A Survey on Network Security for Modern Internet of Things in DDOS Attack

N. Nithya[1], Aruchamy Rajini[2]
[1]Research Scholar, Department of Computer Science (Aided), NGM College, Pollachi, India
[2]Assistant Professor, Department of Computer Science (Aided), NGM College, Pollachi, India

***Abstract*: Network security is an important way of computing because many types of attacks are increasing day to day life. Protecting computer and network security are critical issues. Organizations would attempt to prevent network attacks by using network security tools such as firewalls or intrusion detection systems. While these still have their place, they are no match for modern day security attacks, for example modern Distributed Denial of Service (DDOS) attacks, as these attack on a much deeper level. These traditional perimeter-based solutions rely on a "castle and moat" method whereby anybody who manages to penetrate the network is automatically trusted, rather than authenticated before entering. These may introduce new threats due to improper configuration is sub-standard patching. Enterprises may also carry out vulnerability management and penetration testing. These help to meet compliance requirements and help to address gaps in information security, but they are very resource consuming. For a fully scalable, multi-layered defense solution, companies should invest in cloud security solutions.**

***Keywords*: DDOS, IoT, HTTP, Firewall, Mitigation**

1. Introduction

In the computer network an attack is an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. A computer attack may be defined as actions directed against computer systems to disrupt equipment operations, change processing control or corrupt the stored data. [1] A firewall is a term used for 'barrier' between a network of machines and uses that to operate under a common security policy and generally trust each other and the outside world [2].

2. Role of firewall

Firewall are often regarded as some as an irritation because they are often regarded as an impediment to accessing resources. [2] A firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules. In general, the purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate communication to flow freely [3].

A firewall is simply a program or hardware device that filters the information coming through the internet connection into a private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through. [4] A firewall is a system designed to prevent unauthorized access to form a private computer network. The firewall is to protect confidential information from those not authorized to access it and to protect against malicious users and accidents that originate outside of a network [5].

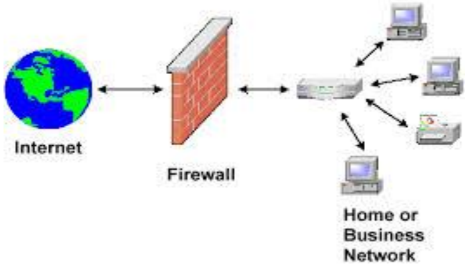

Fig. 1. Firewall

3. Internet of things

Technology becomes faster and smaller day by day and moving toward the "always connected" model. This revolution makes each and every device to communicate with each other and fabricate new future internet. This new concept of future internet is known as the Internet of Things. Every device from cell phone to car, alarm clock to coffee machine becomes connected to the internet with open standard IPv6 allowing unique addressing schema for them. IOT integrates physical things into an information network. These physical things sense the properties from the environment and send them for further processing to some information network [6].

A. IoT Attack

The IOT attack surface is the sum total of all potential security vulnerabilities in IoT devices and associated software and infrastructure in given network, be it local or the entire internet.

B. Security in IoT

IoT security is the technology area concerned with safeguarding connected devices and networks in the internet of things. Allowing devices to connect to the internet opens them up to a number of serious vulnerabilities if they are not properly protected.

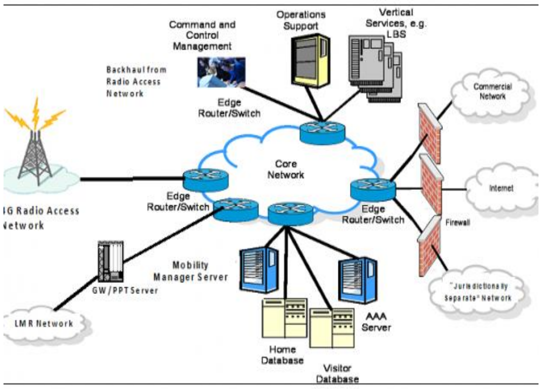

Fig. 2. Network security

C. *Security is important*

While business cannot stop IOT attacks from happening, they can be proactive in mitigating threats to network security and protecting valuable data and IT systems. For their part, consumers must hold business to higher standards and approach any IOT related purchase with a critical eye.

4. DOS/DDOS attack

A. *Denial of Services*

In denial of services attack, malicious node sending the message to the node and consume the bandwidth of the network. The main aim of the malicious node is to be busy the network node. If a message from unauthenticated node will come, then receiver will not receive that message because he is busy and beginner has to wait for the receiver response [7].

B. *Attack types*

The Manual attacks involve the attacker scanning the network, IP Addresses, Machines for vulnerabilities, break into the system and deploy code and executes a malicious payload for remote control access of that user system which is kept ready to launch an attack on the attacker's command.

Semi-automatic attacks involve deploying attack scripts that scan and compromise the user machines and download a payload and installing the attack codes. These victim systems are bots under control of the handlers who choose when and how about the attack type and target victims.

