IP Fragmentation 공격에 대비하는 실시간 접근 로그 설계 및 구현

국경완, 이상훈
국방대학교 전산정보학과
e-mail:kugstone@hitel.net

Design and Implementation of a Real Time Access Log holding in check IP Fragmentation Attack.

Kyoung-Wan Kug and Sang-Hoon Lee
Dept. of Computer Science, Korea National Defense University

요 약

네트워크가 보편화되면서 사이버 공간을 이용한 테러가 전 세계적으로 발생하고 있다. IP Fragmentation은 이 기종 네트워크 환경에서 IP 패킷의 효율적인 전송을 보장해주고 있지만, 몇 가지 보안 문제점을 가지고 있다. 불법 침입자는 이러한 IP Fragmentation 취약점을 이용해 IP Spoofing, Ping of Death, ICMP 공격과 같은 공격 기술을 이용하여 시스템에 불법적으로 침입하거나 시스템의 정상적인 동작을 방해한다. 최근에는 IP Fragmentation을 이용한 서비스 거부공격 외에도 이를 이용하여 패킷 필터링 장비나 네트워크 기반의 침입탐지시스템을 우회할 수 있는 문제점이 대두되고 있다. 본 논문에서는 패킷 재조합 기능을 제공하고 있지 않은 일부 라우터나 침입차단시스템 그리고 네트워크 기반의 침입탐지시스템들에서 불법 사용자가 패킷을 다수의 데이터그램으로 분할하여 공격할 경우 이를 탐지하거나 차단하지 못하는 경우에 대비하여 실시간 접근 로그 파일을 생성하고, 시스템 관리자가 의사결정을 할 수 있도록 함과 동시에 시스템 스스로 대처할 수 있는 시스템을 구현하여 타당성을 검증하고 그에 따른 기대효과를 제시한다.

1. 서론

최근에 등장하고 있는 정보 시스템 기술이나 정보 보호 시스템은 해킹에 대응할 수 있는 각종 방법을 고려하여 개발되고 있지만 이에 따른 새로운 공격기법 또한 우후죽순처럼 생겨나고 있다. 최근의 공격기법은 대규모 단위의 네트워크를 대상으로 하고 있으며 네트워크 자체를 아예 정지시키거나 파괴해 버리는 엄청난 위력을 보이고 있다.

기존의 공격방법은 이미 잘 알려져 있어 침입차단시스템(IDS, Intrusion Detection System)등을 이용하여 공격패턴에 대한 탐지가 가능해졌고 보안시스템 구축을 통하여 적절히 방어할 수 있었다. 이러한 보안기술의 발전과 더불어 이를 극복하기 위한 공격기술 또한 발전하였고 새로운 공격모델이 등장하였다. 새로운 공격모델에서는 보다 복잡한 공격 탐지기법이 필요하며, 그 대응방법에 대한 변화를 요구한다. 반면 공격자 입장에서는 공격도구의 자동화로 인하여 공격기술이 대중화되고 있으며, 따라서 네트워크 관련 공격이 점점 많아지고 있다.

IP Fragmentation 은 하나의 패킷이 너무 커서 하나의 엔티티(entity)로서 전송되어질 수 없을 때, 네트워크를 통해 보내어질 수 있는 두 개 이상의 더 작은 패킷조각(piece)으로 분리시키는 것을 말한다[8]. IP Fragmentation은 TCP/IP 상에서 매우 빈번하게 이루어지며, 이러한 기술은 네트워크 상에서 IP 패킷의 효율적인 전송을 보장해 주지만 몇 가지 문제점을 가지고 있다. 일부 라우터, Firewall이나 IDS는 패킷 재구성(Reassemble)작업을 수행하지 않기 때문에 공격자들은 인공적으로 시스템의 기능장애를 발생시키거나, Firewall의 보안정책을 우회시키고, IDS의 탐지 정책을 피하기 위하여 다수의 fragment된 패킷들로 쪼개서 공격할 경우 이를 탐지하거나 차단하지 못하는 경우가 발생하고 있다[10].

