Snort Wireless 기반의 무선 침입 방지 시스템

김아용 · 정대진 · 박만섭 · 김종문 · 정회경

배재대학교 컴퓨터공학과

Wireless Intrusion Prevention System based on Snort Wireless

A-Yong Kim · Dae-Jin Jeong · Man-Seub Park · Jong-Moon Kim · Hoe-Kyung Jung

Department of Computer Engineering, PaiChai University

E-mail : janlssary@pcu.ac.kr, daejin4u@nate.com, ceo@egluon.com, elcomtech@elcomtech.co.kr, hkjung@pcu.ac.kr

요 약

모바일 기기의 활성화로 인해 무선 네트워크 환경이 확산되고, 이로 인해 무선 네트워크를 악용하는 사례도 증가했다. 네트워크 보안 및 침입 탐지는 기존 유선뿐만 아니라 무선에도 주목 받고 있으며, 활발하게 연구가 진행되고 있다. Snort 기반의 침입 탐지 시스템(Intrusion Detection System)은 기존 유선 네트워크에서 악의적인 활동 탐지를 위해 널리 사용되고 있는 검증된 오픈 소스 시스템이며, Snort Wireless는 802.11 무선 탐지 기능을 활성화하기 위해 개발되었다.

본 논문에서는 Snort Wireless Rule을 분석하고, 향후 연구 진행방향을 제시한다.

ABSTRACT

Wireless network environment is spreading due to the increase of using mobile devices, causing wireless network abuse. Network security and intrusion detection have been paid attention to wireless as well as wired existing and studied actively Snort-based intrusion detection system (Intrusion Detection System) is a proven open source system which is widely used for the detection of malicious activity in the existing wired network. Snort Wireless has been developed in order to enable the 802.11 wireless detection feature.

In this paper, Snort Wireless Rule is analyzed. Based on the results of the analysis, present the traveling direction of future research.

키워드

Rule, Snort Wireless, WIDS, Wireless-LAN

Ⅰ. 서론

무선 통신 기술의 발달과 스마트폰 및 태블릿 PC의 보급과 활성화로 인해 우리는 언제, 어디서나 장소와 시간의 제약 없이 인터넷을 이용할 수 있다. 이러한 변화는 우리 생활의 많은 부분을 변화시켰으며, 이러한 배경의 주요 기술은 무선 랜(Wireless LAN) 기술이다.

무선 랜은 다양한 장점과 편의성을 갖고 있지만, 유선 랜에 비해 보안성은 더욱 취약하다. 무선 랜을 사용할 경우 전파가 도달 가능한 거리에 있는 위치라면 어디서나 공격이 가능하며, 개인정보를 탈취하여 제 2의 범죄로 이어질 수 있다.

국내 사례로는 은행의 무선 인터넷 공유기를 해킹해 관리자 아이디와 암호를 탈취하려던 피의자들이 경찰에 붙잡힌 사례가 있었으며, 국내 유명 백화점을 대상으로 진행했던 무선 해킹 테스트에서 무선 암호화의 취약성으로 인해 쉽게 해킹이 가능한 사례가 있다[1].

무선 랜의 보안 취약성을 보완하기 위해서 IEEE 이나 Wi-Fi Alliance에서 표준화된 기술이 사용되고 있으며, SSID(Service Set Identifier)숨기기, MAC Filtering, WEP(Wired Equivalent Privacy)보안, WPA(Wi-Fi Protected Access)보안,

802.1.x 보안, TKIP보안, VPN기반 보안으로 구분된다[2].

다양한 보안 기술이 존재하지만, 무선 네트워크 사용자가 늘어나면서 내부 시스템을 공격하려는 공격자의 패턴도 다양해지고 있다. 이러한 공격자의 패턴을 탐지하기 위해 침입 탐지 시스템의 중요성이 부각되고 있다. 본 논문에서는 Snort Wireless의 Rule을 분석하여 침입 탐지 시스템의 발전 방향에 대해 연구한다.

Ⅱ. 관련 연구

2.1 보안 침해 유형

무선랜을 위협하는 주요 공격유형들은 외부 해커들에 의한 데이터 유출, 비인증 AP(Rogue AP), 접속 취약점, 핫스팟 해킹 등이 주를 이루고 있다[3].

보안 침해 유형들은 패킷 스니핑, MITM(Man in the Middle), Evil Twin 공격(Wi-Fi 피싱), 워드라이빙(Wardriving), 워초킹(Warchalking), 암호사전 공격(Dictionary Attack)이 있다.

2.2 침입 탐지 시스템

침입 탐지 시스템이란 시스템과 네트워크 작업을 분석하여 권한이 없는 사용자가 로그인하거나 악의성 작업이 있는지 찾아내는 활성 프로세스 또는 장치를 말한다. 침입 탐지 시스템은 다수의 종류들이 존재하며, 전통적인 방화벽이 탐지할 수 없는 모든 종류의 악의적인 패턴을 탐지하기 위해 필요하다.

