이더넷 주소를 이용한 침입자 역추적 시스템 연구

정근훈, 육상조, 이극
한남대학교 컴퓨터공학과

A Study on an Intruder Backtrace System using Ethernet Address

Geunhoon Chung, Sangjo Youk, Geuk Lee
Dept. of Computer Engineering, Hannam University
E-mail : spfalcon@hanmir.com, leegeuk@ai.hannam.ac.kr

요 약

본 논문에서는 보안 침해의 사후 처리 방법으로 이용되는 침입자 역추적 기법 및 시스템에 대해 알아보고, 기존 침입자 역추적 시스템의 특징과 문제점을 파악하여, 역추적에 대한 오버헤드를 초래하지 않으며 보다 효율적으로 작동하는 새로운 역추적 시스템인 이더넷 주소를 이용한 침입자 역추적 시스템을 제시한다.

1. 서론

오늘날 컴퓨터 네트워의 발전으로 많은 사람들이 인터넷의 혜택을 받고 있다. 이렇게 전 세계에 연결된 글로벌 네트워은 사용자들에게 많은 순기능을 제공하기도 하지만, 컴퓨터 네트워의 개방으로 인한 보안의 취약성으로 개인과 기업 그리고, 국가의 비밀 정보가 유출되어 악용되기도 하며, 시스템에 치명적인 손상을 주는 일들이 증가하고 있다. 따라서, 컴퓨터 네트워에 대한 보호가 요구되어 침입 탐지 시스템(Intrusion Detection System)이나 침입 차단 시스템(Intrusion Blocking System, Firewall)들이 개발되고 광범위하게 사용되고 있다.

그러나, 이러한 시스템들은 보안 침해 사고에 대한 사전 방지책이며, 보안침해의 사후 처리에 대한 별다른 대응 방안을 제시해 주지 못하고 있다. 완전한 사전 방지가 보장되지 않는 상황에서는 사전 방지만큼이나 사후 처리도 보안 침해 사고 방지를 위해 중요한 조건이 된다. 따라서, 침입자를 보안 침해 사고 후에 추적하는 방법에 대한 연구가 필요하다.

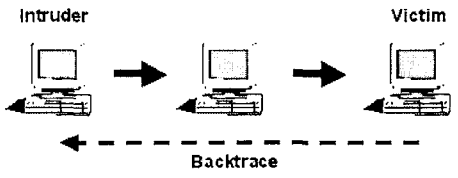
본 연구에서는 컴퓨터 네트워에서 효율적인 침입자 역추적 시스템 개발을 위하여 기존에 연구된 침입자 역추적 방법을 고찰한 후, 보다 효율적이며, 침입의 확실한 증거를 포착할 수 있도록 이더넷 주소를 이용한 침입자 역추적 시스템을 설계한다.

본 논문은 2장에서 역추적 시스템이란 무엇인지 정의를 내리고, 기존에 연구된 침입자 역추적 시스템의 특징 및 문제점들에 분석한다. 3장에서 이더넷 주소를 이용한 침입자 역추적 시스템의 기반 기술에 대해 알아보고, 4장에서 이더넷 주소를 이용한 침입자 역추적 시스템의 동작 및 요구 사항을 알아보고, 마지막으로 결론을 내린다.

2. 관련 연구

2.1 역추적 시스템

침입자는 자신의 위치가 노출되는 것을 피하기 위하여 자신의 IP를 위조하거나 여러 경로를 거치게 된다. 이러한 경우, 침입자의 위치를 알아내기가 매우



[그림 1] 역추적 시스템

힘들다. 일반적으로 침입자의 확인과 역추적을 위한 분석 작업을 자동으로 수행하여 원래 침입자의 위치를 확인하기 위한 시스템을 침입자 역추적 시스템이라 한다.

2.2 기존 연구

2.2.1 로그 정보 기반 침입자 역추적 기법

별도의 역추적 설비가 없는 시스템에서는 UNIX의 기본적인 로그 정보를 바탕으로 특정 사용자나 호스트의 정체를 파악하기 위해 관련 명령어를 사용하여 침입자를 추적할 수 있다.

