# 네트워크 기반 프로토콜 공격에 대한 침입탐지 시스템의 구성 방안

° 이주영, 김성주, 이준호, 조성훈, 박석천
경원대학교 컴퓨터 공학과

# Configuration of Network-based Intrusion Detection System for Protocol Attack

° Lee-Ju Yeong, Sung-Ju Kim, Jun-Ho Lee, Seong-Hoon Jo, Seok-Cheon Park
Dept. of Computer Engineering, Kyungwon University

**요 약**

DOS (Denial Of Service)에 대한 공격은 시스템의 정상적인 동작을 방해하여 시스템 사용자에 대한 서비스 제공을 거부하도록 만드는 공격으로 현재 이의 공격에 대한 탐지 알고리즘 및 연구들이 많이 제시되고 있다. 본 논문에서는 네트워크 또는 트랜스포트 계층에 해당하는 프로토콜(TCP/IP, ICMP, UDP) 공격을 분석하고 이들 프로토콜의 취약점을 공격하는 DOS 공격 이외의 다른 공격을 탐지하기 위하여 프로토콜의 기능별, 계층별에 따른 모듈화 작업을 통하여 네트워크 침입탐지 시스템을 구성하였다.

## 1. 서론

초기에 연구와 군사 목적으로 발전한 인터넷은 인터넷의 확산과 분산 컴퓨팅 환경의 발달로 원격 접속의 컴퓨터 사용이 증가하면서 다양한 인터넷 프로토콜과 이를 기반으로 인터넷 서비스들이 적용되는 응용 범위가 확장되고 있다. 이를 통해서 외부인의 시스템 불법 침입과 중요 정보 유출 및 변경 등 역기능들이 날로 증가되고 있으며 그 피해 규모 또한 심각한 수준에 이르고 있다. 이에 대한 대책을 위해 많은 연구 개발자들이 보안 도구나 알고리즘 개발에 관심을 갖고 연구를 추진해오고 있지만 다수의 연구용 침입탐지 시스템은 관리상의 불편 및 탐지 규칙의 부족 등으로 인해 실제 환경에서 적용하기에 너무 힘든 점을 가지고 있다. 현재 널리 알려져 있는 네트워크 공격 방법들을 보면 미국의 대표적 웹 싸이트들이 무차별하게 공격을 당할 때 사용되었던 방법인 서비스 거부 공격(DOS : Denial of Service Attack)이 많이 사용되고 있다. 현재 이러한 서비스 공격에 대해서는 많은 연구 개발자들이 보안 도구나 알고리즘 개발에 대한 연구를 추진해오고 있다. 하지만 서비스 거부 공격 방식을 자세히 살펴보면 전체적으로 프로토콜의 취약점을 공격한 방법들 중의 일부분으로 볼 수 있다. 따라서 본 논문에서는 기존에 널리 알려진 이러한 서비스 거부 공격(DOS) 뿐만 아니라 네트워크 프로토콜의 취약성을 공격하는 행위에 대해 리눅스 상에서 네트워크 패킷을 분석하고 각 프로토콜에 해당하는 침입들을 탐지하여 프로토콜별 공격 유형들을 탐지 할 수 있는 네트워크 기반 침입탐지 시스템을 구성하였다.

## 2. 침입탐지 시스템

### 2.1 침입 탐지 시스템의 개요

침입탐지 시스템이란 불법적인 침입 행위를 신속하게 감지하고 대응하는 소프트웨어를 말한다. 탐지 방법에 따라 비정상적인 침입탐지 기법과 오용 침입탐지 기법으로 나뉠 수 있으며 데이터 소스의 종류에 따라 호스트 기반과 네트워크 기반의 침입탐지 시스템으로 분류 될 수 있다. 본 논문에서는 네트워크 또는 트랜스포트 계층에 해당하는 프로토콜 공격을 분석한다.

