TCP/IP 프로토콜 취약성 공격 탐지를 위한 실시간 접근 로그 설계 및 구현

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

Design and Implementation of a Real Time Access Log for TCP/IP Protocol Weakness Attack Detection.

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. TCP/IP 프로토콜은 현재 가장 많이 사용되고 있는 네트워크 기술중의 하나로 인터넷뿐만 아니라, 많은 소규모의 사설 컴퓨터네트워크에서도 많이 사용되고 있다. 그러나 TCP 자체가 가지고 있는 보안 취약점 때문에 SYN 공격, TCP Sequence Number 공격, IP Spoofing, TCP Connection hijacking, Sniffing 과 같은 다양한 해킹 기법이 등장하고 있다. 본 논문에서는 TCP/IP 프로토콜 취약점을 이용하여 공격할 경우 이를 탐지하거나 차단하지 못하는 경우에 대비하여 실시간 접근 로그 파일을 생성하여 시스템 관리자가 의사결정을 할 수 있는 것과 동시에 시스템 스스로 대처할 수 있는 시스템을 구현하여 타당성을 검증하고 그에 따른 기대효과를 제시한다.

1. 서 론

TCP/IP(Transmission Control Protocol/Internet Protocol)는 다양한 네트워킹 기술을 통해 여러 공급업체 장비 사이의 연결을 제공한다. 이는 정의가 잘된 통신 프로토콜과 여러 개의 표준 응용 프로토콜로 구성되어 있다. TCP/IP가 포함된 응용 프로토콜들은 화일 전송, 전자 메일, 원격 로그인, Name Service를 지원한다. TCP/IP의 상위계층인 TCP는 메시지나 파일들을 좀더 작은 패킷으로 나누어 인터넷을 통해 전송하는 일과, 수신된 패킷들을 원래의 메시지로 재조립하는 일을 담당한다. 하위계층, 즉 IP는 각 패킷의 주소부분을 처리함으로써, 패킷들이 목적지에 정확하게 도달할 수 있게 한다. 네트웍 상의 각 게이트웨이는 메시지를 어느 곳으로 전달 해야 할지를 알기 위해, 메시지의 주소를 확인한다. 한 메시지가 여러 개의 패킷으로 나뉘어진 경우 각 패킷들은 서로 다른 경로를 통해 전달될 수 있으며, 그것들은 최종 목적지에서 재조립된다.

TCP/IP는 통신하는데 있어 클라이언트/서버 모델을 사용하는데, 컴퓨터 사용자의 요구에 대응하여, 네트웍 상의 다른 컴퓨터가 웹 페이지를 보내는 식의 서비스를 제공한다. TCP/IP는 본래 점대점(point-to-point) 통신을 하는데, 이는 각 통신이 네트웍 상의 한 점으로부터 시작되어, 다른 점 또는 호스트 컴퓨터로 전달된다는 것을 의미한다. TCP/IP와 TCP/IP를 이용하는 상위계층의 응용프로그램들은 모두 "커넥션리스 (connectionless)"라고 불리는데, 이는 각 클라이언트의 요구가 이전에 했던 어떠한 요구와도 무관한 새로운 요구로 간주된다는 것을 의미한다. 커넥션리스는 네트웍을 독점하지 않으므로, 모든 사람들이 그 경로를 끊임없이 공동으로 사용할 수 있게 한다[15]. 본 논문에서는 TCP/IP 프로토콜의 보안취약점과 이를 이용한 공격유형을 살펴보고, Firewall, IDS (Intrusion Detection System)등과 같은 보안 도구들이 이러한 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 TCP/IP 보안 취약점을 이용한 공격유형을 살펴보고, 3장에서는 TCP/IP 공격탐지를 위한 실시간 접근 로그를 생성하는 프로그램을 설계 및 구현하여 시스템을 검증하였다. 4 장에서는 본 논문과 관련된 결론을 맺고 향후 연구 방향을 기술한다.

