2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

Loki 프로젝트를 적용한 Stacheldraht에서의 ICMP 패킷 분석

이중현* 이상영** 유철중** 장옥배**

*전북대학교 정보과학대학원 **전북대학교 컴퓨터과학과

play-hyun@hanmail.net, leesy@cs.chonbuk.ac.kr,

{cjyoo, okjang}@moak.chonbuk.ac.kr

Analysis of ICMP Packet in Stacheldraht Applying Loki project

*Jung-Hyun Lee **Sang-Young Lee **Cheol-Jung Yoo **Ok-Bae Chang

*Dept. of Information Science, Chonbuk National University

**Dept. of Computer Science, Chonbuk National University

요 약

ICMP는 두개의 호스트(host)간에 혹은 단일 호스트와 라우터와 같은 네트워크 장비 간에 에러 메시지를 주고 받을 때 사용된다. 이러한 ICMP는 특히 비 연결 지향 프로토콜인 UDP와 IP의 에러 메세지 전송 시 사용된다. DDoS 도구인 Stacheldraht는 ICMP 패킷을 통해 상호 존재 확인과 위장된 패킷 사용이 가능한지를 테스트하는 수단으로 ICMP ECHO REPLY와 ICMP ECHO REQUEST를 사용한다. 이러한 Stacheldraht에서의 ICMP 패킷을 통한 과정에 보안 채널인 Loki 프로젝트를 적용하면 ICMP 패킷 이동에 따른 마스터와 에이전트의 존재 여부를 확인하고 탐지하는데 효율적이다.

1. 서론

최근 IT 분야의 발달에 따라 기업 등의 다양한 고급기술 정보들이 해킹에 의해 피해를 당하고 있다. 즉, 급속도로 해킹에 관련된 도구들이 강력해지고 있고 고도화된 해킹 기법들이 속속 등장하면서 모든 영역에서의 시스템에 대한 보안 위협이 날로 증가하고 있다. 또한 이에 맞서는 안전한 시스템을 구축하기 위한 노력도 강도 있게 진행되고 있으며 효율적인 여러 보안 도구들이 등장하고 있다. 특히 최근에 이슈가 되고 있는 DDoS(Distributed Denial of Service) 공격은 단순한 공격 방법들이 많아 누구나 쉽게 이용할 수 있고 공격의 원인 및 원천지를 찾기 힘든 특징이 있어 크래커들이 자주 사용하는 해킹 기법 중의 하나이다[1, 2, 3]. 아울러 DDoS 공격은 마스터 시스템이나 에이전트 시스템으로 이용당하거나 더욱 심각한 것은 시스템 관리자 자신도 인지하지 못하면 보안의 취약성은 물론 자칫하면 DDoS 공격자로도 의심받는 경우까지 있는 특징이 있다. 본 논문에서는 Linux 기반 DDoS 도구중 여러 대의 공격 컴퓨터가 하나의 목표 컴퓨터를 동시에 공격하는 특징을 가지는 TFN(TribedFlood Network)의 발전된 버전인 Stacheldraht의 DDoS 도구에 Loki 프로젝트를 적용한 새로운 관점에서의 ICMP(Internet Control Message Protocol) 패킷 탐지에 대한 분석을 제시하고자 한다.

2. 관련연구

1999년 8월 trinOO와 유사한 개념인 TFN이 Mixter에 의해 개발된 이래 1999년 10월 TFN의 발전된 버전인 Stacheldraht라는 새로운 DDoS 도구가 미국이나 유럽의 해킹당한 시스템에서 발견되고 있다. Stacheldraht는 독일어로 철조망이라는 의미를 가지고 있으며 ICMP flood, SYN flood, UDP flood와 스머프(smurf) 등의 공격에 의해서 DDoS 공격을 할수

있는 기능을 가지고 있다. 이것은 trinoo와 TFN 보다 공격자와 Stacheldraht의 마스터 사이에 telnet과 유사한 암호화 통신프로그램(telnetc/client.c)을 추가한 개념이다[4].