일반적으로 사용자 추적에 사용되는 명령어는 finger, users, whodo 등이 있다. 또한 현재 사용자가 시스템에서 활동 중일 경우, 사용자의 연결 상태와 활동을 파악하기 위해 netstat 명령어를 사용한다.

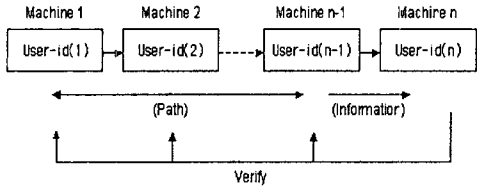
사용자 추적에 사용될 수 있는 로그 파일들로는 utmp, wtmp, acct, lastlogm messages 등의 로그 파일들이 있으며, 이러한 로그 파일들은 자동으로 생성된다.

그러나, 이러한 명령어와 로그 파일의 정보를 이용하여 컴퓨터 네트웍 침입자를 역추적하는 방법은 여러 가지 한계가 있다. 첫째, 관리자가 방대한 로그 파일을 이용하여 직접 수작업을 해야만 한다. 따라서, 침입자가 자신의 자취를 은폐할 수 있는 충분한 시간을 얻을 수 있다. 둘째, 로그 파일이 제공하는 많은 정보 중에서 침입자의 추적에 관계되는 확실한 증거를 찾아내기 어렵다. 셋째, 로그 파일의 정보는 침입자가 쉽게 위조할 수 있기 때문에 로그 정보를 이용하는 방법은 신뢰성을 보장받지 못한다.

2.2.2 Caller Identification System

Caller Identification System은 침입자 역추적을 위한 시스템으로, ETCPW(Extended TCP Wrapper)와 CIS(Caller Identification Server)로 구성되며 이러한 구성 요소에 의해 침입자에 대한 모든 경로를 제공하는 기능을 얻게 된다. ETCPW는 UNIX 보안을 위한 응용 프로그램인 TCP Wrapper의 기본적인 필터링 및 로그 기능을 강화시켜 인접 시스템에 대한 정보뿐만 아니라 침입자가 지나온 이전의 모든 시스템에 대한 경로 정보를 저장할 수 있는 구조를 갖는다. CIS는 ETCPW에 의해 전달된 사용자의 접속 경로를 확인하고, 그 결과를 다시 ETCPW에 제공하는데, ETCPW는 이 정보를 토대로 사용자의 접근 여부를 결정한다.

침입자는 자신의 위치가 노출되는 것을 피하기 위해 여러 단계를 거쳐 침입 대상 컴퓨터에 접근하며, 이러한 경우에 시스템 관리자는 침입자의 위치를 알아내기가 매우 힘들다. Caller Identification System은 이러한 상황에서 침입자를 역추적 하기 위하여 호스트 접속 요구가 발생할 때마다 사용자의 경로를 확인한다.



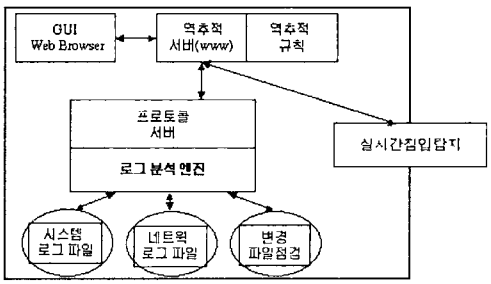
[그림 2] 사용자가 user-id(n)으로 machine(n)에 접근 시도

[그림 2]는 Machine(1)의 사용자가 User-id(n)으로 Machine(n)에 접근하려고 하는 상황을 나타낸다. 사용자가 이미 Machine(1)에서 Machine(n-1)까지의 접근이 이루어진 상태에서 Machine(n)에게 접근을 요청할 때, Machine(n)은 Machine(n-1)에게 사용자의 모든 경로에 대한 정보를 전송받은 후, 그 경로상의 모든 Machine들에게 인증 요청 메시지를 보내어 Machine(n-1)이 보낸 경로를 확인한다. Machine(n)은 사용자가 지나쳐온 모든 Machine으로부터 인증 확인 메시지를 받은 이후에 사용자의 접근을 허용한다. Caller Identification System은 이러한 정보를 바탕으로 침입자의 초기 위치를 탐지해낼 수 있다.

