4 ICLICE 2016-66 Jae-Ung Lee

Denial of Service Prevention Techniques on IoT Home Servers

Jae-Ung Lee[a] , Rae-Young Jang[a] , Sung-Jae Jung[b], Yu-Mi Bae[b], Woo-Young Soh*[a]
[a]Department of Computer Engineering, Hannam University,
70 Hannam-ro, Daedeok-gu, Daejeon, Korea
[b]Research Institute, ENBER Co., Ltd, Neungdong-ro, Gwangjin-gu, Seoul, Korea
*Corresponding Author: wsoh@hnu.kr

ABSTRACT

The so-called internet of things (IoT) technology that connects physical objects to internet network and provides with the cutting edge intelligent services has recently been attracting a lot of attention. However, this connectivity draws many problems because the serious risk of cyber-attacks has been moving further to the real world situations as physical objects become connected to internet. This paper will analyse the types of Dos attack techniques which are considered as a typical threat to IoT and provide with a method to prevent DoS attacks by utilizing iptables(firewalls) and PAM (Pluggable Authentication Modules) in Linux which serves as the operating system of home servers.

Keywords: Internet of Thing, IoT, Linux, Server, Denial of Service, PAM, iptables

Introduction

With the outstanding development of IoT(Internet of Things), a plethora of areas such as electronic devices, medical treatments, transportation have begun using this technology. The internet of things (IoT) is network connectivity between physical objects and the internet, which provides with cutting edge intelligent services. Especially, the IoT technology in home appliances has recently been drawing people's attention. This is because it allows users to control all the home appliances, such as domestic surveillances or automatic doors or any kind of electronic devices, by connecting all of them with IoT home server from outside of the home. However, at the same time, this connectivity draws a lot of problems because there is a serious risk of cyber-attacks. This risk has been steadily increasing as physical objects become connected to internet. Furthermore, even though electronic devices with IoT are as advanced as they can prevent security threats and the communications between those devices are standardized, The devices are not very advanced in terms of their specifications, making it hard to apply security systems. In addition, unstandardized communications are being to be pointed out. Moreover, the users of IoT devices are not interested in cyber security. According to a study by HP in 2014, 70 percent of total IoT devices deliver data using unlocked networks. This suggests anyone can easily attack other people's home servers and the attacked devices cannot be controlled by its owners if the server becomes paralyzed. Therefore, it's really important to protect home servers from possible attacks in advance. This paper will analyze the types of Dos attack techniques which are considered to be typical threats to IoT. The paper will also provide a method to prevent DoS attacks by utilizing iptables(firewalls) and PAM(Pluggable Authentication Modules) in Linux which serves as the operating system of home servers.

DoS Attack Techniques

A denial-of-service (DoS) attack is an attempt to interrupt or suspend services of a host connected to the Internet. Thus, there is a variety of attack techniques. The techniques are divided depending on the location of the attacker. One type of attacks is when the attacker directly affects inner resources by attacking from inside of the system and the other one is the external attack which is indirectly conducted by the networks outside of the system.

Table 1
The impact of DoS attacks on the system

DoS attack	The impact on the system
Destruction attack	Delete or modulation of Disks, Data or Systems
Exhausting System Resources	Resource shortage due to CPU/Memory/Disk overload
Network resource attack	Network frequency shortage due to the appearances of unnecessary packets

The internal DoS attack is relatively simpler than an external DoS attack. However, considering that you need to access to the inside of the system, it is regarded as less risky than external DoS attacks. However, the internal Dos attack is critical because it can start simply by typing a few commands and paralyze the system with not only root-authentication but also general-authentication.

Table 2
Types of internal DoS attacks

Type	Details
Exhausting Disk space	Exhausting disk space by constantly making files and increasing the size of the files.
Exhausting Memory Space	Exhausting not only the actual memory capacity but also Swap, the virtual memory, by upsizing memory.
Exhausting Process	Exhausting the process table by constantly making the processes.

The external DoS attack is a conduct of operation that attacks through the vulnerability of protocols by using networks and it needs complex and a high level of techniques which is more than the internal DoS attacks require.

