JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 5 : 1122~1127 May. 2014

시그니처 기반의 무선 침입 탐지 시스템에 관한 연구

박상노 · 김아용 · 정회경*

A Study on Signature-based Wireless Intrusion Detection Systems

Sang-No Park · A-Yong Kim · Hoe-Kyung Jung*

Department of Computer Engineering, Paichai University, Daejeon 302-735, Korea

요 약

무선랜은 경제성, 유연성, 설치의 용이성, 스마트 기기의 보급으로 인해 사용과 AP(Access Point)구축의 단순화로 사무실, 매장, 학교에서 쉽게 접할 수 있다. 무선랜은 공기를 전송매체로 사용하기 때문에 전파가 도달하는 영역에서는 보안 위협에 항상 노출이 되며 불법 AP 설치, 정책위반 AP, 패킷 모니터링, AP 불법 접속, 외부 AP 및 서비스 접속, 무선네트워크 공유, MAC 주소 도용 등 새로운 보안 위협을 지닌다.

본 논문에서는 시그니처 기반의 Snort를 사용하여 무선 침입 탐지 시스템 개발 방법을 제안한다. 공개된 해킹 툴을 사용하여 모의 해킹을 실시하고, Snort가 해킹 툴에 의한 공격을 탐지하는지 실험을 통하여 논문의 적합성을 검증한다.

ABSTRACT

WLAN is affordability, flexibility, and ease of installation, use the smart device due to the dissemination and the AP (Access Point) to the simplification of the Office building, store, at school. Wi-Fi radio waves because it uses the medium of air transport to reach areas where security threats are always exposed to illegal AP installation, policy violations AP, packet monitoring, AP illegal access, external and service access, wireless network sharing, MAC address, such as a new security threat to steal.

In this paper, signature-based of wireless intrusion detection system for Snort to suggest how to develop. The public can use hacking tools and conduct a mock hacking, Snort detects an attack of hacking tools to verify from experimental verification of the suitability of the thesis throughout.

키워드 : 공통평가기준, 백트랙, 스노트, 시그니처, 침입 탐지 시스템

Key word : Common Criteria, Backtrack, Snort, Signature, Intrusion Detection System

접수일자 : 2013. 12. 22 심사완료일자 : 2014. 01. 14 게재확정일자 : 2014. 01. 29

* **Corresponding Author** Hoe-Kyung Jung(E-mail:hkjung@pcu.ac.kr, Tel:+82-42-520-5640)
Department of Computer Engineering, Paichai University, Daejeon 302-735, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2014.18.5.1122 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

무선 통신 기술 발전과 노트북, 태블릿 PC, 스마트폰을 많이 사용하는 현대 사회는 편리하고 저렴한 초고속 인터넷 서비스를 요구한다. 이러한 요구를 해결한 무선랜은 사회 모든 분야에 걸쳐 사용되고 있으며, 일상생활의 필수적인 부분이 되었다. 무선랜은 물리적인 연결 없이 사용할 수 있다는 편리성이 최대 장점이지만, 대부분의 AP는 노출된 형태로 설치되기 때문에 악의적인 사용자가 쉽게 접근 할 수 있다. 특히, 무선랜 신호는 벽, 천장, 건물의 창문 등 건축물의 제한없이 수신되기 때문에 전파가 닿는 영역에서 침투를 시도할 수 있어 네트워크 위협이 된다.

