EVALUATION OF SINGLE GATE SECURED AUTHENTICATION MODEL TO PREVENT THE CLOUD BASED SERVER FROM DISTRIBUTED DENIAL OF SERVICE ATTACKS

M. Manoj Kumar
Department of Computer Science Engineering, TKM College of Arts and Science, India

Abstract

Distributed Denial of Service (DDoS) attacks are attacks on computer systems (network resources or communication channels) that make them inaccessible to legitimate users. DDoS attacks involve sending a large number of simultaneous requests from one or more computers on the Internet towards a specific resource. If thousands, tens of thousands or millions of computers start sending requests to a particular server (or network service) at the same time, the server will fail or the bandwidth of the communication channel for this server will be insufficient. In both cases, Internet users cannot access the attacked server, or even all servers and other resources connected through the blocked communication channel. Many experts may be aware that there are specialized solutions to protect against DDoS attacks, which include traffic anomaly detection, traffic profiling and attack profiling, and sequential dynamic multistage traffic filtering. But sometimes more effective measures can be taken to suppress DDoS attacks through existing mechanisms of the data transmission network and its administrators.

Keywords:

DDoS, Attacks, Computer Systems, Network Resources, Communication Channels

1. INTRODUCTION

DDoS attacks can be launched against any resource on the Internet. The greatest damage caused by DDoS attacks is received by companies directly related to business on the Internet - banks (providing Internet banking services), online stores, trading platforms, auctions and other activities, operation and performance of which the representative office on the Internet (travel agencies, airlines, hardware and software manufacturers, etc.) depends [1]. DDoS attacks are regularly launched against the resources of global IT giants like IBM, Cisco Systems, Microsoft and others [2]. Massive DDoS attacks have taken place against eBay.com, Amazon.com, many famous banks and companies. The main objectives of DDoS attacks are to gain profit (directly or indirectly) through intimidation and extortion, or to pursue political interests, aggravation and revenge [3]. The most popular and dangerous way to launch DDoS attacks is the use of botnets (BotNets). A botnet is a collection of computers on which special software bookmarks (bots) are installed; Translated from English, a botnet is a network of bots [4-5]. Bots are usually created by hackers individually for each botnet and have the main purpose of sending requests to a specific resource on the Internet through botnet command and command received from the control server [6]. A botnet control server is managed by a hacker, or someone who has purchased a botnet from a hacker and is capable of launching a DDoS attack.

Bots are distributed on the Internet in different ways, as a rule - by attacking computers with vulnerable services and installing software bookmarks on them, or by tricking users and forcing them to install bots under the guise of offering other services or completely harmless or functional software [7]. Effective operation there is many ways to distribute bots, new Ways are constantly being discovered.

If the botnet is large enough - tens of thousands or even hundreds of thousands of computers - sending legitimate requests from all these computers simultaneously to a specific network service (for example, a web service on a specific site) can lead to exhaustion. Service or server resources or exhaust communication channel capabilities. In any event, the Service will not be available to the Users and the Owner of the Service will suffer direct, indirect and reputational losses. If each computer does not send a single request, but sends tens, hundreds or thousands of requests per second, the strike of the attack increases many times, this makes it possible to disable the most productive resources or communication channels [8]. Some attacks are launched in more innocuous ways. For example, a flash mob of users of certain forums will, by contract, initiate pings or other requests from their computers toward a specific server at a specific time. Another example is placing a link to a website on a popular web resource, which causes users to visit the target server. A fake link (it looks like a link to a resource, but actually refers to a completely different server) connecting to the website of a small company, but if it is hosted on popular servers or forums, can cause such an attack, the arrival of unwanted visitors to this site. The last two types of attacks are in order Servers at organized hosting sites rarely lead to downtime.

2. LITERATURE REVIEW

A feature of DDoS attacks is that they contain many simultaneous requests, each of which is individually very legitimate, and these requests are sent by computers (infested with bots), which may belong to very ordinary real or potential users [1]. Attacked service or resource. Therefore, it is very difficult to properly detect and filter the requests that constitute a DDoS attack using standard methods. Standard systems class IDS / IPS (intrusion detection / prevention system - a system for detecting / preventing network attacks) cannot find corpus delinquency in these requests, unless they perform a qualitative analysis of traffic, they will not understand that they are part of an attack [2]. Even if they figured it out, filtering unwanted requests is not so easy - standard firewalls and routers filter traffic based on clearly defined access lists (control rules) and don’t know how to modify a specific attack profile [3]. Firewalls can adjust traffic flows based on criteria such as source addresses, network services used, ports, and protocols. But ordinary [4] Internet users participate in a DDoS attack; they send requests using very common protocols - the telecom operator will block everyone and everything. Then he will stop providing communication services to his subscribers and stop providing access to the network resources he serves, in fact, the attacker is trying to reach [5].