Table 3
The External DoS Attack

Types	Details
Ping of Death	A type of attack on a computer system that maximize the ICMP packet length as large as 65,536 bytes with the use of Ping. The abnormally large length of packet is routed and segmentalized while it reaches to the aim of attack. The system has to deal with all the segmentalized packets, which causes overload.
UDP Flooding	In a system of which IP address is spoofed, UDP flooding exhausts resources (network frequency) by sending a large number of UDP packets to the victim.
TCP SYN Flooding	A type of attack that sends a large amount of SYN packets to the victim in a very short period of time, exhausting resources (available space).
Teardrop Attack	A type of attack that causes overload by duplicating or damaging Sequence number and then hindering the system from rebuilding the segmentalized packets.
Land Attack	A type of attack that causes the machine to reply to itself continuously by disguising the source IP address as the destination IP address. It not only exhausts available space like SYN flooding but also makes the CPU flooded with traffic
Smurf Attack	It makes the victim's computer flooded with traffic by disguising source IP address as the IP address of the victim and then sending ICMP packets to a lot of systems. A large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address.
Mail Bomb	A type of attack that exhausts disk space of the mail server by sending a large amount of mails

System Implementation

As a result of the analysis of DoS attacks, DoS attacks paralyze the victim system in a very short of period of time and it is very difficult to normalize the attacked system. Thus, it's important to prevent the initial attacks. When it comes to internal DoS attacks, limiting the user process with PAM is regarded as a typical way to prevent resource depletion. PAM is a module in which an application programs identifies the users and take control of the access to the service.

You can limit the user process with PAM. To change the limit, you can edit /etc/security/limits.conf file as root and directly edit the files by using the editing system such as vi editor. The form of limits.conf consists of four fields as below.

Table 4
The format of the limits.conf

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

Table 5
Domain field

<domain>	A username A groupname, with @group syntax. This should not be confused with netgroups The wildcard *, for default entry. The wildcard %, for maxlogins limit only. An uid range specified as <min_uid>:<max_uid>. A gid range specified as @<min_gid>:<max_gid>. A gid specified as %:<gid> applicabled to maxlogins limit only.

Table 6
Type field

hard	For enforcing hard resource limits.
soft	For enforcing soft resource limits.

Table 7
Item Field

core	Limits the core file size (KB)
data	Maximum data size (KB)
fsize	Maximum filesize (KB)
memlock	Maximum locked-in-memory address space(KB)
nofile	Maximum number of open files
rss	Maximum resident set size (KB)
stack	Maximum stack size (KB)
cpu	Maximum CPU time (minutes)
nproc	Maximum number of processes
as	Address space limit(KB)
maxlogins	Maximum number of logins for this user except for this with uid=0
maxsyslogins	Maximum number of all logins on system
priority	The priority to run user process with
locks	Maximum locked files
sigpending	Maximum number of pending signals
msgqueue	Maximum memory used by POSIX message queues
nice	Maximum nice priority allowed to raise to values: [-20,19]
rtprio	Maximum realtime priority allowed for non-privileged processes

For instance, in case of Figure 1, to change the limit, edit /etc/security/limits.conf file as root and set it as Figure 1. Then the system won't get paralyzed because the memory capacity gets limited to 102400KB and the number of process gets limited to 30.

```
#<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
```

Figure 1: Linux system implementation for the internal DoS attack

It is commonly used to set up a firewall by using iptables in order for the Linux system to prevent external DoS attacks. iptables is a packet filtering tool used for firewall construction. iptables does not directly conduct packet filtering. Rather, a module called netfilter, included in a kernel, conducts the filtering operations.

Table 8
Filter tables and chains

INPUT	A chain involved in packet filtering and strategies for firewall protection. It manages access to the firewall.
OUTPUT	A chain taking control of packet. It hinder systems outside from firewall from accessing to it.
FORWARD	A chain taking charge of the packet passing through the linux system. It's used in order for a network to be connected to another network by using iptables.

Table 9
Major actions

Action	Details
-N	Make a new user-defined chain
-X	Get rid of empty chains, provided you don't get rid of basic chain.
-P	Set a basic chain policy.
-L	List the basic chain rule.
-F	Get rid of the rule from the chain
-Z	Make the count of packet and bite of all the rules in the chain 0
-A	Add new rule to the chain. It will be registered as the last rule in the chain.
-I	Add the rule of the chain to the forepart. You can add it

	specifically to some places by using rule numbers.
-R	Exchange the rules of the chain.
-D	Get rid of the rule of the chain.

Table 10
Major match extensions

Action	Details
-s	Source specification. Address can be either a network IP address or matching domain, a network mask.
-d	Destination specification. Address can be either a network IP address or matching domain, a network mask.
-p	Matching a specific protocol. Using titles like TCP, UDP, ICMP, Ignoring case Protocol all will match with all protocols and is taken as default when this option is omitted.
-i	Matching with an interface via which a packet is received.
-o	Matching with an interface via which a packet is going to be sent.
!	It means 'not' and be used to exclude a specific matching.
-m	A matching option used to subtly control.
--state	Matching with the connection states. Using INVALID, ESTABLISHED, NEW, RELATED
--string	Matching with specific patterns.

