DoS 공격에 대비한 PAM 기반 사용자 프로세스 제한 기법

이재웅* · 정성재** · 배유미** · 장래영* · 소우영*

*한남대학교 컴퓨터공학과, **(주)엔버

Limiting user process method based on PAM against DoS attacks

Jae-Ung Lee* · Sung-Jae Jung** · Yu-Mi Bae** · Rae-Young Jang* · Woo-Young Soh*

*Hannam University, **Enber Co., Ltd

E-mail : leejaeung1990@gmail.com, posein@naver.com, yumidw@hanmail.net, jangraeyoung@hnu.kr, wsoh@hnu.kr

요 약

최근 남북관계 갈등의 골이 깊어지면서 북한의 사이버 테러(Cyber Terror) 가능성이 높게 제기되고 있다. 따라서 사이버 테러의 대표적 공격방법인 DoS(Denial of Service) 공격이 사회적으로 이슈(Issue)가 되고, 이에 따라 정보 보안에 대한 관심 또한 높아지고 있다.

DoS 공격의 다양한 유형 중에서 내부적인 DoS 공격 방법에는 디스크, 메모리, 프로세스 리소스의 고갈이 있다. 리눅스(Linux) 시스템에서 내부적인 DoS 공격에 대응하는 방법으로 PAM(Pluggable Authentication Module)을 이용한 사용자의 프로세스 제한을 꼽을 수 있다. 본 논문에서는 PAM을 이용하여 내부적인 DoS 공격에 의한 리소스(Resource) 고갈을 예방할 수 있는 기법을 제시하였다.

ABSTRACT

Considering that interkorean relations got worse and worse recently, cyber terror of North Korea has seriously become a possibility. Therefore, DoS(Denial of Service), a typical way of cyber terror, is becoming a big issue. Consequently, people are growing more and more interested in information security.

Internal DoS attacks, out of a variety of ways of Dos attacks, include disks and memories and shortages of process resources. PAM(Pluggable Authentication Module) is one of the ways of preventing internal DoS attacks in Linux system. This paper provides with a method to internally respond to dos attacks and efficiently prevent shortages of resources by utilizing PAM.

키워드

DoS, 프로세스(Process), 리눅스(Linux), 리소스(Resource), PAM

Ⅰ. 서론

최근의 사이버 테러(Cyber Terror)는 과거의 금전적인 이득을 위한 공격과는 달리 국가의 핵심 시설을 공격하여 국가 전체를 혼란의 도가니에 빠트린다. 우리나라는 2011년 농협 인터넷뱅킹 마비사건, 2012년 중앙일보 신문제작 서버 해킹, 2013년 6개 방송·금융사의 전산망 마비, 2014년 한국수력원자력 해킹공격 등 매년 사이버 테러가 발생하고 있고, 피해규모는 점점 커지고 있다[1]. 아울러 최근 남북관계 갈등의 골이 깊어지면서 북한의 사이버 테러 가능성이 높게 제기되고 있다. 따라서 사이버 테러의 대표적 공격방법인 DoS(Denial of Service) 공격이 사회적으로 이슈(Issue)가 되고 이에 따라 정보 보안에 대한 관심 또한 높아지고 있다. DoS 공격은 사용자들에게 정상적인 서비스를 제공하지 못하게 하는 것을 목표로 하며 매우 다양한 공격 유형을 가지고 있다. DoS 공격은 짧은 시간에 시스템을 마비시키고, DoS 공격이 시작된 시스템을 정상화 시키는 것이 매우 어렵기 때문에 예방이 중요하다.

본 논문에서는 DoS 공격 유형을 분석하고, 리

눅스(Linux) 시스템을 기반으로 내부적인 DoS 공격 방법인 리소스(Resource) 고갈 공격 방법을 제시한다. 그리고 이 공격에 대응하는 방법으로 PAM(Pluggable Authentication Module)을 이용해 사용자 프로세스를 제한하여 DoS 공격에 의한 리소스 고갈을 예방할 수 있는 기법을 제시하고 결론을 맺는다.