네트워크 보안은 방화벽, 암호화, 인증 및 VPN으로 개발되었지만 방화벽을 회피하거나 취약점을 악용하고 무력화하는 기술이 발달하여 침입 탐지 시스템이 개발되었다. 유선 기반의 침입 탐지 시스템은 무선랜 환경의 특성에 의해 무선 기반의 공격을 탐지 못한다. 이러한 보안 취약점을 해결하기 위해 802.1x, WEP(Wired Equivalent Privacy), WPA(Wi-Fi Protected Access) 등 인증, 암호화 기법이 개발되고 있으나, 이러한 인증, 암호화 기법은 무선 트래픽 분석 및 인가 사용자로의 위장 등의 의도적인 외부 침입에는 취약점을 내포하고 있다[1]. 또한, 무선랜 사용자가 늘어나면서 공격 시도와 패턴이 다양해지고 있으며, 침투 테스트나 교육 목적을 위해 사용하는 도구들을 악용한다. 또한, GUI 기반의 해킹 툴을 제작하고 무분별하게 배포하여 컴퓨터 관련 지식이 없는 사람도 공격을 시도할 수 있어 보안을 위협한다. 이러한 이유로 침입 탐지 시스템의 중요성이 부각되고 있다. 이에 본 논문에서는 시그니처 기반의 Snort를 사용하여 무선 침입 탐지 시스템 개발 방법을 제안하고 해킹 툴을 사용하여 공격한다. 또한, Snort가 해킹 툴에 의한 공격을 탐지하는지 판단하여 논문의 적합성을 검증하였다.

Ⅱ. 침입 탐지 시스템

2.1. Snort

시그니처 검출 기반[2]인 Snort는 libpcap을 사용하여 패킷 스니퍼 및 로거를 사용하며, 로깅(Logging)에 기반을 둔 콘텐츠 패턴 매칭을 수행한다. 또한, 버퍼 오버플로우, 포트 스캔, CGI 공격 , SMB(Server Message Block) 탐색, OS fingerprint 시도 등 다양한 형태의 침입 및 탐색 행위를 감지 할 수 있다. Snort는 모니터링을 할 필요 없이 실시간으로 경고 시스템을 지원하며, 간단한 명령어를 사용하여 패킷 검사 및 규칙을 할 수 있다[3].

Snort의 아키텍처(Architecture)는 성능, 단순성, 유연성에 초점이 있으며, 스니퍼(Sniffer), 전처리기(Preprocessor), 탐색 엔진(Detection Engine), 출력 모듈(Logging)로 구성되어 있다.

- 스니퍼 : 네트워크에서 데이터를 수집하며, 수집한 네트워크 패킷을 전처리기로 이동한다.
- 전처리기 : 패킷을 탐지 엔진에서 비교하기 전에 사전 처리 작업을 하며, 전처리기는 플러그 인 방식으로 구성된다.
- 탐색 엔진 : 핵심 모듈로서 패킷과 규칙을 비교하며, 경고를 발생한다. 규칙 문법은 프로토콜의 종류, 콘텐츠, 길이, 헤더, 기타 여러 요소를 포함하고 있으며, 사용 환경에 맞게 커스터마이징하는 것이 가능하다.
- 출력 모듈 : Snort가 발생시킨 경고는 출력 모듈로 전송되며, 경고를 데이터베이스로 보낼 수 있다.

Snort의 규칙을 사용하면 간단하면서도 다양한 감지를 할 수 있으며, Snort의 규칙에는 헤더와 옵션을 가지고 있다. 헤더는 규칙 동작, 프로토콜, 대상 목적지 주소, 포트로 구성되어 있다[4].

2.2. 무선 Snort

무선 Snort는 802.11 환경에서 무선 신호를 탐지하기 위해서 새로운 탐지 규칙을 추가하고, Snort 2.0.x와 호환되게 했다. 또한, 새로운 “Wi-Fi” 규칙 프로토콜뿐만 아니라 악성 AP, 애드혹 네트워크를 검출할 수 있다. 그림 1은 802.11을 위해 새로 추가된 규칙이다.

```
alert wifi any -> any (msg:"Mangement Frame"; type:TYPE_MANAGEMENT;)
alert wifi any -> any (msg:"Control Frame"; type:TYPE_CONTROL;)
alert wifi any -> any (msg:"Data Frame"; type:TYPE_DATA;)
```

그림 1. 무선 Snort 규칙
Fig. 1 Wireless Snort Rules

Snort 규칙 동작에는 경고(Alert), 로그(Log), 패스(Pass), 활성화(Activate), 동적(Dynamic)이 있다.