본 논문에서는 IP Fragmentation 개념과 IP Fragmentation의 취약점을 이용한 공격유형과 대처 방안에 대하여 살펴보고, Firewall, IDS 등과 같

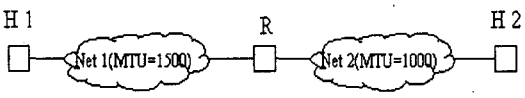
은 보안 도구들이 IP Fragmentation을 이용한 공격을 당했을 때 이를 탐지하거나 차단하지 못할 경우를 대비하여 실시간 접근 로그를 생성하여 시스템을 보호할 수 있는 방법을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2 장에서는 IP Fragmentation 의 개념에 대하여 살펴보고, 3장에서는 이러한 IP Fragmentation 의 보안 허점을 이용한 공격기술과 대처 방안에 대해 기술하였다. 4 장에서는 IP Fragmentation이용하여 공격할 때 실시간 접근 로그를 생성하는 프로그램을 설계 및 구현하여 시스템을 검증하였다. 5 장에서는 본 논문과 관련된 결론을 맺고 향후 연구 방향을 기술한다.

2. IP Fragmentation 개념과 패킷 모니터링

모든 네트워크는 이 기종의 시스템을 가지고 있으므로 동일한 형태의 프레임으로 전송 할 수 없다. 즉, 자료를 보내고자 하는 소스 호스트는 자료를 패킷이라고 하는 작은 블록으로 나누고 이를 목적지 주소와 함께 묶어 보낸다. 이때 각 패킷 각각의 조각을 fragment라 하며 시스템 및 네트워크 장비에서 이러한 패킷을 조각내는 작업을 fragmentation이라 한다. fragmentation은 TCP에서 가장 번하게 이루어지지만 UDP(User Datagram Protocol), ICMP (Internet Control Message Protocol)프로토콜 등에서도 fragmentation이 이루어진다. 이와 같이 IP 프로토콜은 IP 패킷을 몇 개의 작은 패킷으로 나누어서 전송되고 목적지 시스템에서 재 조합되는 것이 허용되며, 서로 다른 최대 패킷 사이즈의 제한을 가진 이기종의 전송매체에서도 IP 데이터그램을 전송 가능하게 한다.

(그림 1) 과 같이 호스트 컴퓨터 H1에서 호스트 컴퓨터 H2로 1500바이트 크기의 데이터그램을 전송한다고 하면 라우터 R은 데이터그램을 수신할 것이고, NET 2를 통해 전송할 수 없을 것이다. 왜냐하면 NET 2의 MTU(Maximum Transmission Unit) 용량이 1000 바이트 크기밖에 되지 않기 때문이다. 이 문제를 해결하기 위해 Fragmentation란 기술을 이용하여 데이터그램을 쪼개고 프레임으로 캡슐화 (Encapsulation)하여 보내는 것이다[8].



(그림 1) IP Fragmentation

이처럼 fragmentation은 지극히 일반적이고 정상적인 이벤트이지만, 비정상적인 fragment를 발생시켜 서비스 거부공격에 이용하기도 하고, fragmentation을 처리하지 않는 라우터나 침입탐지시스템을 피하기 위한 목적으로 고의로 fragmentation을 이용하기도 한다. 목적지로 모든 fragment 들과 데이터그램이 안전하게 도착을 했다면 이를 재조립을 해야 하는데, 이를 중간 단계의 라우터에서 하지 않는 이유는 네트워크 트래픽을 줄이기 위해서이다. 라우터는 수신되는 데이터그램이 fragment인지 아닌지를 알 필요가 없어지며, 수신 즉시 전달할 수 있다. 만약 라우터가 재조립을 한다면 모든 단편들을 다 수신할 때까지 기다려야 하기 때문에 네트워크 트래픽이 증가한다.

3. IP Fragmentation을 이용한 공격유형

IP Fragmentation은 큰 패킷을 전송하기 위해 발생되는 정상적인 과정이지만 공격자는 이 fragment를 조작하여 패킷필터링 장비나 침입차단시스템을 우회하거나 서비스거부공격을 유발시킬 수 있는데 이러한 공격의 대표적 유형은 다음과 같다.