### 2.2 패킷 캡처를 위한 데이터링크 접근 유형

(1) BSD 패킷 필터(BPF)

4.4BSD와 많은 Berkeley 파생 구현들은 BPF 즉 BSD 패킷 필터를 지원한다. 그림 1은 BPF의 패킷 수신을 보여주고 있다. 패킷이 네트워크 인터페이스로 도착이 되면 Data link level 드라이버는 시스템 프로토콜 스택을 BPF로 보낸다. 만약 BPF가 인터페이스를 listening하고

있는 중이라면 BPF의 첫 번째 네트워크 Tap을 호출하며 Tap은 각각의 배당된 어플리케이션 필터를 패킷으로 공급을 하는 역할을 한다. 어플리케이션은 한번에 하나 이상의 패킷을 받을 수 있는데 이러한 경우 BPF driver는 각각의 프로세스가 요구하는 필터들을 모두 고려하여 패킷을 처리한다[3][6].

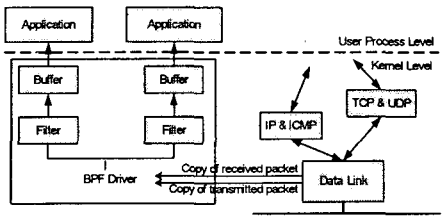


그림 1. BPF 필터링 구조

(2) DLPI (Data Link Provider Interface)

SVR4로부터 유래된 DLPI는 데이터링크 제공자 인터페이스를 통하여 데이터링크의 접근을 제공한다. DLPI는 데이터링크에 의해 제공되는 프로토콜 독립 인터페이스로 링크계층으로의 접근을 위해 raw packet 및 접근 흐름 메시지를 제공하며 보다 효율적인 동작을 위해 두 가지의 STREAM 모듈을 일반적인 흐름에 포함한다. 그림 2에 pfmod와 bufmod을 나타내었다. pfmod는 전송 데이터로부터 요구되는 제한된 여러 내용들을 효과적으로 증가시키거나 버퍼링 메시지를 제공한다. pfmod는 가상 머신을 이용하여 패킷 내부에서의 필터링을 도와 주는 기능을 하는데 이는 BPF에서 제공되고 있는 filter와 동일한 기능을 가진다[3][8].

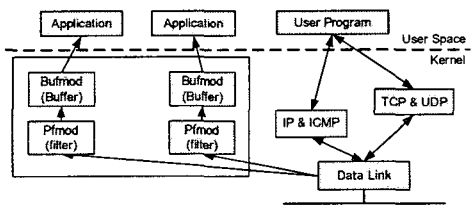


그림 2. DLPI를 이용한 패킷 캡쳐

(3) SOCK_PACKET

리눅스 환경에서 네트워크로 직접 접근을 허용하는 방법으로 두 가지의 소켓을 제공하고 있다. 첫 번째 소켓이 SOCK_PACKET이다. 일반적으로 데이터링크 계층으로부터 패킷을 전달받기 위해서는 SOCK_PACKET이라는 특별한 소켓형을 이용하여 데이터 링크에 접근 할 수 있다[3].

```
sock=socket(AF_INET, SOCK_PACKET, htons(ETH_P_ALL)
```

다른 소켓형으로는 SOCK_RAW가 있다. 보통 데이터그램 지향적인 SOCK_PACKET은 데이터 링크로의 접근이 가능한 반면 SOCKET_RAW는 데이터 링크 계층으로의 접근을 제외한 내부 네트워크 프로토콜 인터페이스로의 접근을 제공한다. 패킷의 접근 방법은 아래와 같이 SOCKET_PACKET과 비슷한 인터페이스를 통해서 패킷을 연다.

```
sock=socket(AF_INET, SOCK_RAW, protocol )
```

### 2.3 프로토콜(Protocol) 별 침입 유형

(1) IP (Internet Protocol) Attack

가) IP Spooping

현재 인터넷에서 가장 많이 쓰이는 TCP/IP는 4.2BSD 시스템에서 구현된 것으로 이는 매우 유동적이며 사용하기에 편리하지만 보안측면에서는 많은 약점을 가지고 있다. 이 약점의 하나를 공격하는 IP Spoofing Attack은 DOS 공격과 source address의 주소를 속이는 통합 공격 방법이다[1]. 일반적으로 공격 시스템은 현재 작동하고 있지 않는 다른 소스 주소를 이용한다. 공격 시스템의 SYN 번호를 알아내기 위해 가장한 소스 주소를 이용하여 연결 요청을 하고 현재 존재하지 않은 주소로의 ACK를 중간에 가로채 공격 시스템과의 연결을 맺는 공격 방법이다.