3. PROPOSED MODEL

In some special cases, there are certain mechanisms and tricks that allow DDoS attacks to be suppressed. Some can be used only if the data transfer network is built into the equipment of a particular manufacturer, while others are more or less universal. The company recommends network foundation security, which includes the control plane, management plane, and data plane. SNMP v3 provides security measures, while SNMP v1 practically does not, and SNMP v2 only partially - the default community values must always be changed;

- Different values should be applied to public and private society;
- The telnet protocol sends all data including login and password in clear text (if the traffic is intercepted, this information can be easily retrieved and used), it is always recommended to use the ssh v2 protocol instead;
- Likewise, use https instead of http for hardware access Strong controls on hardware access including adequate password policy, centralized authentication, authorization and accounting (model AAA) and local authentication for redundancy.

Control of allowed connections to the source addresses using access control lists; disables unused services, many of which are enabled by default (or were forgotten to disable after detecting or configuring the system); Equipment resource utilization monitoring. It is worth dwelling on the last two points in more detail. Certain services enabled by default or forgotten to turn off after configuration or detection of hardware can be used by cybercriminals to circumvent existing security rules. Naturally, before disabling these services, you should carefully analyze the lack of need for them in your network. This option is only for testing local host. That is why:

- It illegal against other people sites, and for this they are already sitting in the West (which means they will soon be jailed here as well).
- The flooding address will be calculated quickly, they will report to the provider, who will alert you and remind you of the first thing
- In low-bandwidth networks (i.e., all homes), the little thing won’t work. Everything is the same in the TOR network.
- If you set it up right, you’ll clog up your communication channel faster than harm someone. So this is the correct option when punching a boxer, not the other way around. The option with a proxy follows the same principle: nobody wants a flood from your side.

It is desirable to monitor the utilization of equipment resources. This is, firstly, to timely notice the congestion of individual network elements and take measures to prevent the accident, and secondly, to detect DDoS attacks and anomalies, if not provided by special mechanisms.

Monitoring can be carried out manually (periodic monitoring of the status of equipment), but it is better to do this with special network monitoring or monitoring systems. Remotely induced black holes are used to dump (delete, send anywhere) traffic entering the network by diverting this traffic to special null 0 interfaces. This technology is recommended for use at the network edge to eliminate DDoS attack traffic as it enters the network. A limitation (and significant) of this method is that it applies to all traffic destined for a specific host or hosts targeted for attack. Thus, this method can be used in cases where one or several hosts are subjected to a massive attack, which causes problems not only for the attacked hosts, but also for other subscribers and the operator network as a whole. Therefore, the entire DDoS protection cycle consists of the following key stages:

- Traffic Control Characteristics Training (Profile, Basic Learning)
- Detection of Attacks and Contradictions
- Diversion of traffic
- Filtering (mitigating) traffic to suppress attacks
- Injecting traffic back into the network and forwarding it to the destination (injection).

Points (sections of the network) are selected, traffic analyzed to identify anomalies. Depending on what we are protecting, these points may include telecom operator peer-to-peer links with upstream operators, connection points of downstream operators or subscribers, channels to connect data centers to the network. Special detectors analyze the traffic at these points, create (analyze) the traffic profile in its normal state, when a DDoS attack or anomaly occurs, they detect it, analyze it and change its characteristics. Further, the information is analyzed by the computer operator, and a semi-automatic or automatic suppression process begins. Suppression means that traffic destined for the victim is dynamically redirected through a filtering device that applies filters created by the detector to this traffic, reflecting the unique nature of the attack. Cleaned traffic is fed into the network and sent to the receiver (hence the name clean pipes - the subscriber receives a clean channel that does not contain attacks).

4. RESULTS AND DISCUSSION

The proposed single gate secured authentication model (SGSA) was compared with the existing Optimized cyber-attack detection (OCAD), DoS attack detection (DAD), sybil attack detection (SAD) and LDoS attack detection (LAD).

Table.1. Comparison of network safety

Entries	OCAD	DAD	SAD	LAD	SGSA
100	83.89	79.50	51.49	79.15	91.86
200	83.86	79.78	51.89	79.79	92.10
300	83.84	79.06	51.32	79.21	91.45
400	83.81	79.01	51.40	79.44	91.39
500	83.79	78.79	51.31	79.47	91.19
600	83.76	78.57	51.23	79.50	90.98
700	83.74	78.35	51.14	79.53	90.78

Management plane includes all traffic controlled or monitored by routers and other network equipment. This traffic is directed to or originated from the router. Examples of traffic include Telnet, SSH and http(s) sessions, syslog messages, SNMP traps. This was shown in Table.1.