3.1 IP Spoofing

TCP/IP 프로그램은 매우 유동적이며 사용하기 편리하지만 보안 측면에서는 호스트의 인증문제와 순서 번호(Sequence Number)의 생성문제와 같은 보안 문제점을 가지고 있다[14].

3.2 Ping of Death

TCP/IP 프로토콜에서 IP 패킷의 최대 길이는 65,535까지로 제한되어 있으며, 대부분의 시스템이 규정 길이보다 큰 패킷을 전송할 수 없도록 설정되어 있다. 그러나 윈도우 시스템을 포함한 일부 시스템에서는 이 같은 제한이 없어 규정된 길이 이상의 IP 패킷을 전송할 수 있다. 이 경우 최대 길이를 가정하여 구현된 시스템들은 IP 패킷 처리 코드의 버퍼가 초과되어 결과적으로 표준에 규정된 길이 이상으로 큰 IP 패킷을 전송함으로써 이 패킷을 수신받은 OS에서 이 비정상적인 패킷을 처리하지 못함으로써 서비스거부공격을 유발하도록 하는 방법이다.

3.3 ICMP 공격

ICMP은 인터넷프로토콜에서 문제가 생기면 보고해주는 프로토콜로서, 예를 들어 네트워크 접속문제인 "Echo Reply", "Destination Unreachable" 혹은 네트워크 라우팅 문제인 "Redirect" 등을 보고한다. 여기에서 잘 접속되어 있는 시스템이 문제가 있는 양 ICMP 메시지를 만들어 접속을 거부할 수 있으며, ICMP Redirect 를 의도적으로 만들어 네트워크 라우팅 자체를 혼란에 빠지게 할 수 있다. 외부에서의 ICMP 공격 시도를 방화벽(Firewall) 개념에서 모니터 하거나 막을 수 있다.

3.4 Packet Sniffering

최근에 널리 쓰이고 있는 방법으로, tcpdump, snoop, sniff 등과 같은 네트워크 모니터링 툴을 이용해 네트워크 내에 돌아다니는 패킷의 내용을 분석해 정보를 알아내는 것이다. Ethernet은 로컬 네트워크내의 모든 호스트가 같은 선(wire)을 공유하도록 되어 있기 때문에 같은 네트워크내의 컴퓨터는 다른 컴퓨터가 통신하는 모든 트래픽을 볼 수 있다.

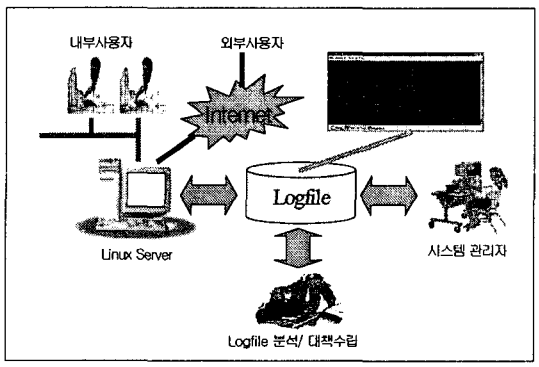
이외에도 최초의 fragment를 아주 작게 만들어서 네트워크의 침입 탐지 시스템이나 패킷 필터링 장비를 우회해서 공격하는 Tiny Fragment 공격, fragment 들이 재 조합될 때의 허점을 이용한 Fragment Overlap 공격, IP를 가로채는 IP Hijacking등이 있다[10].

4. 실시간 접근로그 구현 및 평가

본 절에서는 네트워크 공격을 하기 위해서는 먼저 정보를 수집하기 위하여 표준 프로토콜 방식인 TCP/IP 기반의 ping, finger, host 과 같은 명령어들을 사용하는데, 이때 사용하는 ICMP프로토콜을 이용하여 실시간 접근 로그 프로그램을 설계하고 구현하는데 보다 세부적으로 기술한다. 본 시스템 구현 환경으로는 영문 레드헷 리눅스 7.1 환경에서 ansi-C로 작성하였으며, 컴파일러는 gcc를 사용하였다.