나) IP Fragment Attack

데이터 전송시 IP 패킷은 몇 개의 작은 패킷 (MTU : Maximum Transmission Unit)으로 나누어서 전송되고 목적지 시스템에서 재조립되는 것을 허용한다. 이러한 fragmentation은 지극히 일반적이고 정상적인 이벤트이지만, 비정상적인 fragment를 발생시켜 라우터나 방화벽을 피하기 위한 목적으로 이용하기도 한다[2]. 공격은 TCP 헤더를 2개의 fragment에 나뉘어질 정도로 작게 분할하여 목적지 TCP 포트번호가 두 번째 fragment에 위치하도록 한다. 일반적으로 패킷이 들어가기 위해서는 포트번호를 확인하는데 포트번호가 포함되지 않을 정도로 아주 작게 fragment된 첫 번째 fragment를 통과시키고 실제 포트번호가 포함되어 있는 두 번째 fragment는 이전에 이미 허용된 fragment의 ID를 가진 fragment 이므로 통과된다. 그 결과 보호되어야할 목적지 서버에서는 이 패킷들이 재조립 되어져 공격자가 원하는 포트의 프로그램으로 무사히 연결될 수 있게 되는 공격 방법이다.

(2) TCP (Transport Control Protocol) Attack

가) SYN Flooding Attack

SYN Flooding Attack은 TCP가 데이터를 보내기 전에 연결을 맺어야 하는 연결 지향의 헛점을 이용한 방식이다[3]. 공격자는 우선 라우팅은 되지만 현재

사용중에 있지 않은 호스트의 주소를 이용한다. 공격 대상의 시스템은 요청 패킷에 응답을 하기 위해 현재 사용중에 있지 않은 호스트에 ACK를 보내지만 호스트는 응답을 하지 않을 것이고 그러면 타겟 시스템은 호스트로부터 ACK를 받기 위해 connection time-out이 걸릴 때까지 큐에 이 연결을 대기시켜 놓을 것이다. 이러한 연결 요청을 공격자가 계속적으로 보낸다면 타겟 시스템의 큐는 오버플로우되고 그 이후에 그 포트로 들어오는 연결 요청은 모두 무시된다[3][4].

나) LAND Attack

Land Attack은 TCP 연결요청 패킷인 SYN 패킷 헤더의 발신자 주소 및 포트를 조작하여 전송하므로써 네트워크 자원을 낭비시키거나 시스템의 실행속도를 현저히 저하시키는 원인이 되고 있다. Land Attack은 TCP 연결요청 패킷인 SYN 패킷 헤더의 발신자 IP 주소와 포트 필드의 값을 공격대상 시스템의 IP 주소와 포트로 설정하여 공격대상 시스템에 보낸다. 이때, 이 패킷을 수신한 시스템은 자기 자신으로부터 발송된 연결요청인 것으로 받아들여 자신에게 계속적인 응답 패킷을 보내게 되어 결국에는 불완전한 연결설정 상태에 빠지게 된다[5].

(3) ICMP (Internet Control Message Protocol) Attack

가) Smurf Attack

이 공격은 서비스 거부 공격의 한 형태이며 공격의 매개 역할을 하는 네트워크와 공격 목표 시스템 쌍방에 극도의 트래픽 혼잡을 유발함으로써 영향을 미치게 된다. 공격자는 IP 근원지 주소를 목표 시스템의 IP 주소로 위장한 브로드캐스트 echo request를 매개 네트워크에 보내는 것으로 공격을 시작하며 시간 지연 없이 패킷을 연속적으로 보낸다. 따라서 매개 네트워크상의 여러 시스템들은 엄청난 echo request에 응답하느라 자원을 소비하게 되며, 목표 시스템의 경우 궁극적으로 수많은 echo reply에 시스템 마비상태가 된다[5].

나) Ping of death Attack

Ping of death 공격은 packet fragment의 취약점이나 서비스 거부 공격을 이용한 방법이다. 일반적으로 ping은 ICMP 메시지 타입 중 echo 요청과 echo 응답을 이용한 것이다. 실제적으로 이러한 ping을 이용한 공격은 가장 손쉽게 IP 패킷을 전송 할 수 있는 타입으로서 ICMP echo 요청 패킷을 상대방에게 전송을 한다. 이때 공격 패킷은 표준 규정 길이 이상으로 큰 IP 패킷을 전송하게 되는데 패킷이 재조립 될 때 규정된 길이 이상으로 큰 IP 패킷으로 조립 되도록 조작된 패킷을 보냄으로써 공격 패킷을 받은 시스템은 TCP/IP 스팩 내부에 이상 현상이 발생되어 시스템이 정지되거나 데이터들이 손실되는 피해가 발생된다[7].