MAC 주소는 원본 및 대상 MAC 주소의 IP 주소가 Snort 규칙에 지정하는 것과 같은 방식으로 지정할 수 있으며, 하나의 MAC 주소는 옥텟(Octets)의 콜론으로 구분된 목록 또는 쉼표로 구분하고, 중괄호로 묶인 목록으로 지정할 수 있다. 또한, '!'문자로 논리적 NOT 연산을 수행할 수 있다. MAC 주소의 형식은 그림 2와 같다[5].

```
# Single MAC Address
00:DE:AD:BE:EF:00
# MAC Address List
[00:DE:AD:BE:EF:00, 00:DE:AD:C0:DE:00, ....]
```

그림 2. MAC 주소
Fig. 2 MAC Address

방향 연산자는 트래픽의 방향을 지정하기 위해 두 개의 연산자를 포함한다. 규칙 옵션은 콘텐츠와 메시지, 그리고 다른 정보들로 구성되어 있으며, 하나의 규칙은 여러 개의 콘텐츠 영역을 가질 수 있다. 콘텐츠 영역 내부에는 패킷 검사에 사용되는 시그니처가 저장되어 있다[6]. 무선 탐지에는 802.11 특정 규칙 옵션인 "Wi-Fi" 프로토콜을 사용하여 규칙을 만들 수 있다. Wi-Fi 옵션에는 frame_control, type, stype, more_frags, from_ds, to_ds, retry, pwr_mgmt, more_data, wep, order, duration_id, bssid, seqnum 등이 있다[7].

2.3. 무선 침입 탐지 시스템 요구사항

무선랜의 보안요소에는 사용자 인증, 접근제어, 권한검증, 데이터 기밀성, 데이터 무결성, 부인방지, 안전한 핸드오프가 있다[8]. 보안기능 요구사항은 국제 사회 내에 널리 사용되고 있는 공통평가기준(Common Criteria)을 충족해야 한다. 공통평가기준은 모든 보안제품에서 필요로 하는 "보안기능"의 전체집합을 클래스, 패밀리, 컴포넌트, 엘리먼트를 통해 계층적으로 분류한다[9]. 보안기능 요구사항은 11개의 클래스로 구성되어 있으며, 보증 요구사항은 9개의 클래스로 구성되어 있다[10]. 실험해야할 침입 탐지 시스템의 보안 요구사항은 표 1과 같고, 알려진 공격이나 알려지지 않은 공격을 탐지할 수 있어야 하고, 실시간으로 경고 메시지를 전송하여 관리자에게 알리는 모니터링 기능이 되어야 한다.

표 1. 침입 탐지 요구사항
Table. 1 Intrusion Detection Requirements

침입 탐지요구사항	비인가 클라이언트 탐지
	비인가 AP 탐지
	정책 위반 AP 탐지
	서비스 거부 공격 탐지
	WEP Cracking 탐지
	MAC Spoofing 탐지
	Fake AP 탐지
	다중 공격 탐지

Ⅲ. 실험

3.1. 실험 환경

실험에 사용된 침입 PC 사양은 표 2와 같으며, 사용된 해킹 툴은 백트랙에 내장된 오픈 소스 해킹 툴과 윈도우기반에서 동작하는 프리웨어 해킹 툴을 사용하여 실험을 진행하였다.

표 2. 침입 PC 사양
Table. 2 Intrusion PC Specifications

CPU	i7-3635QM	i7-2600
RAM	8GB	4GB
무선랜카드	ipTime n100mini	ipTime 150UA
운영체제	백트랙 5 R3	윈도우 7

탐지에 사용된 PC 사양은 표 3과 같으며, Libpcap을 사용하여 패킷을 수집하였다.

표 3. 탐지 PC 사양
Table. 3 Detection PC Specifications

CPU	i5-760
RAM	4GM
무선랜카드	ipTime n100mini
운영체제	CentOS 6.4
Snort	snort-wireless-2.4.3-alpha04
Libpcap	Libpcap-1.4.0
Mysql	Ver 14.14

실험에 사용된 구성 환경은 그림 3과 같고, 보안 기능이 없는 AP 1대와 WPA를 지원하는 AP 1대, WPA2를 지원하는 AP 1대를 사용하여 실험을 진행하였다.