4.1 실시간 접근 로그 프로그램 구조

본 논문에서 제안한 실시간 접근 로그 프로그램(Real Time Access Log Program, 이하 RTAL)은 (그림 2)에서 볼 수 있듯이 세 부분으로 구성된다. 네트워크 상에 존재하는 자신의 컴퓨터와 관련이 있는 모든 패킷의 정보를 필터링하고, 이를 바탕으로 실시간 접근 로그를 생성하며, 해당 패킷 정보를 종합적으로 분석 할 수 있도록 구성되어 있다.



(그림 2) RTAL 프로그램 구조

4.2 ICMP 분석 및 로그 생성 모듈

ICMP는 호스트 서버와 인터넷 게이트웨이 사이에서 메시지를 제어하고 에러를 알려주는 프로토콜로서 RFC 792에 정의되어있다. ICMP는 IP 데이터그램을 사용하지만, 메시지는 TCP/IP 소프트웨어에 의해 처리되며, 응용프로그램 사용자에게 직접 분명하게 보이지는 않는다. 일례로서, ping 명령어는 인터넷 접속을 테스트하기 위해 ICMP를 사용한다. ICMP는 5개의 오류 메시지와 4개의 정보 메시지를 정의하며, 가장 일반적으로 이용되는 ICMP 질의 메시지는 ping 프로토콜을 구현하는데 사용되는 ICMP 메시지들로 구성된다. 호스트나 라우터가 ICMP Echo Request 메시지를 수신한다면 ICMP Echo Reply로 응답한다[1]. (그림 3)은 RTAL 프로그램을 이용, ICMP 패킷을 필터링 하여 ICMP Echo Requested 및 Replay 형식에 맞추어 그 결과를 보여준다. 이와 같이 RTAL은 자신의 시스템과 관련이 있는 각각의 패킷정보와 포함하고 있는 데이터를 분석하여 ICMP 형식에 맞추어 실시간 접근 로그를 생성한다.

```
- Begin of packet number:  1
- Arrival date: Wed Jun 13 16:13:45 2001
IP Source address (From)     : 192.168.0.20 ( )
IP Destination address       : 192.168.0.4 ( )
******* ICMP Header *******
Type                         : Echo Request (8)
Code                         : 0     (0)
CheckSum                     : 18012 (0x465c)
Identification               : 512   (0x200)
Sequence                     : 1280  (0x500)
******* ICMP Data *******
0000000  61 62 63 64  65 66 67 68
         69 6A 6B 6C  6D 6E 6F 70  abcdefghijklmnop
0000010  71 72 73 74  75 76 77
         61  62 63 64 65  66 67 68 69  qrstuvwabcdefghi
-End of packet number:  1
```

(그림 3) ICMP 패킷 분석을 통한 실시간 접근 로그 파일 생성 결과

4.3 TCP 분석 및 로그 생성 모듈

많은 응용 서비스들, 즉 FTP, TELNET, SMTP, X.400 등과 같은 기능을 구현하기 위해 TCP를 사용한다. TCP는 전송되는 데이터를 연속된 Octet 스트림으로 보는 스트림 중심의 데이터 전달 서비스를 제공한다. 한 TCP 사용자로부터 다른 사용자로 전송되는 octet들은 보내진 순서대로 목적지 호스트에 나타난다.

TCP에서는 동일한 데이터 스트림이 목적지 호스트에 모두 나타나거나, 아니면 연결이 해제되어 양쪽 TCP 사용자에게 오류 사실이 통보된다. (그림 4)는 TCP와 관련된 메시지에 포함된 패킷을 분석하여 RTAL 프로그램이 생성한 실시간 접근 로그 파일을 보여준다.

```
- Begin of packet number:          1
- arrival date: Wed Jun 13 16:26:28 2001
IP Source address (From)     : 192.168.0.20 ( )
IP Destination address       : 192.168.0.4 ( )

******* TCP Header *******
Source port address (From)  : 1052/1052
Destination port address    : 23/telnet
Sequence Number : 3492141458 (0xd025d992)
Acknowledgement Number      : 0 (0x0)
TCP Header Length : 7 (0x7) == 28 bytes
Reserved                    : 0     (0x0)
URG flag                    : OFF
ACK flag                    : OFF
PUSH flag                   : OFF
RST flag                    : OFF
SYN flag                    : ON
FIN flag                    : OFF
Window size                 : 16384 (0x4000)
TCP checksum                : 5067  (0x13cb)
Urgent pointer              : 0     (0x0)
TCP Options       : Kind    : 2     (0x2)
Meaning: Maximum Segment Size.
Length : 4      (0x4)
Max. Seg. Size: 1460  (0x5b4)
TCP Options padding bytes   :
0000000  01 01 04 02                ....
- End of packet number:           1
```