(4) UDP (User Datagram Protocol) Attack

가) Trinoo Attack

Trinoo는 많은 소스로부터 통합된 UDP flood 서비스 거부 공격을 유발하는데 사용되는 도구로 공격은 몇 개의 서버들(마스터들)과 많은 수의 클라이언트들(데몬들)로 이루어진다. 공격자는 trinoo 마스터에 접속하여 마스터에게 하나 혹은 여러개의 IP 주소를 대상으로 서비스 거부공격을 수행하라고 명령을 내린다. 그러면 trinoo 마스터는 특정한 기간에 하나 혹은 여러 개의 IP 주소를 공격을 하기 위해 데몬들과 통신을 한다[9][10]. Trinoo 공격시 주로 사용되는 port는 1524 TCP 포트, 27665 TCP 포트, 27444 UDP 포트, 31335 UDP 포트 등이 주로 사용되는 공격 포트가 된다.

나) UDP packet storm Attack

UDP 폭풍 또는 UDP 서비스 거부 공격으로 불리는 이 공격법은 UDP echo requests 등의 포트를 이용한다. 즉 ineted 서비스가 제공하는 echo 서비스와 chargen 서비스를 통해서 공격이 가능하다. 해커가 패킷을 조작함에 있어서 출발지의 주소 포트를 7(echo)로하고 목적지 주소 포트를 19(chargen)번으로 하여 패킷을 전송한다. 보내진 패킷은 포트 특성상 출발지 시스템과 목적지 시스템 사이를 계속적으로 왕복하게 되며 만일 해커가 이러한 패킷을 하나가 아닌 수많은 패킷을 보내게 된다면 네트워크의 부하는 증가하게 되고 급기야 시스템은 마비상태가 된다[3].

## 3. 네트워크 기반침입탐지 시스템의 구성

네트워크에 흐르는 패킷을 감시함으로써 침입을 감지하는 시스템을 네트워크 기반 침입탐지 시스템이라 하고 그 기능을 보면 다음과 같다. 분석 측면에 있어서 패킷을 분석하는 모듈은 필터링을 수행하는 시스템에 따라 달라질 수 있다. 만약 일반 패킷필터링 수준의 시스템이면 BPF 드라이버를 통해 들어오는 패킷들을 프로토콜별로 헤더를 분석하여 관리자에게 알려줄 것이며, 어플리케이션 수준의 모니터링 시스템이면 이러한 패킷들을 모아서 보다 복잡한 정보를 생성하고 분석하여 각 프로토콜 별 침입에 대한 탐지를 한다. 그리고 분석한 패킷이나 모아진 어플리케이션의 정보를 나중에 이용하기 위해서는 적절한 형태로 변형되어 데이터베이스에 기록을 해두고 다음 공격에 대비한다. 이러한 네트워크에서 패킷의 효율적인 처리를 위해 제안한 침입 탐지 시스템의 구성은 그림 3과 같다.