II. DoS 공격 유형 분석

DoS 공격은 사용자들에게 서비스를 제공하지 못하게 방해하는 행위라고 정의할 수 있다. 따라서 DoS 공격은 한 가지의 유형이 아닌 매우 다양한 유형을 가지고 있다. DoS 공격은 공격자의 위치에 따라 시스템 내부에서 내부 리소스에 직접적으로 공격을 하는 내부에서의 공격과 시스템 외부에서 네트워크를 통해 간접적으로 공격하는 외부에서의 공격으로 분류 할 수 있다[2].

표 1. DoS 공격이 시스템에 미치는 영향

DoS 공격	시스템에 발생하는 영향
파괴 공격	디스크, 데이터, 시스템의 삭제 또는 변조
시스템 리소스 고갈 공격	CPU, 메모리, 디스크의 부하로 인한 리소스 고갈
네트워크 리소스 공격	불필요한 패킷 유발로 인한 네트워크 대역폭 고갈

내부에서의 DoS 공격은 시스템에 계정을 가지고 있는 사람이 시스템의 리소스를 고갈 시키는 방법이 대표적이다. 이 방법은 외부에서의 공격에 비해 단순하지만, 시스템 내부에 계정을 가지고 있어야 한다는 단점이 있어 외부에서의 공격보다 위험성이 낮다고 판단하는 경향이 있다. 하지만 간단한 스크립트 몇 줄로 공격이 가능하고, 루트 권한을 가진 사용자가 아닌 일반 사용자가 시스템을 마비시킬 수 있기 때문에 결코 무시할 수 없다[3].

표 2. 내부에서의 DoS 공격 유형

외부에서의 DoS 공격	공격 유형
디스크 고갈 공격	파일을 생성하고, 파일의 크기를 계속 증가시켜 디스크 리소스를 고갈 시키는 공격이다.
메모리 고갈 공격	프로세스가 사용하는 메모리의 크기를 계속 확장하여 실제 메모리뿐만 아니라 가상메모리인 스왑까지 모두 고갈시키는 공격이다.
프로세스 고갈 공격	프로세스를 계속 생성하여 시스템의 프로세스 테이블을 고갈시키는 공격이다.

외부에서의 DoS 공격은 네트워크를 사용하여 시스템의 각종 프로토콜의 보안 취약점을 통해 공격하는 공격방법으로 내부에서의 DoS 공격과는 다르게 복잡하고 고도의 기술을 필요로 한다[4].

표 3. 외부에서의 DoS 공격 유형

외부에서의 DoS 공격	공격 유형
Ping of Death	Ping을 이용하여 ICMP 패킷을 비정상적으로 크게(65,535 bytes)만드는 것이다. 비정상적인 패킷은 네트워크를 통해 라우팅되어 공격 대상에 도달하는 동안 세그멘테이션(Segmentaion)화되고 공격 대상 시스템은 세그멘테이션 된 패킷을 모두 처리해야 하기 때문에 과부하가 걸리게 되어 정상적인 서비스를 제공할 수 없다.
UDP Flooding	소스 주소가 스푸핑(Spoofing)된 시스템에서 UDP 패킷을 공격 대상 시스템에 대량 전송하여 리소스(네트워크 대역폭)를 고갈시키는 공격이다.
TCP SYN Flooding	짧은 시간에 대량의 SYN 패킷을 보내 리소스(접속 가능한 공간)를 고갈시킴으로써 다른 사용자의 접속을 막는 공격이다.
Teardrop Attack	시퀀스 넘버(Sequence Number)를 중복되고 손실되게 하여 세그멘테이션 된 패킷을 재조합하지 못하도록 하여 과부하를 발생 시키는 공격이다.

Land Attack	발신지 주소(Source IP Address)를 도착지 주소(Destination IP Address) 속여 패킷이 외부로 나가지 않고 자신에게 되돌아오게 만드는 공격으로 SYN Flooding처럼 리소스(접속 가능한 공간)을 고갈시키는 것뿐만 아니라 CPU 부하까지 발생시킨다.
Smurf Attack	발신지 주소를 공격 대상 IP로 위장하여 ICMP Request 패킷을 브로드캐스트를 통해 다수의 시스템에 전송하면 ICMP Echo Reply 패킷이 공격 대상 IP로 전송되어 공격 대상 시스템에 과부하가 걸리게 된다.
Mail Bomb	Mail Bomb는 폭탄 메일이라고 부르는 것으로 다량의 메일을 전송하여 메일 서버의 리소스(디스크 공간)를 고갈시킴으로써 더 이상의 메일 수신이 불가능하게 만드는 공격이다.

