IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SKY SHIELD

[1]Krishna v s, [2]Prameeja Prasidhan

[1]Student, [2]Assistant Professor
[1]Computer Science Department,
[1]St Joseph's College(Autonomous),Irinjalakuda , India

Abstract: **DDoS stands for distributed denial of service attack. DDoS is a denial of service attacks, that is in DOS attacks requests are send from single node to a targeted node to deny its services. But in DDoS attacks the requests are send from multiple systems to single targeted node. The nodes that are in under control of the bot master are the zombies. Zombies are the vulnerable systems. The bot master sends commands to the zombies and simultaneous requests are send from these vulnerable systems to targeted systems. Sky Shield application is designed to detect these attacks and also it uses some prevention methods. We use a data structure for hashing. Sketch data structure uses unique IP address or QR code as key, because systems can be uniquely identified. The values of sketch data structure are the number of packets send. We know that in DDoS attacks, number of requests are send from bots. When simultaneous requests are send from nodes, we track each and every nodes requests and calculate sketch for each requests and also update it. Here we calculate the divergence between two sketches and based on observation flag mark it as malicious or genuine user.**

Index Terms - DDoS Attacks, Captcha, Sketch, Bloom Filtering, File Transfer

I. INTRODUCTION

In this paper we discuss about DDoS attacks. DDoS attacks are the denial of service attacks. In this type of attacks the command is given by the bot master to the nodes which are in under control of the bot master. These nodes sends requests to the targeted system to deny its services by exhausting its resources. Sky Shield application is used to detect these types of attacks. For detection we use captcha test. Captcha test is the challenge response. Captcha test can be used to detect the bots. We know that bots cannot recognize the images as well as it cannot type distorted letters and digits. We determine a number for the requests the nodes can send, if the number of requests send are more than the determined number we consider it as a malicious system. So this method can be used to determine the legitimate and malicious users. Next we concentrate on the behaviour of the systems. Consider the example of downloading the same file more than one time. We suspect the system based on the behaviour.

We know that DDoS attacks have number of nodes that accepts the commands of the bot master. So the targeted nodes as well as the nodes that are in under control of the bot master are also the victims of DDoS attacks. A data structure called sketch design is used to calculate the sketch. For the sketch design we use the key as unique IP address or QR code to identify the system uniquely. For sketch design we use hashing. The values are the number of packets send, bytes etc. by using sketch design we can calculate the divergence between number of requests send. When the divergence is calculated it is updated when new requests are send. When any rise in number of requests are found then it is marked as malicious. The another data structure called bloom filtering is used to distinguish between the legitimate and malicious systems.

