System)이다[3,4].

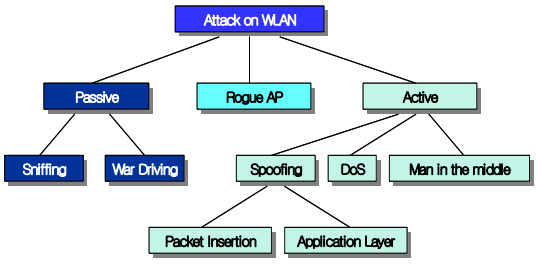
본 연구에서는 Rule기반의 침입방지 시스템의 Snort inline을 이용한 침입 탐지 및 차단 시스템을 구현하였고, Snort[11]와 패킷 분석 툴, 모니터링 툴을 이용하여 유무선 네트워크의 트래픽 관리와 비정상적인 트래픽의 분석을 실시하였다. 무선의 환경을 지원하기 위해 Sonrt-Wireless의 Snort 패치를 통하여 인라인 모드로 구현하였다. 네트워크의 모니터링을 위한 툴은 Ntop를 사용하였으며, 분석과 관리를 위한 툴로 ACID를 사용하였다. 비정상행위의 탐지는 규칙기반 접근법을 이용하여 일정한 정해진 패턴을 벗어난 행위를 탐지하고, 모니터링 하여 차단 여부를 결정하는 요인이 되도록 한다.

1) 본 연구는 정보통신부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2005-(C1090-0502-0020))

II. 무선 네트워크 취약점

1. 무선 네트워크 공격 및 대응

악의적인 사용자들에 의해서 사이버 공격 기법은 날로 다양해고 있으며, 해킹 기법의 발달로 자동화, 지능화 된 해킹 툴이 공개적으로 유포되어 국내외 해킹 발생빈도는 급격히 증가하고 있는 추세이다. 특히 네트워크의 취약점이 지속적으로 증가하고 있으며 웜바이러스와 같은 치명적인 공격에 의해 네트워크 서비스를 마비시킬 수 있는 DDoS 공격이 급증하고 있는 가운데 무선 네트워크상에서의 무선 랜 공격은 아래 그림과 같이 passive, active, rogue AP 공격으로 분류할 수 있다[5,6].



[그림 1] 무선랜 공격 유형

2. 대응방법 : Wireless IDS/IPS

현재 Wireless IDS/IPS 기능을 제공하기 위해 수행된 연구 결과는 AirMagnet, AirDefense 등이 있다. Airmagnet 센서는 SQL DB를 기반으로 WLAN 관리 및 모니터링 기능을 수행한다. Rogue AP 탐지 및 추적 기능을 제공하며 DoS 공격에 대한 대응을 통해 무선 네트워크에 대한 안전성 확보를 목적으로 하고 있다.

AirDefense 시스템은 wireless AP 센서와 자바 기반 웹 콘솔 시스템으로 구성된 Red Hat 리눅스 서버로 구성되어 있다. AirDefense 웹 콘솔과 AP 센서는 서버와 안전한 무선 통신을 통해 트래픽에 대한 관리 및 차단 기능을 수행한다. AirDefense에서 제시하는 Wireless IPS는 정책 기반 IDS/IPS 시스템으로 네트워크에 대한 관리, 성능 및 안전성을 설정하며 WLAN 세션에 대한 보안 기능을 제공한다. 또한 일반적으로 리눅스 운영체제를 기반으로 공개 소프트웨어 형태로 개발되어 현재 활발한 연구가 진행되고 있으며 현재 Snort-Wireless[12] 및 WIDZ와 같은 코드가 제시되고 있다[8,9].

III. 제안한 시스템

1. 본 연구에서의 접근방법

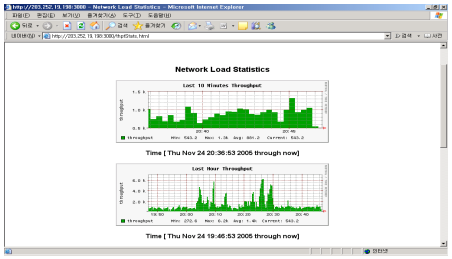
네트워크의 트래픽의 증가는 관리자에게 두 가지의 원인을 생각하게 한다. 첫 번째는 네트워크의 사용자가 많이 증가하여 트래픽이 증가했을 수도 있을 것이고, 또는 네트워크 정보의 유출이나 침입을 위한 고의적이고 불법적인 접근으로 인해 트래픽이 증가하는 경우도 있을 것이다[3,4].