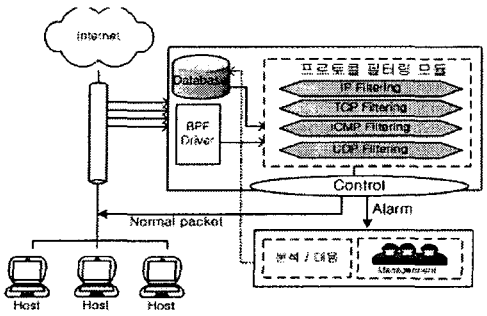


그림 3. 침입 탐지 시스템 구성도

## 4. 침입 탐지 시스템의 프로토콜 공격 탐지

프로토콜 별 공격에 대해서 패킷들을 탐지하기 위해서는 네트워크상의 패킷을 실시간으로 수집하고 프로토콜을 분석하여 이를 받아(accept)들일지 거부(reject)할지를 결정하는 기술이 필요하다. 우선 물리적인 네트워크 트래픽을 사용자 수준에서 접근하기 위해서는 필터링을 수행하고자 하는 호스트의 디바이스 드라이버와 상호 동작할 수 있는 효율적인 기술이 필요하다. 보통의 경우 네트워크 디바이스는 목적지가 자신의 주소로 되어 있는 데이터 프레임만을 수신하지만, Libpcap 라이브러리가 지원하는 Promiscuous 모드로 동작하는 경우에는 프레임의 목적지 주소에 관계 없이 모든 데이터 프레임을 수신하게 되며 기본적으로 BPF 드라이버를 지원하기 때문에 사용자가 패킷 수집을 위한 드라이버를 만들 필요가 없이 내부 네트워크로 들어오는 패킷을 프로토콜 별로 분석을 할 수 있게 되는 것이다. 본 논문에서 제안한 침입탐지 시스템 탐지는 내부 네트워크로 들어오는 이더넷(Ethernet 10Base_T) 데이터에 대해서 작동을 한다. 데이터 패킷은 전송 할 때 frame이라 불리우는 덩어리 형태로 전송을 하게되는데 링크계층을 구성하는 인터페이스의 특성에 따라 이더넷에서 제공하는 MTU 1500 바이트 패킷을 필터링하고 BPF 드라이버를 이용해서 침입 탐지 시스템을 구성하였다. 전체적인 프로토콜 공격 탐지는 표 1에서 보여지는 바와 같은 기능을 통해서 탐지가 가능하다.

표 1 . 공격 유형에 따른 프로토콜 공격 탐지

| 공격 유형들 | 프로토콜 공격 유형 및 관련 자료 |
|---|---|
| Source/Destination address filtering | IP Spoofing Attack, LAND Attack |
| Port filtering | IP Spoofing Attack(21 Port), LAND Attack(139 Port), UDP packet storm Attack(7 port, 19 Port) , IP Fragemtn(specific port), SYN Flooding (specific port) |
| Over size filtering | IP Fragment Attack |
| Buffer overflow filtering | SYN Flooding Attack |
| Traffic counting filtering | Smurf Attack, Trinoo Attack, SYN Flooding Attack |

## 5. 결론

본 논문에서는 내부 내트워크로의 침입을 프로토콜 별로 탐지하기 위해 네트워크 기반 침입 탐지 시스템을 구성하고 현재 데이터 링크 계층으로부터 네트워크 계층 그리고 트랜스포트 계층에 이르기까지 각 프로토콜의 기능별, 계층별에 따른 모듈화 작업을 통하여 DOS 공격 이외에 각 프로토콜 상에서 발생 할 수 있는 침입자에 의한 침입 형태를 분석하였다. 그리고 이를 방어하기 위한 네트워크 기반 침입 탐지 시스템을 구성하였다. DOS 공격에 대한 해결 방법 및 알고리즘은 많이 제안되어었지만 본 논문에서는 DOS 공격을 프로토콜의 각각에 해당하는 공격으로 포함시켜 놓고 그 외에 발생되는 침입을 프로토콜 별로 모듈화 시켰다.

## 참고문헌

[1]infomation Security, Dept. of Math. Inha Univ,1999~2000.

[2]http://ns.certcc.or.kr/paper/tr2001/tr2001-03/IPFragmentation.html#top.

[3]Security+ For UNIX,The Pohang University of Science and Technology, February,1997.

[4]An Approach for TCP Connection Hijaking Attack D.H.Kim, S.I.Park, Y.s.Sek, K.s.Park, J,Y,Lee Dapartment of Computer Engineering, Hallym, University.

[5]윈도우 시스템에 대한 원격 서비스 거부 공격(DOS)과 대책,1998. 06. 한국정보보호센터 기술본부 기술대응팀.

[6]UNIX network programing Networking APIs:socket and XTI,W.RICHARD STEVENS,1998.

[7]윈도우 시스템 거비스 거부 공격과 대책, 1998, 한국정보보호 센터 기술본부 기술 대응팀.

[8]"Effective TCP/IP Programming"/44 Tips to Improve Your Network Programs, Jon C.Sander.

[9]http://cert.certcc.or.kr/announce/WinTrinoo/Trinoo.html

[10]Building Internet Firewalls, 채규혁(아이티웍스)역, 한빛미디어.