Table 11
Extra options

Action	Details
-n	Numeric output. It will be printed in numeric format.
-v	Verbose output. Detailed information on the rule or rules including the number of packets or bite is printed.
--line-number	When listing rules, add line numbers to the beginning of each rule, corresponding to that rule's position in the chain.

Table 12
Major targets

Action	Details
ACCEPT	Letting the packet through. Using the original routing
DROP	Dropping the packet on the floor when nothing is conducted.
LOG	Recording packet delivered to syslog. Generally saved in /var/log/messages

REJECT	Rejecting the packet and simultaneously delivering response pakets. In case of TCP, messaging reset packet In case of UDP,messaging ICMP Port Unreachable
RETURN	Keep conducting packet operations in the chian.

For example, in order to prevent an external DoS attack from causing ICMP flooding, you make a chain called ICMP by typing Table 13 into the terminal. And then you send the packet related to ICMP protocol to the ICMP chain and drop the icmp echo request.

Table 13
ICMP Flooding prevention technique

```
# iptables –N ICMP
# iptables –A INPUT –p icmp –j ICMP
# iptables –A ICMP –p icmp –icmp-type echo-request –j  DROP
```

With the same purpose, you can use table 14 and set up a chain with the title of UDP. Then then send the packet related to UDP protocol to UDP chain and add a policy where packets are dropped when more than 10 of them per second are brought into it. Record this as “UDP FLOOD” in the UDP chain.

Table 14
UDP Flooding prevention technique

```
# iptables –N UDP
# iptables –A INPUT –p udp -j UDP
# iptables –A UDP –p udp –dport 80 –m recent –update –seconds 1 –hitcount 10 –j
drop
# iptables –A –UDP –j LOG –log-prefix “UDP FLOOD”
```

There are three TCP flooding prevention techniques here below as table 15.

Table 15
TCP Flooding prevention technique

iptables –A INPUT –p tcp –dport 80 –syn –m limit –limit 100/s –j ACCEPT Limit the allowed number of access per second.
iptables –A INPUT –p tcp –dport 80 –syn –m connlimit –limit –above 30 –j DROP Limit the allowed number of access per one IP adress.
iptables –A INPUT –p tcp –dport 80 –m recent –update –seconds 1 –hitcount 10 –j DROP Limit the allowed number of request from a specific IP address.

Finally, in order to cope with SSH random input attacks, insert Table 16 and make a chain named SSH.Next, send the packet accessing to the 22 port to SSH chain. If SSH access is attempted at 15 times per 60 seconds, add a policy to drop them and record the policy as "SSH Brute".

Table 16
TCP Flooding prevention technique

iptables –N SSH # iptables –A INPUT –p tcp –dport 22 –m state –state NEW –j SSH # iptables –A SSH –p udp –dport 22 –m recent –update –seconds 60 –hitcount 15 –j DROP # iptables –A SSH –j LOG –log-prefix "SSH Brute"

Thus, if you use the techniques like ICMP Flooding, UDP Flooding, TCP Flooding and the iptables commands against an SSH random input attack, your system wouldn't get paralyzed.

Conclusion

Even though IoT technology has come a long way, IoT security has lagged behind. Furthermore, the technology has shown its underlying weaknesses due to the technical problems of IoT devices and unstandardized skills. And it is suggested that the system gets paralyzed in a very short period of time and after the attack, it's very hard to normalize the system again. Thus it's very important to prevent the security threats in advance. If you utilize the PAM and iptables presented in this paper, you will prevent not only the internal DoS attacks but also external DoS attacks and ultimately reduce the damage from those attacks.

Acknowledgement

This work was supported by the Security Engineering Research Center granted by the Ministry of Trade, Industry and Energy.

References

Y. M. Bae, and S. J Jung, 2011. A study on the linux firewall, *Journal of Security Engineering*, 8(5), 599-610.

Sung-hyun Cho, Taek-kyu Lee, Seon-woo Yi, 2014. Case analysis of vulnerabilities and DoS attacks DoS Attacks of TCP / IP Network Protocol, *REVIEW OF KIISC*, 24(1), 45-52.

S. J. Jung, and Y. M. Bae, "Conquer Linux Master Class 1", BOOKSHOLIC Publishing, pp.563-566,(2015)

D. I. Yang, Information Security Introduction and Practice, 3th ed. Seoul, Korea: HANBIT Publishing, (2014)

United States Computing Emergency Readiness Team. (2009, November 4), *Understanding Denial-of-Service Attacks* [Web Log Post]. Retrieved from https://www.us-cert.gov/ncas/tips/st04-015/.

Netfilter "iptables" Project, *What is iptables?* [Internet Web Page]. Retrieved from http://www.netfilter.org/projects/iptables/