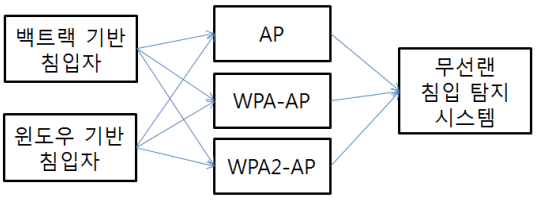

그림 3. 실험 구성도
Fig. 3 Experiment Configuration

3.2. 실험 방법

실험은 무선랜에서 사용되는 오픈소스의 해킹 툴과 프리웨어를 사전에 입수하여 침입 용도로 사용하였다. 일반적인 실험 순서는 그림 4와 같은 순서로 진행하였으며, 본 논문에서는 서비스 거부 공격을 통해 논문의 적합성을 판단한다.

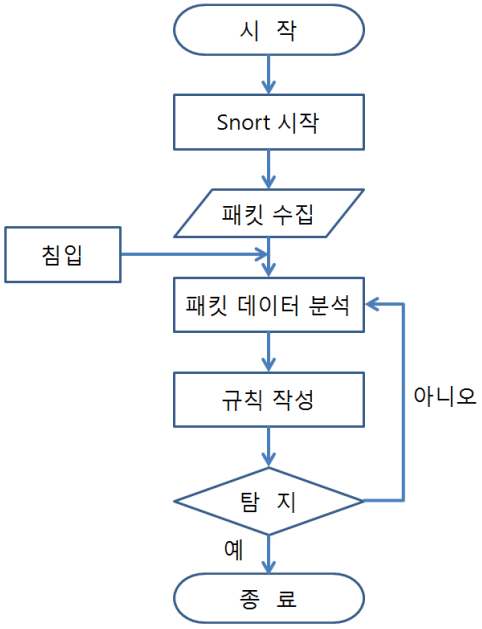

그림 4. 실험 순서도
Fig. 4 Testing Flowchart

주변 AP 정보를 수집하기 위해 그림 5와 같이 백트랙에 내장되어 있는 Airmon-ng와 Airodump-ng을 사용하였으며, 윈도우 기반에서는 그림 6과 같이 카인과 아벨을 사용하여 AP 정보를 수집할 수 있다.

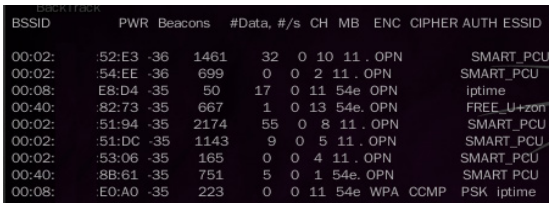

그림 5. 주변 AP 모니터링
Fig. 5 AP Around Monitoring

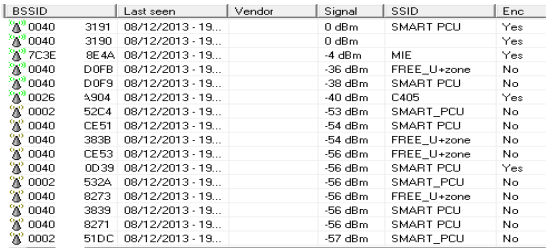

그림 6. 카인과 아벨
Fig. 6 Cain and Abel

Airodump-ng를 사용하여 그림 7과 같이 BSSID와 채널을 고정할 수 있고, 침입할 AP 정보만을 수집할 수 있다.

그림 7. 목표 AP 모니터링
Fig. 7 Goal AP Monitoring

수집한 AP 정보를 통해 침입 탐지 시스템의 정보를 수집할 수 있으며, Aireplay-ng를 사용하여 그림 8과 같이 서비스 거부 공격을 실행한다.