본 논문에서 제안하는 시스템은 이러한 네트워크의 트래픽을 기반으로 비정상적인 트래픽의 발생은 침입이라고 가정하고 비정상적인 트래픽이 발생하였을 경우, 네트워크의 패킷을 분석하여 공통된 공격의 signature를 찾아내고 새로운 룰을 적용함으로써 네트워크의 이상행위를 탐지하고 차단할 수 있는 시스템을 제안하였다.

본 장에서는 기존의 IPS 시스템의 성능을 보완하여 유선 네트워크의 시스템에 무선 랜 환경을 지원하도록 하고, 무선네트워크의 트래픽을 중심적으로 관찰하며 네트워크 트래픽의 관찰로 비정상적인 트래픽이 발생하였을 경우의 대처방안을 모색하고자 한다. 기존의 rule기반의 탐지방식과 함께 비정상 행위 탐지방법으로 새로운 rule을 발견하고 적용함으로써 향상된 시스템을 구현한다.

2. 비정상 행위 탐지 기법의 분석

본 연구에서의 비정상 행위 탐지 기법은 네트워크 트래픽으로부터 비정상 행위를 탐지하는 기법으로, 우선 모니터링하는 트래픽이 일정한 수치를 초과하게 될 경우를 침입으로 가정한다는 조건을 전제로 하여 비정상적인 트래픽의 사용을 침입이라고 판단한다. 이상의 조건 하에서 네트워크 트래픽의 실시간 모니터링을 하며 네트워크의 패킷들을 database에 저장한다. 해당 네트워크의 트래픽이 과도하게 사용될 경우는 사용 시점부터 저장된 데이터를 분석하게 되고, 패킷으로부터 공통적인 signature를 탐지하게 된다. [그림 3]은 Ntop[10]을 사용하여 네트워크의 트래픽을 모니터링하는 경우의 한 화면이다. 아래 그림과 같이 시간의 변화에 따라 네트워크의 사용량도 불규칙적으로 변화한다.



[그림 2] Ntop을 이용한 네트워크 트래픽 현황

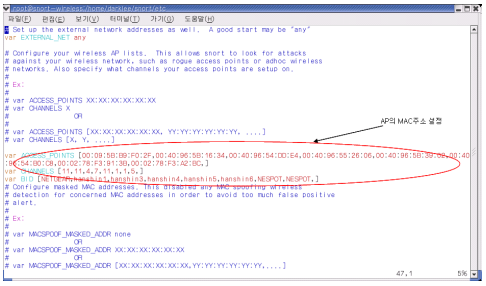
이상 트래픽이 지속적으로 발생한다면, 공격 패킷의 가능성이 크기 때문에 네트워크 분석툴인 ACID를 이용하여 해당 시간대의 패킷을 분석하고, 해당 패킷으로부터의 컨텐츠 정보를 통해 새로운 공격의 정보를 등록시키게 된다. ACID를 이용하여 공격 정보에 대한 침입 signature와 네트워크의 침입이 이루어진 시간대를 분석하게 되며, 이와 같은 과정을 통해 탐지된 침입으로부터 규칙을 발견하여 엔진의 Rule에 추가한다.

3. 무선 트래픽 침입탐지

무선 네트워크 기반 무선 랜 환경에서의 침입행위를 탐지하는 방법을 알아보도록 한다. 무선에서 가능한 침입을 전처리단계에서 모듈화 하여 처리하도록 하고, snort의 설정파일에서 해당 전처리기를 사용할 것인지의 여부를 사용자가 결정하도록 한다. 또한 사용자들을 엔진이 구동되기 이전에 등록하여 주어 거짓 경보 발생을 줄이도록 하였다. 무선 네트워크의 공격에 대한 전처리 모듈로는 rouge AP 전처리기, MAC spoof 전처리기, Auth-flood 전처리기, Deauth-flood 전처리기 등이 있고, 무선 네트워크의 sniffing으로 인한 공격을 방지하고자 netstumbler의 행위를 탐지하는 전처리기도 정의되어 있다.

이러한 전처리기의 설정은 snort를 설정하는 conf파일 내부에서 설정하게 된다. conf파일은 snort의 기본이 되는 설정파일로 내부/외부 네트워크의 정의와 탐지하게 될 rule들은 어떠한 것인지에 대한 내용과 사용될 전처리기의 정의부도 포함되어있다.