이러한 특징에도 불구하고, Caller Identification System은 몇 가지 문제를 가지고 있다. 첫째, 침입자가 거쳐온 모든 지점에 역추적 시스템이 설치되어 동작하고 있어야 하며, 역추적 시스템이 설치되지 않은 호스트로부터의 접근에 대한 역추적은 불가능하다. 둘째, 역추적 시스템이 설치된 호스트의 보안 취약성으로 인해 역추적 시스템의 신뢰성이 떨어진다. 침입자가 접근한 경로중 한 곳에서 침입자가 루트 권한을 획득했다면 위조된 경로 정보를 전달하여 자신의 침입 경로를 위장할 수 있다. 셋째, 모든 호스트에 역추적 시스템을 설치해야 함으로 호스트의 성능이 떨어진다. 넷째, 침입자가 경유할 수 있는 모든 호스트의 운영체제에 대해 역추적 시스템을 개발해야 한다.

2.2.3 인젠 역추적 시스템

인젠 역추적 시스템은 로그 정보 기반 침입자 역추적 기법을 로그 분석 엔진을 통하여 자동화시킨 시스템이다.



[그림 3] 인젠 역추적 시스템

인젠 역추적 시스템은 자동화된 로그 분석 엔진을 탑재함으로써 로그 기반 침입자 역추적 기법이 가지고 있는 관리자의 방대한 업무를 줄여주고, 침입자가 로그 파일을 위조할 수 있는 기회를 줄여주기는 했지만, 여전히 역추적에 대한 단서를 찾기 어렵고, 신뢰성 또한 보장받지 못한다.

3. 이더넷 주소를 이용한 침입자 역추적 시스템(Intruder Backtrace System using Ethernet Address, IBSEA)의 기반 기술

3.1 TCP/IP 프로토콜 그룹의 계층

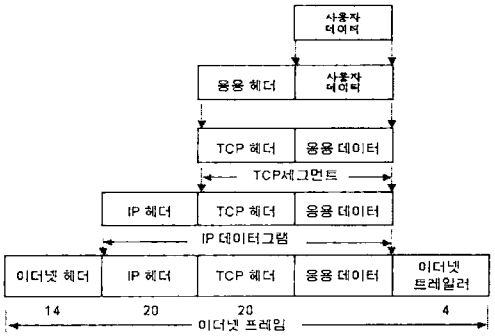
TCP/IP와 같은 프로토콜 그룹은 여러 계층의 프로토콜 조합으로 되어있다. TCP/IP는 보통 [그림 4]처럼 4계층 시스템으로 생각할 수 있다.

Application Layer	telnet, rlogin, ftp
Transport Layer	TCP, UDP
Network Layer	IP, ICMP, IGMP
Link Layer	장치드라이버와 인터페이스카드

[그림 4] TCP/IP 프로토콜 그룹의 4계층

3.2 데이터 캡슐화

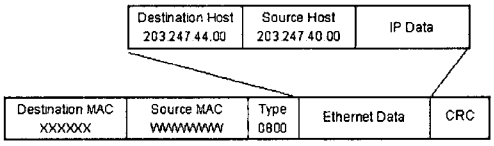
응용 프로그램이 TCP를 이용하여 데이터를 송신할 때, 데이터는 아래의 프로토콜 스택으로 보내지며, 각 층을 통과해서, 마지막에는 비트 스트림으로 네트워상에 전송된다. 이때 각 계층은 데이터가 목적지에 잘 전달되도록 하기 위하여, 수신된 데이터에 각종 헤더(Header) 또는 트레일러(Trailer) 정보를 추가한다. [그림 5]는 이에 대한 처리 과정을 보여준다.(UDP 데이터에 대해서도 거의 같은 구조로 되어있다.)



[그림 5] 프로토콜 스택에 따른 데이터 캡슐화

3.3 이더넷 주소

이더넷 프레임이 로컬 네트워의 어떤 호스트에서 다른 호스트로 전송될 때 프레임의 목적지 인터페이스를 결정하는 것은 이더넷 주소(Ethernet Address, Media Access Control Address, MAC Address)이다. 이더넷 주소는 48비트의 크기를 가지며 네트워 인터페이스 카드(Network Interface Card)에 있는 고유한 주소이다. 디바이스 드라이버 소프트웨어는 IP 데이터그램(Datagram)에 들어있는 목적지 IP 주소를 알 수 없다.