2. TCP/IP 공격유형

2.1. SYN 공격

이 방법은 특정 시스템에 불법적인 권한을 얻는 능동적인 방법이 아니라 시스템이 정상적으로 동작을 할 수 없게 만드는 다소 수동적인 방법으로 일종의 Dos(Denial of Service) 공격 중의 하나로 볼 수 있다. 이것은 TCP가 데이터를 보내기 전에 연결을 맺어야 하는 연결 지향(connection-oriented) 방식이라는 착안하여 많은 수의 SYN bit가 설정 되어있는, 즉 연결을 요청하는 TCP 패킷을 호스트의 특정 포트에 보내어 이 포트의 대기 큐(backlog queue)를 가득차게 하여 이 포트에 들어오는 연결 요청을 큐가 빌 때 까지(connection time out) 무시하도록 하게 끔 하는 것이다[14].

2.2 TCP Sequence Number 공격

TCP Sequence Number 공격은 출발지 IP 주소를 목적지 호스트가 신임하는 호스트를 설정한 후 r-command 포트와 같이, 주소를 가지고 인증을 하는 포트 연결을 맺어 데이터를 보낼 수 있게 하는 것이다. 연결을 맺기

위해서는 몇 가지 사전 작업이 필요한데 우선 필요한 것은 목표 호스트가 어떤 식으로 ISN을 발생하는가 하는 것을 알아야 한다. 대부분의 TCP를 구현한 운영체제 커널은 ISN의 값을 무작위로 발생하지 않고 일정 수만큼 증가시켜서 발생시키고 있다[14].

2.3. IP Spoofing

스푸핑은 속이는 방법을 통해서 해킹을 하는 것으로 마치 로그인 화면 같은 프로그램을 통해 사용자로 하여금 패스워드와 계정을 입력하게 해 패스워드를 알아내는 방식이다. 예를 들어 대상 이 되는 호스트의 IP를 똑같이 주게 되면 Duplicate IP Address라는 에러가 발생 하고 서버 시스템은 잠시 네트워크가 멈추게 되는데, 이 순간에 가짜 IP를 다시 한번 이용해 다른 시스템으로 하여금 자신이 대상이 되는 호스트로 보이게 하는 착각을 일으키게 한다.

2.4. Connection Hijacking

Connection Hijacking은 TCP 연결에서 클라이언트와 서버 사이에 확인하는 것이 Sequence Number와 Acknowledgement Number만이기 때문에 가능하다. 즉, 공격자가 서버와 클라이언트간에 교환되는 패킷을 꺼내 IP 패킷을 모방 할 수 있다면 모든 행동이 공격자의 컴퓨터를 통하게 된다. 따라서 그 스트림에 데이터를 추가하고 삭제할 수 있는 방법이다.

2.5 스니핑

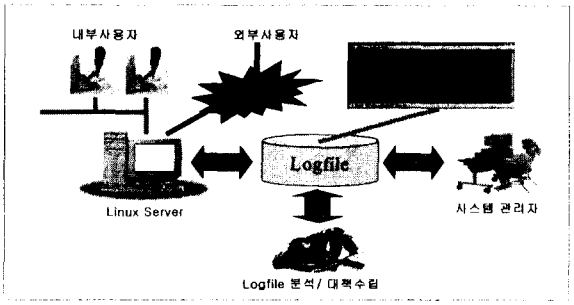
스니핑 (sniffing)은 네트워크상의 한 호스트에서 그 주위를 지나 다는 패킷들을 엿 보는 것으로 다른 사람의 계정과 패스워드를 알 아내기 위해 자주 쓰이는 방법이다. 스니핑 프로그램은 네트워크디바이스를 열어서 Promis cuous mode로 만들어 지나가는 모든 패킷을 읽는 방법이다. 실제로 대부분의 시스템 들이 아직 암호화된 통신을 하지 않고 있기 때문에 스니핑에 의해 빼낼 수 있는 정보는 더 많다고 할 수 있다. 일단 암호화 통신을 하는 경우에는 스니핑에 의해 빼낸 정보를 복호화 하지 못하는 이상 내용을 볼 수 없기 때문에 안전하다.