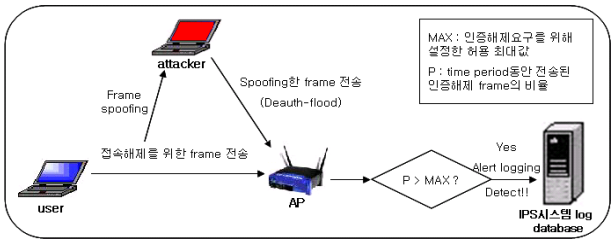
snort는 설정파일을 사용하여 서비스를 제공하게 될 AP의 MAC address를 conf 파일에 지정해주어 정해진 장비의 MAC이 아닌 다른 MAC을 갖는 AP는 rouge AP로 간주하고 전처리 단계에서 탐지하도록 되어있다. 무선 네트워크의 데이터들은 특정한 방향성을 갖고 움직이는 것이 아니라 무선 패킷을 공중에 뿌리고 신호를 감지한 장치만이 응답을 하게 되고, AP와 연결되어진 네트워크 인터페이스만이 통신을 하게 되기 때문이다.



[그림 3] 설정파일에서 허가된 AP를 등록

엔진과 연결이 되어있는 다른 네트워크를 통해서 AP가 설정될 수도 있지만 이러한 AP설정은 허가되지 않은 AP이기 때문에 rouge AP로 판단되어 snort에서 경고메시지와 함께 해당 AP의 접근을 허가하지 않게 된다.

인증과정을 이용한 공격방법도 마찬가지로 전처리기의 설정을 snort 설정파일에 미리 설정하게 된다. 인증된 사용자가 AP로 보내는 패킷을 스니핑하고, 패킷으로부터 인증자의 정보를 악용하여 AP에게 인증과 인증해제 요청을 과도하게 보내어 정식으로 인증된 사용자가 시스템에 접근하는 것을 거부하도록 하는 방법이 Auth flood / Deauth flood 공격 방법이다.



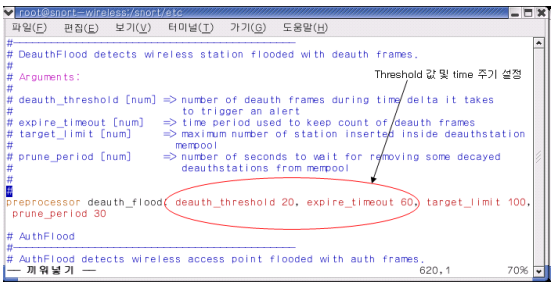
[그림 4] Deauth-flood detecting 과정

공격의 탐지 방법은 [그림 4]와 같다. 관리자가 설정한 threshold와 time period로 인증해제 요청의 MAX 수치를 정한다. 인증해제 요청이 있을 시에 미리 설정한 time period 동안 요청된 frame의 수의 비율을 P라 했을 때, P를 MAX값과 비교하여 MAX값을 넘어설 경우 공격으로 탐지하게 된다. 이를 수식으로 나타낸다면 아래와 같다.

$$P = \frac{\text{요청된 } frame\text{의 수}}{time\ period}$$

공격으로 탐지되면, 관리자에 의해 공격자의 MAC address와 IP address를 snort 설정 파일에 기록함으로써, 이후의 접근을 금지한다. auth-flood공격의 경우도 이와 유사한 방법으로 탐지하게 된다.

MAC spoof 공격은 이전에 설명한 바와 같이 자신의 MAC address를 숨기고 접근 허가된 사용자의 MAC address로 위조하여 자신의 정보를 감추고 네트워크에 접근하여 피해를 가하는 공격이다. MAC spoofing 공격은 실제 공격자의 정보는 알 수 없고 spoofing 당한 접속자의 정보는 알 수 있다. snort에서는 설정 파일에 rogue AP를 찾아내는 방법과 같이, 내부 네트워크의 각 interface를 등록하여 사용함으로써 MAC spoofing 공격을 탐지하고 차단한다.

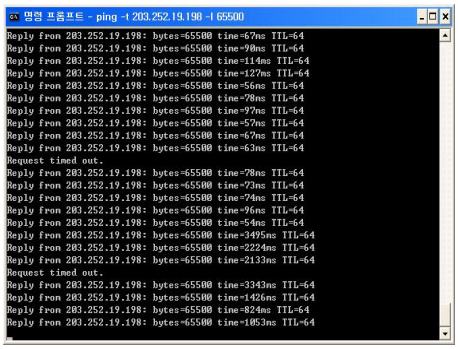


[그림 5] Deauth-flood 전처리기의 설정

이러한 방법은 무선 네트워크를 사용하고자하는 등록되지 않은 사용자들은 네트워크를 접근할 수 없게 되어, False positive를 줄일 수 있고 spoofing으로 인한 침입도 바로 알아낼 수 있다.