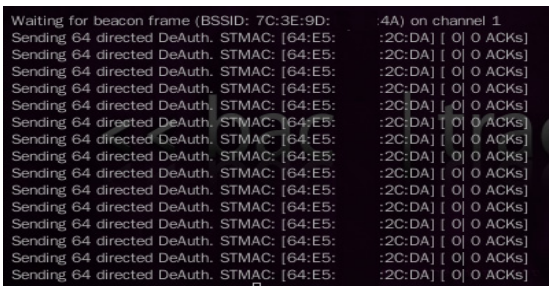

그림 8. 서비스 거부 공격
Fig. 8 Denial-of-Service Attacks

서비스 거부 공격이 실행되면 침입 탐지 시스템에서는 그림 9와 같이 패킷들이 수집된다.

```
12/12-23:21:21.596385 7C:3E:  :  :8E:4A -> 64:E5:  :  :2C:DA type:0x800 len:0x42
173.223.227.26:80 -> 192.168.0.122:46879 TCP TTL:51 TOS:0x0 ID:6818 IpLen:20 DgmLen:52 DF
***A***F Seq: 0xBDEF0A2  Ack: 0x98A6698  Win: 0x1C48  TcpLen: 32
TCP Options (3) => NOP NOP TS: 3620257379 39198086
12/12-23:21:21.636958 64:E5:  :  :2C:DA -> 7C:3E:  :  :8E:4A type:0x800 len:0x42
192.168.0.122:46879 -> 173.223.227.26:80 TCP TTL:64 TOS:0x0 ID:31558 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x98A6698  Ack: 0xBDEF0A3  Win: 0x1F7  TcpLen: 32
TCP Options (3) => NOP NOP TS: 39260596 3620257379
```

그림 9. 패킷 수집
Fig. 9 Packet Collection

수집되는 패킷들은 로그 디렉토리(/var/log/snort)에 저장된다. 그림 10과 같이 로그 파일은 고유의 번호가 부여되며 공격 패턴을 분석하기 위해 해당 로그파일을 열고 분석을 시작한다.

```
drwx------. 2 root root  4096 Dec 12 20:27 192.168.0.125
-rw-------. 1 root root     0 Dec 12 16:40 alert
-rw-------. 1 root root 20015 Dec 12 23:21 ARP
-rw-------. 1 root root     0 Dec 12 20:27 PACKET_NONIP
-rw-------. 1 root root     0 Dec 12 17:09 snort.log.1386835782
-rw-------. 1 root root     0 Dec 12 17:47 snort.log.1386838053
-rw-------. 1 root root     0 Dec 12 17:48 snort.log.1386838084
```

그림 10. 패킷 저장
Fig. 10 Packet Storage

Aireplay-ng에 의한 서비스 거부 공격 패턴을 분석하여 Snort 규칙을 생성한다. 그림 11은 서비스 거부 공격에 관련된 규칙이다.

```
alert wifi any -> any (msg:"Power-Save Poll"; stype:STYPE_PSPOLL;)
alert wifi any -> any (msg:"RTS"; stype:STYPE_RTS;)
alert wifi any -> any (msg:"CTS"; stype:STYPE_CTS;)
alert wifi any -> any (msg:"Ack"; stype:STYPE_ACK;)
alert wifi any -> any (msg:"CF-End"; stype:STYPE_CFEND;)
alert wifi any -> any (msg:"CF-End+CF-Ack"; stype:STYPE_CFEND_CFACK;)
```

그림 11. 주소 결정 프로토콜 규칙
Fig. 11 ARP Rules

‘규칙을 적용하고 다시 서비스 거부 공격을 실행하면 그림 12와 같이 who-has와 reply log가 비정상적으로 생성되는 것을 알 수 있다.

```
who-has 192.168.0.1 tell 192.168.0.101
who-has 192.168.0.122 tell 192.168.0.1
reply 192.168.0.122 is-at 64:E5:99:F0:2C:DA
who-has 192.168.0.1 tell 192.168.0.122
reply 192.168.0.1 is-at 7C:3E:9D:11:8E:4A
```

그림 12. 침입 탐지
Fig. 12 Intrusion Detection

Ⅳ. 결 론

본 논문에서는 주변 AP 정보와 목표로 하는 AP의 정보들을 수집하기 위해 Airodump-ng를 사용했다. 주변에 있는 AP들의 정보들을 먼저 수집하고, 수집되고 있는 AP 중에서 목표 AP를 정한 후 목표 AP의 정보를 집중적으로 수집했다. 수집된 목표 AP의 정보를 활용하여 Aireplay-ng로 서비스 거부 공격을 실시했다.