The network management layer covers all service traffic, ensuring the operation and connectivity of the network according to specific topologies and parameters. Examples of control plane traffic are traffic generated or destined for a routing protocol (RR), including all routing protocols, sometimes SSH and SNMP and ICMP. Any attack on the operation of the routing application, especially DDoS attacks, can lead to significant problems and interruptions in the operation of the network. Best practices for securing control aircraft are described below Table.2. It uses QoS (quality of service) mechanisms to give higher priority to control traffic than user traffic (of which attacks are a part). It ensures the operation of the service protocols and the routing process, i.e., the topology and connectivity of the network, as well as the actual routing and switching of packets. This was shown in Table.3.

Table.2. Comparison of network security

Entries	OCAD	DAD	SAD	LAD	SGSA
100	83.85	77.83	49.97	76.51	90.43
200	83.77	77.38	49.85	75.83	90.46
300	83.70	76.93	49.74	75.16	90.50
400	83.62	76.48	49.62	74.48	90.53
500	83.55	76.03	49.51	73.81	90.57
600	83.47	75.58	49.39	73.13	90.60
700	83.40	75.13	49.28	72.46	90.64

Table.3. Comparison of network control

Entries	OCAD	DAD	SAD	LAD	SGSA
100	84.15	79.70	50.48	79.49	90.53
200	84.04	79.20	50.48	78.40	90.27
300	83.98	78.45	49.65	77.26	89.70
400	83.93	78.45	50.38	77.62	90.84
500	83.85	77.83	49.97	76.51	90.43
600	83.77	77.38	49.85	75.83	90.46
700	83.70	76.93	49.74	75.16	90.50

Table.4. Comparison of neighbor authentication

Entries	OCAD	DAD	SAD	LAD	SGSA
100	79.62	71.29	58.96	82.15	86.92
200	80.28	71.77	61.69	82.63	88.69
300	80.94	72.25	64.42	83.11	90.46
400	81.60	72.73	67.15	83.59	92.23
500	82.26	73.21	69.88	84.07	94.00
600	82.92	73.69	72.61	84.55	95.77
700	83.58	74.17	75.34	85.03	97.54

The main purpose of authenticating neighbor routers is to prevent attacks that send spoofed Routing Protocol messages to change routing in the network. Such attacks lead to unauthorized intrusion into the network, unauthorized use of network resources, and an attacker intercepting traffic to analyze and obtain necessary information is shown in Table.4.

5. CONCLUSION

Today news headlines are filled with reports of distributed denial of service (DDoS) attacks. Any organization on the Internet is vulnerable to denial-of-service attacks. It not a question of whether or not be attacked, but when. Government agencies, media and e-commerce sites, corporate sites, commercial and non-profit organizations are all potential targets for DDoS attacks. The site will stop working until the DDOS attack is stopped. Well, imagine you start reloading any page on the site thousands of times per second (DOS). Thousands of your friends are doing the same thing on their computers (distributed DOS or DDOS). Big servers have learned to recognize when a DDOS attack has started and counter it. However, hackers are improving their approaches. The port with attack options allows you to select the protocol (method) from the three TCP, UDP and HTTP. In the TCP / UDP message field, you can enter a message for the victim.

REFERENCES

[1] Chia-Wei Chang, Seungjoon Lee, Bill Lin, Jia Wang, “The Taming of The Shrew: Mitigating Low-Rate TCP-Targeted Attack”, *IEEE Transactions on Network Service Management*, Vol. 7, No. 1, pp. 1-13, 2010.

[2] Jian-Hua Song, Fan Hong and Yu Zhang, “Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks”, *Proceedings of 7th International Conference on Parallel and Distributed Computing, Applications and Technologies*, 2006.

[3] Wei Ren, Dit-Yan Yeung, Hai Jin and Mei Yang, “Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks”, *International Journal of Network Security*, Vol. 4, No. 2, pp. 227-234, 2007.

[4] Xiapu Luo, Edmond W.W. Chan and Rocky K.C. Chang, “Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals”, *EURASIP Journal on Advances in Signal Processing*, Vol. 9, No. 2, pp. 1-15, 2009.

[5] Ping Yi, Zhoulin Dai, Shiyong Zhang and Yiping Zhong, “A New Routing Attack in Mobile Ad Hoc Networks”, *International Journal of Information Technology*, Vol. 11, No. 2, pp. 83-94, 2005.

[6] John Haggerty, Qi Shi and Madjid Merabti, “Statistical Signatures for Early Detection of Flooding Denial-Of service Attacks”, *Cluster Computing*, Vol. 181, pp. 327-341, 2005.

[7] M. Wang and Zheng Yan, “Security in D2D Communications: A Review”, *Proceedings of IEEE Trustcom/BigDataSE/ISPA*, pp. 63-69, 2015.

[8] M. Aamir and M.A. Zaidi, “A Survey on DDoS Attack and Defense Strategies: from Traditional Schemes to Current Techniques”, *Interdisciplinary Information Sciences*, Vol. 19, No. 2, pp. 173-200, 2013.