III. 리눅스 시스템 구현

DoS 공격을 분석한 결과 DoS 공격은 짧은 시간에 시스템을 마비시키고, 마비된 시스템은 정상화 하는 것이 매우 어렵기 때문에 예방하는 것이 중요하다.

리눅스 시스템에서 DoS 공격에 의한 리소스 고갈을 예방하는 방법으로 PAM을 이용해 사용자 프로세스를 제한하는 것이 대표적이다. PAM이란 응용프로그램이 사용자를 인증하고, 서비스에 대한 엑세스를 제어하는 모듈이다. PAM은 /etc/security/limits.conf를 이용해 root 권한으로 vi편집기 등으로 해당 파일을 직접 설정하면 사용자 프로세스를 제한할 수 있다.

limits.conf의 형식은 다음과 같이 4개의 필드로 구성되어 있다.

표 4. limits.conf의 형식

<domain> <type> <item> <value>

<domain>필드는 username 또는 groupname을 명시하고 groupname는 앞에 @를 붙인다.

<type> 필드는 hard와 soft가 있고 hard는 root의 권한을 가진 사람이 강제적으로 제한하는 값을 말하고 soft는 hard로 정해진 값 내에서 일반 사용자가 제한하는 값을 말한다.

<item>필드는 core, data, fsize, memlock, nofile, rss, stack, cpu, nproc, as, maxlogins, maxsyslogins, priority, locks, sigpending, msqqueue, nice, rtprio 등 다양한 종류가 있다. 내부적인 DoS공격을 예방하기 위한 리눅스 시스템 구현을 위해 fsize, rss, nproc를 사용하여 시스템을 구현한다.

예를 들어 root 권한으로 /etc/security/limits.conf에 그림 1 처럼 설정하면 root를 제외한 사용자의 최대 파일크기를 102400KB, 메모리 크기를 102400KB, 프로세스 개수를 30개로 제한하게 되면 내부적인 DoS 공격이 발생하더라도 시스템이 마비되지 않는다.

```
#<domain>      <type>  <item>         <value>
#

#*              soft    core           0
#*              hard    rss            10000
#@student       hard    nproc          20
#@faculty       soft    nproc          20
#@faculty       hard    nproc          50
#ftp            hard    nproc          0
#@student       -       maxlogins      4

*               hard    fsize          102400
*               hard    rss            102400
*               hard    nproc          30
# End of file
```

그림 1. 리눅스 시스템 구현

IV. 시스템 보안 평가

내부적인 DoS공격에 대비한 리눅스 시스템을 구현하여 디스크, 메모리, 프로세스 리소스를 고갈시키는 가상의 DoS 공격을 발생시켜 시스템의 마비 여부를 확인하여 시스템의 보안을 평가 할 수 있다. 다음 그림 2는 diskattack이라는 파일을 생성하여 파일의 크기를 계속 증가시키는 디스크 리소스 고갈의 예이다.

```
[Lee@www ~]$ cat dosdisk.c
#include <unistd.h>
#include <sys/file.h>
void main()
{
        int fd;
        char buf[100];
        fd = creat("diskattack",0777);
        while (1) {
                write(fd,buf,sizeof(buf));
        }
}
```

그림 2. 디스크 고갈 공격

하지만 PAM을 통해 최대 파일의 크기를 102400KB로 제한하였기 때문에 시스템은 마비되지 않고 정상적으로 작동한다. 관련 정보는 그림 3처럼 실시간으로 디스크 리소스를 확인하는 명령어인 watch df을 이용할 수 있다.