침입 탐지 시스템에서는 Libpcap을 사용하여 패킷들을 수집하고 Log 파일로 저장하여 분석하였다. 분석한 자료를 기반으로 Snort 규칙을 작성하고, 다시 서비스 거부 공격을 실시하여 탐지 여부를 확인하여 논문의 적합성을 검증하였다.

제안하는 무선 침입 탐지 시스템은 기존의 상업용 무선 침입 탐지 시스템에 비해 저렴하게 구축할 수 있으며, 사용하는 환경에 맞게 운영할 수 있다. 하지만, 패킷이 증가하면 탐지율이 저하되는 것을 문제점을 발견했다.

향후 과제는 탐지율이 저하되는 원인을 보완하기 위해 분산 처리가 가능한 하둡을 도입하고, 수집되는 패킷들을 분산 처리하는 방안에 대한 연구가 필요하다.

REFERENCES

[1] Reddy, S. Vinjosh, et al. "Wireless hacking-a WiFi hack by cracking WEP," *2010 2nd International Conference on*, vol. 1, pp. 189-193, 2010.

[2] Ajita. Mishra and Ashish Kumar Srivastava, "A Modular Approach To Intrusion Detection in Homogenous Wireless Network,“ *IOSR Journal of Computer Engineering*, vol. 14, no. 6, pp. 53-59, Oct. 2013.

[3] Martin. ROESCH, “Snort: Lightweight Intrusion Detection for Networks,” *Proceedings of LISA*, pp. 229-238, 1999.
[4] Steven T. Eckmann, "Translating Snort rules to STATL scenarios," *Proc. Recent Advances in Intrusion Detection*, 2001.
[5] Craig. Valli, "Wireless Snort-A WIDS in progress," *Network & Information Forensics Conference*, pp. 112-116, 2004.
[6] H. S. Kim, B. J. Kang, J. S. Yang and E. G. Im, “An Efficient Signature Detection Method using Growing Prefix Indexing for Intrusion Detection Systems,” *Journal of Security Engineering*, vol. 9, no.1, Feb. 2012.
[7] Andrew. Lockhart, "Snort Wireless Users Guide," 2003.
[8] K. S. Kou, G. J. Mun, D. J. Ryu, “A Development of AIRTMS V1.0’s Security Functional Requirements based on Common Criteria Version 3.1,” *Journal of Security Engineering*, vol. 8, no. 6, pp. 645-655, Dec. 2011.
[9] Y. S. Kim, K. S. Kou, J. I. Sin and Y. H. Bang, "Development of Security Functional Requirement Specification Tool of Information Security Operational System Level," *Journal of Security Engineering*, vol.7, no.1, Feb. 2010.
[10] S. Y. Kang and J. H. Park, “The Research about Recent Common Criteria of Information Security Product,” *Journal of Security Engineering*, vol.5, no.4, Aug. 2008.

박상노(Sang-No Park)

2006년 한밭대학교 전자공학과(공학사)
2013년 배재대학교 컴퓨터공학과(공학석사)
2014년 ~ 현재 배재대학교 컴퓨터공학과 박사과정
※ 관심분야 : 네트워크 보안, 클라우드 보안, 무선랜, 무선랜보안, 화상회의

김아용(A-Yong Kim)

2013년 배재대학교 컴퓨터공학과(공학사)
2013년 ~ 배재대학교 컴퓨터공학과 석사과정
※ 관심분야 : 오픈 소스, 리눅스, 클라우드, 분산처리

정회경(Hoe-Kyung Jung)

1985년 광운대학교 컴퓨터공학과(공학사)
1987년 광운대학교 컴퓨터공학과(공학석사)
1993년 광운대학교 컴퓨터공학과(공학박사)
1994년 ~ 현재 배재대학교 컴퓨터공학과 교수
※관심분야 : 멀티미디어 문서정보처리, XML, SVG, Web Services, Semantic Web, MPEG-21, Ubiquitous Computing, USN