3. 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 TCP/IP프로토콜을 이용하여 실시간 접근 로그 프로그램을 설계하고 구현하는데 보다 세부적으로 기술한다. 본 시스템 구현 환경으로는 영문 레드헷 리눅스 7.1 환경에서 ansi-C 로 작성하였으며, 컴파일러는 gcc를 사용하였다.

본 논문에서 제안한 실시간 접근 로그 프로그램(Real Time Access Log Program, RTAL)은 (그림 1)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.

많은 응용 서비스들, 즉 FTP, TELNET, SMTP, X.400 등과 같은 기능을 구현하기 위해 TCP/IP를 사용한다. TCP/IP는 전송되는 데이터를 연속된 Octet 스트림으로 보는 스트림 중심의 데이터 전달 서비스를 제공한다. 한 TCP/IP 사용자로부터 다른 사용자로 전송되는 octet들은 보내진 순서대로 목적지 호스트에 나타난다. TCP/IP에서는 동일한 데이터 스트림이 목적지 호스트에 모두 나타나거나, 아니면 연결이 해제되어 양쪽 TCP/IP 사용자에게 오류 사실이 통보된다. (그림 3)는 TCP/IP 형식을 보여주고 있으며, (그림 2)은 TCP/IP와 관련된 메시지에 포함된 패킷을 분석하여 RTAL 프로그램이 생성한 실시간 접근 로그 파일을 보여준다.

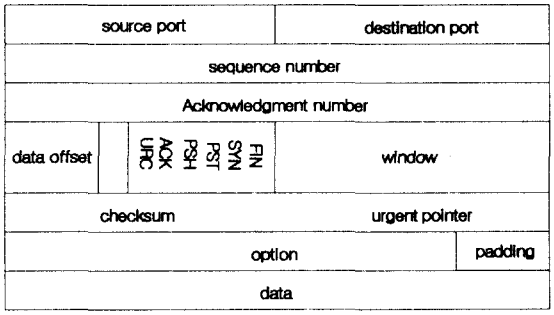


(그림 1) RTAL 프로그램 구조

```
- 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 2) TCP/IP 패킷 분석을 통한 실시간 접근 로그 파일 생성



(그림 3) TCP 세그먼트 형식

4. 결론

TCP/IP 프로토콜의 취약성을 이용한 이러한 적극적인 공격은 지역 네트워크에서 사용되어 질 경우 쉽게 탐지가 되는 반면, 공격이 장거리, 낮은 대역폭, 높은 지연 네트워크 상에서 수행되어질 경우에는 대단히 유효하다.

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 TCP/IP에 관련된 패킷을 분석하여 실시간 접근 로그를 생성하여 침입 탐지 및 대책을 강구할 수 있는 프로그램을 구현 및 평가하여 타당성을 검증하였다. 향후의 연구할 방향으로는 본 논문에서 제안된 모델에 근거하여 실시간 통합 분석 및 다양한 시스템에 이식 가능한 도구와 IPv6에서의 TCP/IP 보안 취약성에 대한 연구가 더 이루어 져야 할 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] 이현우, "네트워크 공격기법의 패러다임 변화와 대응방안", 한국 정보보호 센터, 2000.05
[9] 임채호, "중요정보통신망 해킹시 침입자기법 분석과 대응", 한국 정보보호 센터, Jan 1999.
[10] IP spoofing 공격과 대책, 한국 정보보호 센터, 1996. 02
[11] 박현미, 신은경, 이현후, "네트워크 스니핑 기술 및 방지대책 ", 한국 정보보호 센터, 2000. 07
[12] http://prenet.co.kr/
[13] http://my.netian.com/~kkiso/tcpip1.html
[14] http://daedalus.pe.kr/
[15] http://www.terms.co.kr