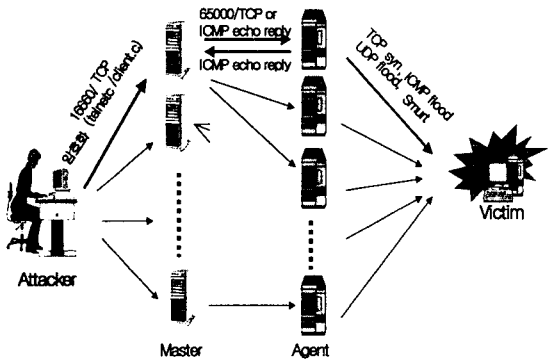

그림 1. Stacheldraht 도구의 네트워크 시스템 구성도

그림 1은 DDoS 공격을 위한 Stacheldracht의 네트워크 시스템을 나타내는데 그림에서 보는 바와 같이 공격자, 마스터, 에이전트 및 목표 시스템으로 구성되어 있다. 여기서 공격자는 공격 마스터 시스템(16660/TCP port)에 접속하기 위해 조절자 프로그램을 사용하며 접속과 동시에 패스워드 입력을 요구한다. 이때 입력된 패스워드는 네트워크를 통해 마스터 시스템의 조절자에게 전달되기 전에 'authentication' 전달 단계를 사용하여 캡슐화된 상태로 보내진다. 에이전트 시스템은 마스터 시스템으로부터 공격 명령을 받아 목표 시스템에 ICMP flood, SYN flood, UDP flood와 스머프 등 실제 다량의 패킷을 넣는데 사용되는 시스템으로 데몬(deamon) 프로그램이 그 역할을 수행한다.

3. Loki 프로젝트를 적용한 Stacheldraht에서의 ICMP 패킷 분석

3.1 Loki 프로젝트 도입

Stacheldraht 공격 도구의 마스터 시스템과 에이전트 시스템에서는 주기적으로 서로의 존재를 확인하는 과정에 ICMP 패킷을 이용한다. 이러한 ICMP 패킷은 네트워크 관리, 테스트 및 측정에 폭넓게 사용되고 있다[5]. 본 논문에서는 이러한 ICMP 패킷에 Loki 프로젝트를 적용하여 많은 방화벽과 네트워크에서 ICMP 패킷을 방해받지 않고 통과할 수 있도록 해주면서 Loki와 같은 비밀 통로를 통한 데이터에 간단한 정보를 실어 보냄으로써 서로의 존재를 확인하는 과정을 탐지할 수 있는 모델을 제시한다.

Loki는 노르웨이 신화에 나오는 사기와 속임수의 신의 이름에서 인용해온 것으로 비밀스러운 의미를 가진다. 기본적으로 방화벽 정책을 보면 우선 두 네트워크 사이를 오가는 트래픽은 반드시 방화벽은 거쳐야 하며 방화벽에 의해 인증 받은 트래픽만 지나갈 수 있다. 이를 전제로 한다면 ICMP 패킷의 활용에 대한 중요한 사항을 검출할 수 있게 된다. 여기서 ICMP는 IP 레이어에 대한 부가 프로토콜으로 에러 메시지와 그 밖의 정보를 유니캐스트 주소로 이송하는데 사용되는 비연결적 프로토콜이다. 이러한 ICMP 패킷은 IP 데이터그램의 내부에 캡슐화되어 있는데 특히 모든 ICMP 메시지의 헤더에서의 처음 4바이트는 동일하다. 반면에 헤더의 나머지 부분은 ICMP 메시지 형식에 따라 상이한 포맷 형식을 갖는다. 이러한 ICMP 메시지에는 표 1에서와 같은 13개의 서로 다른 형식이 존재한다.

표 1 ICMP 형식

형식	기술
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo
11	Time Exceeded
12	Parameter Prob
13	Timestamp
14	Timestamp Reply
15	Info Request
16	InfoReply
17	Address Request
18	Address Reply

여기서 분석할 ICMP의 형식은 0x0과 0x8이다. 그림 2에서 보는 바와 같이 ICMP 형식 0x0은

ICMP_ECHOREPLY(응답)를 나타내고 형식 0x8은 ICMP_ECHO(질의)를 나타낸다. 여기서의 기본적인 작동 과정을 보면 ping 프로그램을 통해 0x8을 서버에 보내어 0x0 응답을 받아내는 과정으로 진행된다.

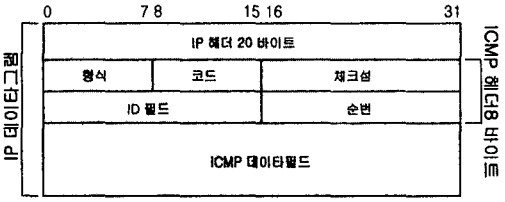

그림 2 ICMP ECHO REPLY와 REQUEST 형식

3.2 Loki 프로젝트 적용

Loki 프로젝트를 적용하면 임의의 데이터가 ICMP_ECHO와 ICMP_ECHOREPLY 패킷의 데이터 영역에 숨겨진다. 이러한 통로는 보통 정보 교환에 사용되지는 않으므로 결과적으로 비밀 채널은 보통의 시스템 보안 정책으로는 감지하고 차단할 수 없다. 이론적으로는 거의 모든 프로세스 또는 데이터 비트가 비밀 채널이 될 수 있다. 그러나 실제로는 비밀 채널로부터 유용한 데이터를 적절하게 도출해내는 것은 어렵다. 그러나 Loki 프로젝트를 적용하면 이러한 문제는 해결된다. 특히 Stacheldraht에 이러한 개념을 도입하면 주기적으로 마스터와 에이전트 사이에 ICMP 패킷을 주고 받으면서 서로의 존재를 확인하게 되는데 이것은 네트워크의 ICMP 패킷을 계속 모니터함으로써 마스터 및 에이전트의 존재를 찾아낼 수 있는 방법이 될 수 있다.