(그림 4) TCP 패킷 분석을 통한 실시간 접근 로그 파일 생성

5. 결론

IP Fragmentation은 이 기종의 네트워크 환경에서 IP 패킷의 효율적인 전송을 보장해주고 있지만 앞서 살펴본 것과 같이 몇 가지의 보안문제를 가지고 있다. 많은 패킷 필터링 장비나 침입탐지시스템, 그리고 각 운영체제의 IP 스택이 IP Fragmentation 재 조합을 적절히 처리하지 못하고 있다.

본 논문에서는 불법으로 특정 시스템을 침입하기 위해서는 먼저 상대호스트 정보를 알아내어야 하는데 이때 사용하는 방법이 바로 표준 프로토콜 방식인 TCP/IP 기반의 ping, finger, host 과 같은 명령어들이다. 이와 같은 명령어를 이용할 때 외부에서 접근한 사용자에 대해서 리눅스 시스템은 로그를 남겨놓지만, 외부에서 사용한 명령어들은 로그를 남겨놓지 않아 이러한 보안 문제점을 보완하기 위해 ICMP, TCP에 관련된 패킷을 분석하여 실시간 접근 로그를 생성하여 침입 탐지 및 대책을 강구할 수 있는 프로그램을 구현 및 평가하여 타당성을 검증하였다. 그 결과 다양한 형태로 쪼개진 fragment 들을 실시간으로 분석하여 시스템 관리자가 의사결정을 할 수 있는 것과 동시에 IP Fragmentation에 관련된 다양한 공격유형에 대처할 수 있도록 패킷 정보를 분석해 내는 기능을 제공하였다.

향후의 연구할 방향으로는 본 논문에서 제안된 모델에 근거하여 IP Fragmentation에 관련된 공격 유형을 재정립하고, 각 공격유형에 대처할 수 있는 데이터베이스를 구축하여 시스템 스스로 대처할 수 있는 시스템을 개발하여 리눅스 보안을 더한층 강화하는 것이다.

참고문헌

[1] James Martin, joe Leben, "Tcp/ip Networking : Architecture, Adminstration, and Programming", Prentice Hall , August 1994.

[2] Chris Hare, Karanjit Siyan, "Internet Firewalls and Network Security", 2nd Bk&Cd edition, New Riders Publishing, August 1996

[3] N. Derek Arnold, " Unix Security A Practical Tutorial", McGraw-Hill, Oct 1995.

[4] Graham Class, "Unix for Programmers and Users A Complete Guide", McGraw-Hill, Aug 1994.

[5] Stephen Northcutt, "Network Intrusion Detection An Analyst's Handbook", New Riders Publishing, 2000

[6] 이상훈, 국경완, "유닉스 시스템 이론과 응용", 사이텍미디어, Jul 2001.

[7] 이상훈, 국경완, "실시간 파일시스템 접근로그 감시를 통한 리눅스 보안강화에 관한 연구", 11 쪽, 한국전자통신연구원, 출간예정, Sep 2001.

[8] http://www.gyro.pe.kr/lecture/internet/17.htm

[9] http://ise.yonsei.ac.kr/yhlee/kvalley/152/3_6.html

[10] 정현철, "IP Fragmentation을 이용한 공격기술들", 한국 정보보호 센터, 2001.09

[11] 이현우, "네트워크 공격기법의 패러다임 변화와 대응방안", 한국 정보보호 센터, 2000.05

[12] 임채호, "중요정보통신망 해킹시 침입자기법 분석과 대응", 한국 정보보호 센터, Jan 1999.

[13] http://wonie.co.kr/security/tcpdump.html

[14] IP spoofing 공격과 대책, 한국 정보보호 센터, 1996. 02

[15] 박현미, 신은경, 이현후, "네트워크 스니핑 기술 및 방지대책 ", 한국 정보보호 센터, 2000. 07