침입 탐지 시스템은 데이터 처리 공격(Data Driven Attack), 권한 상승(Privilege Escalation), 침입자의 의한 주요 파일 접근, 악성 소프트웨어와 같은 호스트 기반 공격을 탐지한다.

Ⅲ. Snort Wireless 분석

Snort Wireless Rule을 분석하기 위한 구현 구성환경은 그림 3과 같다.

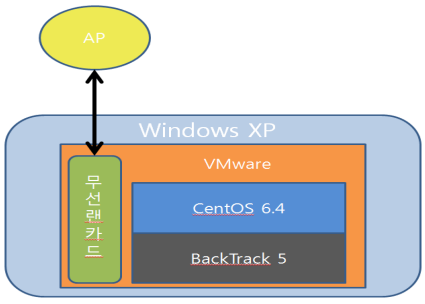

그림 3. 구성도

CentOS에 Snort Wireless와 무선 랜 카드를 설치하고, 무선 AP와 통신이 되도록 하였다. 또한 Snort Wireless Rule을 분석하기 위해 BackTrack5에 내장된 공격 툴을 활용하였다.

침입 탐지 시스템은 오픈 소스와 상용 침입 탐지 시스템이 있지만, 그중에서 Snort는 인기 있는 침입 탐지 시스템이다. Snort는 마틴 로슈(Martin Roesch)에 의해 1998년 개발된 오픈 소스이며, 실시간 침입 탐지 시스템이다. 시그니처 기반의 메트릭을 사용하여 공격을 감지하고 규칙 기반 언어를 이용하여 공격을 방지한다.

Snort Wireless는 무선 패킷에서 정보를 프레임에 따라 작성하는 사용자 정의 규칙이 가능하다. 또한 Rogue AP, War Drivers, AD Hoc 네트워크를 탐색하는 Rule이 포함되어 있다[4]. Snort는 GPL(General Public License)에 따라 사용할 수 있으며, 윈도우나 리눅스에서 작동한다. Snort의 기능은 스니퍼, 패킷 로더, 네트워크 침입 탐지로 분류할 수 있다. Snort는 모니터링을 할 필요 없이 실시간으로 알림을 수신 할 수 있는 기능을 제공한다.

3.1 Snort Wireless Rule 분석

특정 기준과 일치하는 802.11 프레임을 검출하기 위한 사용자 정의 Rule을 작성하면 사용자 지정 Snort Rule의 다른 유형을 작성하는 것만큼이나 간단하다. 또한, Snort Wireless Rule은 Snort Rule 구문과 대부분 동일한 구문을 공유한다[5]. 다음 그림 1은 Snort Wireless에서 제공해주는 Rule이다.

```
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. Snort Wireless Rule

Rule 구성 방식은 <action> Wi-Fi <mac> <direction> <mac> (<rule options>)으로 되어 있다.

Snort Wireless Rule의 첫 번째 항목은 동작(Action)이다.

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 옥텍(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.

```
# 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

방향 연산자는 트래픽의 방향을 지정하기 위해 두 개의 연산자를 포함하고 있다. Rule 옵션은 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, fragnum, addr4, ssid 가 있다.

Ⅳ. 결 론

무선 랜은 유선 랜에 비해 물리적인 전송매체가 필요 없어 구축이 쉽고 유지보수가 용이한 장점을 가지고 있어, 사용량이 증가하고, 많은 무선 네트워크들이 구축되었다. 그러나 무선 랜에 제공되는 서비스는 보안에 많은 취약점들을 가지고 있다.

본 논문에서는 Snort Wireless Rule을 분석하고 Rule 테스트를 위한 연구 환경을 제시하였다.

향후 Snort 기반과 다른 응용분야를 통한 효율적인 침입 탐지 시스템의 개발에 대한 연구가 필요하다.

감사의 글

본 논문은 중소기업청에서 시행한 산학연 공동기술개발사업의 결과입니다.

참고 문헌

[1] “알기쉬운 공중 무선랜 보안안내서,” 한국인터넷진흥원, 2011.12

[2] 박종훈, 김효곤, “무선랜 침입 탐지/차단 강화를 위한 무선기기 정보 자동 수집, 관리 시스템 구현에 관한 연구,” 한국컴퓨터종합학술대회, Vol.37, No.1, pp.30-35, 2010.6

[3] 박재경, “Wi-Fi 보안 침해 및 보안기술 현황,” 한국전파진흥원, Vol.26, pp.38-49, 2010.6

[4] Singh, Rupinder, Jatinder Singh, “A Performance Metrics Scorecard Based Approach to Intrusion Detection System Evaluation for Wireless Network,” Global Journal of Computer Science and Technology, Vol12, No12, 2012

[5] http://snort-wireless.org/, 2013.10