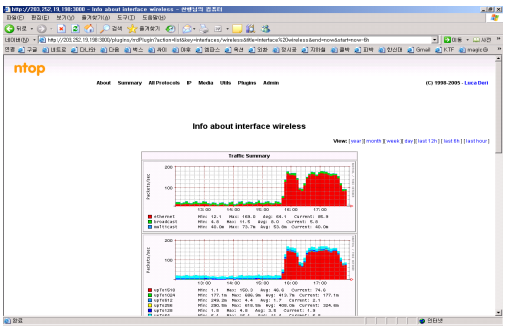
IV. 시스템 설계 및 구현

본 논문에서 제안한 시스템은 웹 브라우저를 이용하여 손쉽게 시스템에 접근할 수 있었으며, 발견한 규칙을 Rule로 추가하여 적용함으로써 새로운 경보를 통한 Rule의 적용이 가능하였다. 기존의 시스템에서는 모니터링과 관리를 위한 툴이 요구되었으나, 본 시스템은 웹 방식의 인증을 통해 시스템에 접근하여 네트워크의 트래픽 관리와 경고를 관리할 수 있었다. 또한 Snort의 Rule을 웹페이지로 관리한다는 점은 웹의 접속을 통한 편리한 사용을 말하며, 이는 다른 특별한 프로그램의 설치나 관리 프로그램이 없이도 사용할 수 있기 때문에 프로세스를 따로 차지하지 않아 시스템을 효율적으로 사용할 수 있도록 추가적인 역할을 한다. 본 시스템의 실험을 위해 시스템의 밑단의 네트워크로부터 해당 시스템으로의 네트워크 공격을 시도하였다.



[그림 6] 무선 어댑터를 이용한 ping test

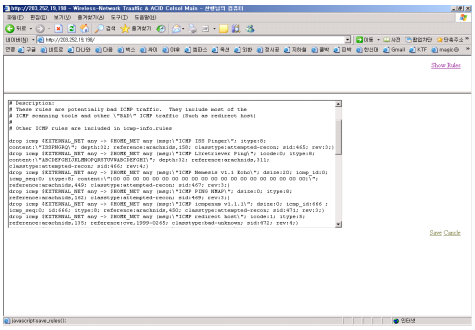
네트워크 공격의 경우, 교내의 방화벽과 기존의 침입차단 시스템으로 인해 실험이 가능하지 않아, 내부 네트워크로부터의 ping test를 공격으로 간주하여 진행 하였다. 무선 어댑터를 장치한 데스크탑과 노트북을 사용하여 진행하였으, ping test의 경우는 size를 기본적인 크기가 아닌 가능한 최대치로 설정하였으며, 이로 인해 네트워크의 트래픽의 증가를 확인할 수 있었고, 가끔 AP로부터의 접속이 끊기는 현상도 볼 수 있었다.



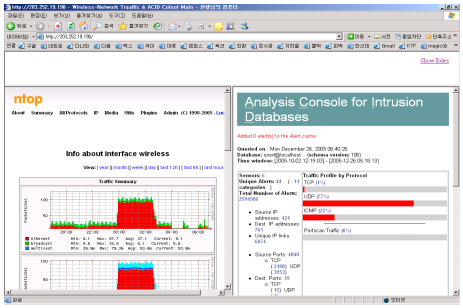
[그림 7] Ping Test후의 트래픽 증가

기존의 Rule파일 중에서 snort의 icmp와 관련된 rule의 헤더 부분을 alert을 모두 drop으로 하여 진행하였을 경우, 네

트워크의 트래픽은 기존의 상태로 되돌아가는 모습을 볼 수 있었으며, 웹상에서 즉시 Rule의 발견과 적용이 가능하게 되었다. 아래의 [그림 8]에서 보는 바와 같이 특정 Rule의 헤더를 변경하여 저장하게 된다. 이후에 시스템의 재가동을 통해서 [그림 9]와 같이 트래픽이 감소되어지는 것을 볼 수 있었다.