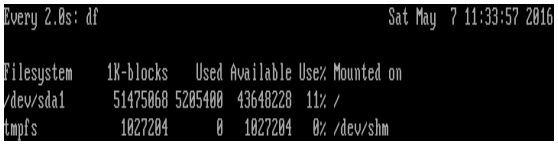

그림 3. 디스크 고갈 공격 예방

다음 그림 4는 malloc()함수를 통해 메모리 할당을 계속해서 수행하는 메모리 리소스 고갈의 예이다.

```
[Lee@www ~]$ cat dosmemory.c
#include <stdio.h>
void main()
{
        char *m;
        while(1){
                m = malloc(1000);
        }
}
```

그림 4. 메모리 고갈 공격

하지만 PAM을 통해 최대 메모리 크기를 102400KB로 제한하였기 때문에 시스템은 마비되지 않고 정상적으로 작동한다. 관련 정보는 그림 5처럼 실시간으로 관련 리소스를 확인하는 top 명령을 이용할 수 있다. 참고로 리눅스 커널 2.4.30이상 버전에서는 PAM을 사용하지 않아도 특정 프로세스의 메모리 점유율이 높아지면 시스템이 마비되면서 자동으로 해당 프로세스를 종료시킨다.

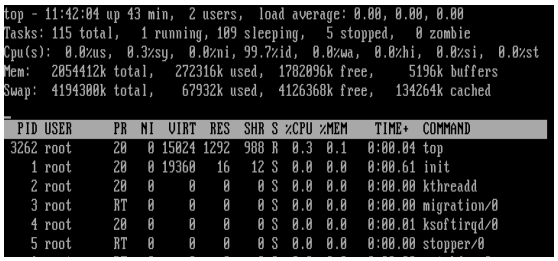

그림 5. 메모리 고갈 공격 예방

다음 그림 6은 fork()함수를 통해 프로세스를 계속해서 생성하는 프로세스 리소스를 고갈시키는 예이다.

```
[Lee@www ~]$ cat dosprocess.c
#include <unistd.h>
void main()
{
        while(1)
                fork();
        return 0;
}
```

그림 6. 프로세스 고갈 공격

하지만 PAM을 통해 프로세스 개수를 30개로 제한하였기 때문에 시스템은 마비되지 않고 정상적으로 작동한다. 관련 정보는 그림 7처럼 사용자의 프로세스 개수를 확인하는 명령어인 'pgrep -u username | wc -l'를 이용할 수 있다.

```
[root@www ~]# pgrep -u Lee | wc -l
30
[root@www ~]# _
```

그림 7. 프로세스 고갈 공격 예방

PAM을 사용하여 구현한 리눅스 시스템은 디스크, 메모리, 프로세스 리소스를 고갈시키는 가상의 DoS 공격을 통해 예방할 수 있음이 증명 되었다.

Ⅴ. 결론 및 향후 연구과제

사이버 테러의 발생 빈도가 높아지고, 피해가 커지고 있는 만큼 DoS공격의 예방이 중요하다. DoS 공격이 발생된 후의 대응도 중요하지만 DoS 공격을 예방하기 위해서는 DoS 공격을 분석하고, 예방을 우선으로 하는 시스템 구현이 가장 중요하다. 본 논문에서 제시한 방법을 활용하면 내부에서 발생하는 DoS 공격을 예방하여 사이버 테러의 피해를 줄일 수 있으리라 여겨진다. 아울러 리눅스 커널 2.4.30이상 버전의 환경에서는 PAM을 통한 최대 메모리 제한이 불가능한 문제점이 발견되었다. 리눅스 커널 2.4.30 이상 버전의 환경에서 사용자의 최대 메모리 점유율을 제한하는 방법에 대한 추후 연구가 필요할 것으로 판단된다.

참고문헌

[1] 경남신문, http://www.knnews.co.kr/news/articleView.php?idxno=1178155, 2016년 4월 21일.

[2] 정성재, 배유미, "리눅스 마스터 1급 정복하기", 북스홀릭 퍼블리싱, pp. 563-566, 2015년.

[3] 금영탁, "DoS 攻擊패턴의 分析을 통한 인터넷 서버保安 方案", 영남대학교 석사학위논문, 영남대학교, pp. 12-16, 2003.

[4] 조성현, 이택규, 이선우, "TCP/IP 네트워크 프로토콜의 DoS 공격 취약점 및 DoS 공격사례 분석", 정보보호학회지, 제24권 제 1호, pp. 45-52, 2014.