II. ARCHITECTURE

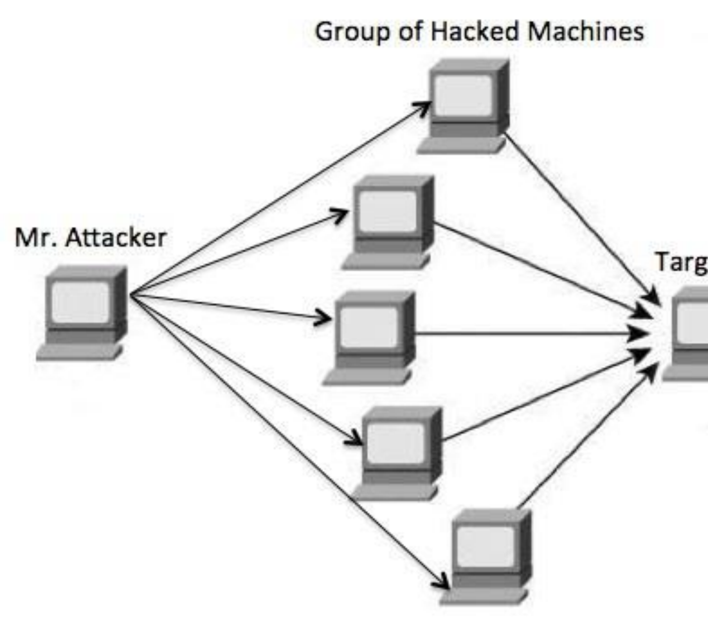

Fig:2.1

The above figure is the architecture for DDoS attacks. There is an attacker called the bot master who gives commands to the group of hacked machines. Hacked machines sends requests to the targeted machines simultaneously. This will lead to deny the services of a normal user. This is how DDoS attacks works. The aim of the attacker is to deny the services of a normal user by exhausting the resources.

III. EXISTING SYSTEM

In the existing system we suspect the systems based on the behavior of the system. When any misbehavior of the system is noticed then it is suspected. Consider the example of downloading the same file more than one time. Then we suspect the system based on its behavior. Next we have a static threshold value. We consider a static number that the number of requests a node can send. When the number of requests send by the node is more than the static number then we consider it as malicious system. Next is the challenge response. We use the captcha test to detect the bots. We know that bots cannot recognize the images as well as it cannot type the distorted letters and numbers.

IV. PROPOSED SYSTEM

In the existing system we have discussed about challenge response, behavioral analysis and static threshold. These three methods can be used to distinguish between legitimate and malicious users. But there are some limitations. We cannot distinguish systems effectively. So we use some methods to distinguish the legitimate and malicious systems accurately. These methods helps to detect the attacks quickly and effectively.

4.1Dectecting Vulnerable Systems

Vulnerable systems are in under control of the bot master. We know that bots cannot recognize images as well as it cannot type distorted letters and digits. Here we use challenge response captcha test. Captcha test is to determine whether the user is a human or a bot. captcha test is to prove human identity. This is an effective method to determine bots.

4.2 File Transfer

We can transfer files from one device to another. But this is possible only if the system enters the correct captcha code. For transferring the devices are connected using four options. We can connect devices either by using hotspot or by any existing network or by scanning QR code or by entering IP addresses if known. We can select files from our device. We set permissions for accessing device files.

4.3 Sketch Data Structure

We use hashing technique in sketch data structure. For hashing we take IP address or QR code to identify the system uniquely. The values of this structure will be number of requests send, bytes etc. since there will be huge traffic when number of nodes sends requests simultaneously. For storing these requests and retrieving it effectively we use hash data structure.

4.3.1 Algorithm for sketch data structure

1. Start
2. We pass the key as the IP address of the packet from the receiver.
3. We get the values as number of packets send, request made for each connection.

4.4 Filtering

Filtering is a method that effectively distinguish between legitimate user and malicious systems. We store the IP addresses of trusted systems in database. This will help to easily communicate with trusted clients. For filtering we use data structure. In this method we make use of captcha test for filtering. In the captcha test if the system is detected as bot, that is , if the system enters incorrect captcha code then the IP address of the vulnerable systems are stored in the black list and the IP address of the legitimate users are stored in white list. So there are white list and black list table to store legitimate and malicious systems IP address.

4.4.1 Algorithm for bloom filtering

1. Start
2. The user first go for captcha test.
3. If the user enters the correct captcha code, the IP address of that system is stored to the whitelist table in database. Otherwise go to step 4.
4. If the user gives incorrect captcha code, the IP address of that system is stored to the blacklist table in the database.

4.5 Rise in request

Here we make use of sketch design to calculate the rise in request. That is, we calculate the divergence between the requests send. We have already discussed about static threshold. When there is a rise in request is found, then it is treated as malicious system. That means if the number of request send by the node is more than the static value, the rise in number of request is calculated. And sketch is updated at each time request is send. This is how divergence is calculated.

4.6 Tracking IP address

This is to track the IP address of the attacker. We can make use of captcha test to find the attacker IP address. If the incorrect captcha code is given then the IP address is stored in black list. Whenever new systems are connecting compare it with the IP addresses in black list. If any match occur then deny the connection with that system. When the IP address is tracked we block that system. This will help systems to prevent from attacks.