[그림 6] 이더넷 헤더의 이더넷 주소

때때로 침입자들은 자신의 위치를 감추기 위해 IP 스푸핑(Spoofing) 기법을 이용하여 IP 주소를 위조한다. 그러나, 하드웨어 주소인 이더넷 주소는 쉽게 위조하지 못한다. 따라서 이더넷 주소를 이용한 침입자 역추적 시스템은 침입자의 신분을 확실히 파악하는 시스템이 된다.

4. IBSEA 설계

4.1 IBSEA의 동작과정

TCP/IP 프로토콜을 사용한다 하더라도 네트웍상의 다른 호스트에 접근하기 위해서는 IP 주소가 아니라 이더넷 주소를 이용한다. 모든 이더넷 어댑터는 48비트의 고유 이더넷 주소를 가지고 있다. 이더넷 주소는 호스트가 송신하는 모든 패킷에 들어있지만, 첫 번째 라우터내의 이더넷 주소까지만 볼 수 있다. 따라서, 수신된 일반 패킷에서 이더넷 주소를 찾을 수 없는 경우, 침입자에게 이더넷 주소를 묻는 질의를 보낸다. 그러면, TCP/IP 패킷의 페이로드(Payload)에 있는 이더넷 주소가 들어난다. 응답이 없을 경우, 첫 번째 라우터에게 침입자 IP의 이더넷 주소를 요청한다.

```
if (local_network()) {
    intruder.MAC = get_MAC();
else if (wide_network()) {
request_MAC_of _ip(ip)
request_to_router(ip);
}
else
    intruders.id = "unknown";
}
```

[그림 7] 이더넷 주소를 가져오는 과정

4.2 IBSEA의 요구사항

IBSEA는 자체적으로 침입자를 탐지하는 부분은 포함되어 있지 않다. 또한 침입자를 발견했다 하더라도 아직 어떠한 대응도 실행하지 않는다. 따라서, IBSEA는 독립적으로도 작동할 수도 있지만 침입 탐지 시스템이나 침입 차단 시스템과 함께 동작할 때 더 효율적으로 운영된다. 따라서 침입 탐지 시스템이나 침입 차단 시스템과 같은 침입 대응을 위한 시스템과의 표준화된 인터페이스가 요구된다.

5. 결론

IBSEA는 호스트기반의 실시간 침입자 역추적 시스템이다. 모든 이더넷 어댑터는 고유의 이더넷 주소를 가지고 있으므로, 사이버 범죄를 추적하는데 유용한 근거가 될 수 있다.

IBSEA는 경유 호스트에 특정한 소프트웨어를 설치할 필요가 없으므로, 구현 및 운영이 편리하다. 또한 네트웍 라우터에 특정한 오버헤드(Overhead)를 초래하지 않으므로 효율적으로 네트웍을 운영할 수 있다. 침입자 역추적 시스템이 활성화된다면, 보안사고의 사후 처리뿐만 아니라 해킹의 예방에도 도움이 될 것이다.

[참고문헌]

[1] H. T. Jung, et. al., "Caller Identification System in the Internet Environment," Proceedings of the USENIX Security Symposium IV, 1993

[2] 김수형, 강명호, 조형재, 송주석, "안전하고 효율적인 침입자 역추적 시스템 연구," 한국정보과학회 봄 학술발표논문집 제25권 1호, 1998

[3]http://www.certcc.or.kr/concert/cs9803/present/te02/index.htm

[4] 임채호, 원유헌, "인터넷 해킹피해 시스템 자동분석 에이전트(AIAA) 및 침입자 역추적 지원도구 구현," 한국정보처리학회 논문지 제6권 11호, 1999.11

[5] W. Richard Stevens, TCP/IP Illustrated The Protocols : Volume 1, Adddison-Wesley, 1998

[6] W. Richard Stevens, UNIX Network Programming Networking APIs:Sockets and XTI Volume 1, 2nd Edition, Prentice Hall, 1998