[그림 8] icmp.rule파일의 변경



[그림 9] 변경된 Rule의 적용 후 트래픽 감소

기존의 시스템은 유선의 환경에서 이미 잘 알려진 signature를 토대로 패턴매칭 기법을 이용하여 침입이나 공격의 패킷들을 탐지할 수 있었다. 알려진 공격들의 규칙성을 검증된 방법을 통해 rule로써 정형화하였으며, www.snort.org나 다른 snort와 관련된 사이트로부터 rule의 업데이트로 새로운 공격의 규칙들을 적용시킬 수 있었다. 즉, 알려진 행위에 대한 탐지와 차단은 가능하였으나, 알려지지 않은 행위에 대한 침입은 대응하지 못하였으며, 또한 무선 네트워크의 범람 공격에 대한 탐지는 유선 네트워크의 것과 비교하였을 때, 크게 다른 점은 찾을 수 없었다. 하지만 제안한 시스템의 경우는 트래픽을 유발시키는 알려지지 않은 침입을 ACID의 분석을 통해 탐지할 수 있었으며, 과도한 트래픽을 유발하는 패킷의 컨텐츠 정보를 추출하여 rule에 추가함으로써 알려지지 않은 트래픽을 증가시키는 침입도 탐지가 가능하였다. 또한 네트워크 트래픽 모니터링 시스템을 통해 과도한 트래픽이 발생하는 시간대별 분석이 가능하며, 시간별, 일별, 주간별, 월별로의 네트워크의 상황을 손쉽게 파악할 수 있어 현재의 네트워크의 성능을 평가하는 데에 기초적인 자료를 제공하여 줄 수 있었다.

기존에 알려진 툴의 사용으로 네트워크의 모니터링과 새로운 규칙의 발견이 가능하였으며, 네트워크 모니터링 서비스와 침입을 탐지하고 차단하는 시스템을 함께 사용하여 시스템에는 다소 과부하가 따를 수도 있으나 이는 시스템의 성능의 향상에 따른 충분히 발생될 수 문제점이라고 생각할 수 있다. 또한 유선의 네트워크와 무선의 네트워크를 함께 지원할 수 있으며, 무선 네트워크의 장점인 이동성과 확장성도 충분히 보장받을 수 있을 것이라고 판단하였다.

이와 같은 내용들을 기반으로 하여, 본 시스템과 기존 시스템의 차이점 비교를 아래의 [표 1]을 통해 간단하게 정리하였다.

[표 1] 기존 시스템과 제안한 시스템의 비교

구분	inline 기반 기존 시스템	snort-wireless기반의 제안 시스템
Base system	snort snort-inline	snort snort-wireless
네트워크 침입 탐지 방식	규칙기반(rule) 오용탐지	규칙기반(rule) 오용탐지 & Network traffic 기반 비정상행위 탐지
네트워크 구성	Inline 방식	Inline 방식
시스템 접근 방법	모니터 프로그램	web browser를 통한 접근 및 제어
rule기반의 침입 탐지 및 차단	○	○
network traffic monitoring	×	○
Rouge AP 탐지	×	○
Auth/Deauth flood 공격 탐지	×	○

V. 결론

본 논문에서 제안한 시스템은 네트워크의 트래픽을 기반으로 무선 네트워크에서 비정상적인 트래픽의 행위를 탐지하고, 그로부터 알려지지 않은 규칙을 발견하고자 제안하였다. Snort 분석툴을 이용한 경고 데이터의 분석으로 이상적인 행위의 사전단계를 탐지하여 해당하는 signature를 Rule로 규정지어 차단함으로써 과탐지 발생률을 줄일 수 있었다. 하지만 Snort에서 발생한 경고 메시지는 오탐지율의 발생이 생겨날 수 있는 요인이 되기도 하며, 새로운 규칙이 적용되기 위해서는 엔진을 다시 구동하여야 한다는 문제점이 있었다. 또한 분석 시스템의 구동으로 인해 기존의 시스템 보다 지연이 증가하는 단점도 있다.

참 고 문 헌

[1] Yu, Yingbing, Anomaly intrusion detection and threat evaluation using artificial immunity model and fuzzy logic, PhD UNIVERSITY OF LOUISVILLE, 2005.
[2] Tao, Kai, A novel intrusion detection system for detection of MAC address spoofing in wireless networks, MCSc DALHOUSIE UNIVERSITY (CANADA), 2005.
[3] Nath, Shyam Varan, Intrusion detection in wireless networks: A data mining approach, MS FLORIDA ATLANTIC UNIVERSITY, 2005.
[4] Undercoffer, Jeffrey L., Intrusion detection: Modeling system state to detect and classify anomalous behaviors, PhD UNIVERSITY OF MARYLAND, BALTIMORE COUNTY, 2004.
[5] 802.11 무선네트워크 구축가이드, 한빛미디어, 2002.12. 매튜 개스트 저
[6] 무선네트워크 해킹방지 솔루션, 정보문화사, 2003.01 크리스찬 반 외 7인 공저
[7] 스노트 2.0 마술상자, 에이콘 출판사, 강유 저
[8] 해킹과 보안, 영진닷컴, 2003.06 김승현, 윤청원 공저
[9] 침입방지시스템(IPS)의 기술 분석 및 성능평가 방안, 전용희, 정보보호학회 15권 2호, 2005.
[10] http://www.ntop.org/ntop.html
[11]] http://www.snort.org
[12] http://www.snort-wireless.org