V. BLOCK DIAGRAM

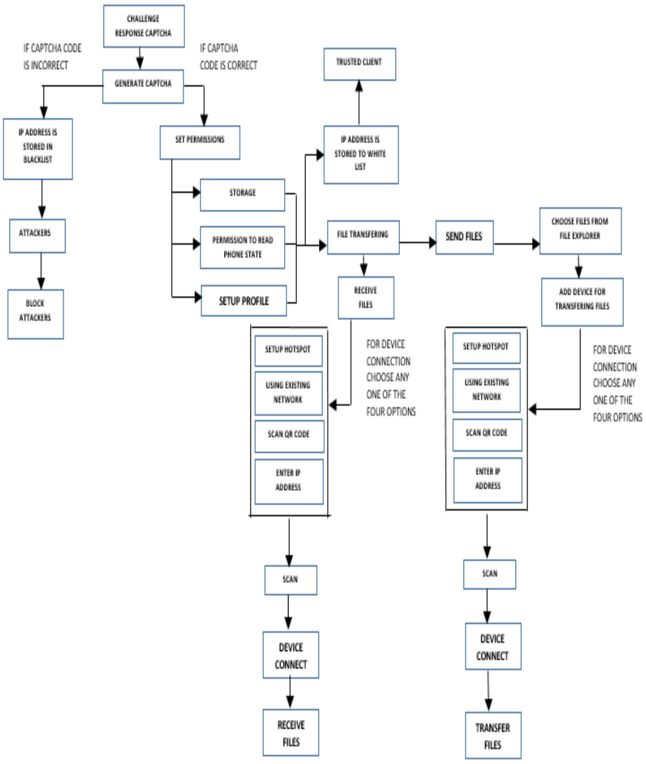
CHALLENGE RESPONSE CAPTCHA
IF CAPTCHA CODE IS INCORRECT
IF CAPTCHA CODE IS CORRECT
GENERATE CAPTCHA
TRUSTED CLIENT
IP ADDRESS IS STORED IN BLACKLIST
SET PERMISSIONS
IP ADDRESS IS STORED TO WHITE LIST
STORAGE
ATTACKERS
PERMISSION TO READ PHONE STATE
FILE TRANSFERING
SEND FILES
CHOOSE FILES FROM FILE EXPLORER
BLOCK ATTACKERS
SETUP PROFILE
RECEIVE FILES
ADD DEVICE FOR TRANSFERING FILES
SETUP HOTSPOT
USING EXISTING NETWORK
SCAN QR CODE
ENTER IP ADDRESS
FOR DEVICE CONNECTION CHOOSE ANY ONE OF THE FOUR OPTIONS
SETUP HOTSPOT
USING EXISTING NETWORK
SCAN QR CODE
ENTER IP ADDRESS
FOR DEVICE CONNECTION CHOOSE ANY ONE OF THE FOUR OPTIONS
SCAN
DEVICE CONNECT
RECEIVE FILES
SCAN
DEVICE CONNECT
TRANSFER FILES

FIG 5.1: BLOCK DIAGRAM

V1. CONCLUSION

As the network traffic increases attacks like denial of services also increases. Cyber security has many issues in security. To overcome this problem we design an application called Sky Shield. Sky Shield is an application which helps to detect attacks. It make use of challenge response, sketch design and bloom filter design to overcome these problems. These techniques are effective as well as it quickly detects the vulnerable systems. This application also helps to prevent systems from attacks. When the attack is detected we try to stop servicing the attackers system.

REFERENCES

[1] https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
[2] https://ieeexplore.ieee.org/document/8055579
[3] https://en.wikipedia.org/wiki/CAPTCHA
[4] HTTP://LKOZMA.NET/BLOG/SKETCHING