Stacheldraht는 마스터 시스템과 에이전트 시스템 사이에서 ICMP 패킷을 이용하는데 크게 두 가지 기능을 수행한다. 하나는 주기적으로 패킷을 보냄으로써 존재 여부를 확인하는 것과 다른 하나는 에이전트 데몬이 실제로 표적 시스템 및 네트워크에 DDoS 공격을 실행할 경우에 목표 시스템 쪽에서 에이전트의 IP를 추적하지 못하도록 소스 주소를 위장하기 위한 위장된 패킷 사용의 목적으로 쓰인다. 특히 이러한 소스 코드를 수정하여 프롬프트나 패스워드, 커맨드, TCP/UDP 포트 번호 등의 특징들의 변형이 가능하다. 이상의 과정을 정리하면 아래 표 2와 같다. 표에서 보는 바와 같이 위장된 주소를 사용하기 위해 현재 에이전트가 속해 있는 네트워크에서 위조된 소스 IP 주소를 가지는 패킷이 네트워크 바깥으로 나갈 수 있는지를 테스트하기 위해 보통의 경우에 ICMP 형식(ECHO REQUEST) 8을 사용하지 않고 독특하게 7을 사용함을 볼 수 있다. 이것은 마스터 시스템에서 이를 받아들이고 ECHO REPLY함으로써 위조할 가능성이 있는지를 확인하는 것이다.

표 2 Loki를 적용한 ICMP 패킷 교환 과정

형식	ID 필드	데이터 필드	패킷 이동
0	666	skillz	마스터 -> 에이전트
0	667	ficken	마스터 <- 에이전트
7	666	위조된 소스 IP 주소	마스터 -> 에이전트
0	1000	spoofworks	마스터 <- 에이전트

그리고 마스터 시스템의 조절자와 에이전트 데몬은 상호간에 통신을 하기 위하여 암호화되지 않은 상태의 ICMP 패킷을 주고 받는다. 따라서 tcpdump나 tcpshow 같은 네트워크 모니터링 도구를 이용하여 마스터와 에이전트간의 통신을 감시하여 에이전트 데몬이나 마스터 조절자(클라이언트) 프로그램을 실행시키는 시스템을 찾아낼 수 있다.

4.결론 및 향후연구

Loki와 같은 비밀통로의 존재가 야기하는 보안 문제의 심각성을 감안하면, 이 비밀통로를 없애는 유일한 확실한 방법은 네트워크에 들어오는 모든 ICMP_ECHO를 모두 거부하는 방법 뿐이다. 하지만 ICMP패킷을 거부는 말처럼 간단하지 않다. 특히 대규모인 네트워크의 경우는 사실상 불가능한 이론적인 방법에 불과할 것이다. 또한 이 비밀통로는 다른 프로토콜에서도 존재가 가능하다. 현대사회의 가장 큰 변혁은 인터넷을 중심으로 하는 정보구조의 구축이다. 지구를 하나로 묶는 거대한 네트워크를 통해 쉴새없이 이동하는 정보의 흐름 이는 또 하나의 세계를 만들어 가는 원동력이기도 하다. 그러나 이흐름 안에

안전이라 함은 사이버 세계를 안전하게 보호 하기 위한 기술 즉 보안인 것이다. 때문에 시스템 관리자는 부지런해야 한다. 관리자의 보안 의식이 결여된 상태에서는 완벽한 시스템 설계 및 구현이 있더라도 비밀통로와 같은 존재가 드러내기 마련이다. DDoS 공격에서 마스터 시스템과 에이전트 시스템으로서 이용당하지 않기 위해서는 주기적인 점검과 모니터링을 통한 패킷분석, 취약점과 관련된 권고안이나 패치를 확인하도록 해야 한다. 향후 연구 방향으로는 DDoS 공격에 대응할 수 있는 도구의 개발있어 여러 프로토콜에서의 존재가능한 비밀통로를 찾아 낼 수 있는 연구가 계속되어야 할 것이다.

참고문헌

[1] Distributed Denial of Service Tools, http://www.cert.org/incident_notes

[2] Result of the Distributed-System Intruder Tools Workshop, http://www.cert.org/reports/dsit_workshop.pdf

[3] Analysis of trin00, bugtra@securityfocus.com

[4] The Stacheldraht distributed denial of service attack tool, http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.

[5] 정진욱, 변옥환, 김병기, "TCP/IP Illustrated", 진영사,1999.