Automatic attacks, on the other hand, are carried with a high degree of automation, with the compromised user systems having the attack code and software with the predetermined type of attack, duration, victim's IP address. The attacker has minimal interaction once the payload gets deployed or during the automatic attack.

5. Attack model

The DDOS attack model is defined as follows. The attackers consist of a small group of m compromised hosts among a large group of n users, and the HTTP traffic originating from the attackers is indistinguishable from that generated by legitimate users.

A. *Session Flooding Attacks*

The attackers send a large number of HTTP requests through overflowing sessions.

B. *Request Flooding Attacks*

The attackers send a large number of HTTP requests with only a few sessions.

C. *Asymmetric Attacks*

To reduce the packet rate and maintain the high load in the server, the attackers send mostly HTTP requests of heavy workload.

D. *Slow Request/Response Attacks*

To hold and prolong HTTP sessions, the attackers slowly sends the HTTP requests/responses by delivering incomplete HTTP headers, diminishing HTTP data rate, or fragmenting HTTP packets.

6. Attack mitigation

Attack mitigation is a detection and protection strategy used to safeguard networks, servers and applications by IT administrators in order to minimize the effect of malicious traffic and intrusion attempts while maintaining functionality for users. DDoS mitigation is a set of techniques or tools for resisting or mitigating the impact of distributed denial-of-service attacks on networks attached to the Internet by protecting the target and relay networks.

A. *DDOS mitigation*

DDOS mitigation refers to the process of protecting a targeted server or network from DDOS attack. Detection - in order to stop a distributed attack, a website needs to be able to distinguish an attack from a high volume of normal traffic.

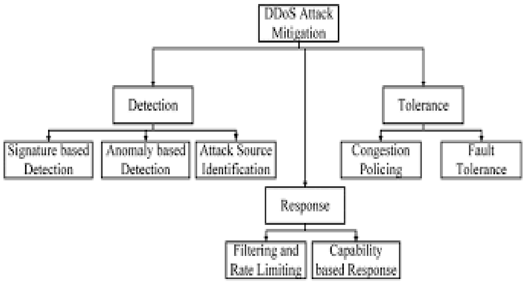
DDoS Attack Mitigation
Detection
Tolerance
Signature based Detection
Anomaly based Detection
Attack Source Identification
Congestion Policing
Fault Tolerance
Response
Filtering and Rate Limiting
Capability based Response

Fig. 3. DDOS mitigation

B. *Detection*

The detection method is very simple as the performance of the service or system degrades dramatically when an attack occurs. The detection methods consists of three different techniques,

- Signature based
- Anomaly based
- Attack source

C. Response

After the detection of the attack traffic or attack source, it is important to make a rapid response to mitigate the attack. In this response mechanism can reduce or omit the impacts of DDOS attack.

- Filtering and rate timing
- Capability based response

D. Tolerance

The techniques of tolerance mechanism work with a very little or even no knowledge about the result of the detection.

- Congestion policing
- Fault tolerance

7. Conclusion

IOT is very fastly developing now days. The IOT ecosystem is heavily populated with unsecure devices, and the number of these devices is expected to grow fastly over coming years, it is therefore reasonable to expect IOT based DDOS attacks to become much more common place.

References

[1] An analysis and classification of collaborative attack on Mobile Ad-hoc network.
[2] Kevin S.Mc Curley sat mar 11:16:00:15 MST 1995 www.McCurley.org
[3] An introduction to firewall, 4th edition.
[4] https://computer.how stuffworks.com>firewall
[5] https://www.itproportal.com
[6] Krushang Sonar, HardikUpadhyay "A survey: DDOS Attack on Internet of Things." IJERD Volume 10, Issue 11, pp. 58-63, November 2014.
[7] TasnuvaMahjabin, Yang Xiao, Guang Sun, Wangdong Jiang "A Survey of distributed Denial of service attack, prevention and mitigation techniques." IJDSN 2017, volume 13(12).
[8] Communication system and network technologies (CSNT), 2014, ISBN:978-1-4799-30692, 7-9 April'2014
[9] Mohan V. Pawar, J. Anuradha "Network security and types of attacks in network." International conference on intelligent computing, communication and convergence (ICC2015). Procedia computer science 48 (2015) 503-506.
[10] A. Karila, S. Fdida, M. May, and M. Potts. A. Gavras, "Future Internet Research and Experimentation: The FIRE Initiative," ACM SIGCOMM Computer Communication Review, vol. 37, no. 3, pp. 89-92, July 2007.
[11] S. K. Fayaz, Y. Tobioka, V. Sekar, and M. Bailey, "Bohatei: flexible and elastic DDoS defense," In Proc. USENIX Security, 2015
[12] M. Shtern, R. Sandel, M. Litoiu, C. Bachalo, and V, Theodorou, "Towards mitigation of low and slow application ddos attacks," IEEE International Conference on Cloud Engineering (IC2E), 2014.
[13] S. Venkatesan, M. Albanese, K. Amin, S. Jajodia, and M. Wright, "A moving target defense approach to mitigate DDoS attacks against proxy based architectures," IEEE Conference on Communications and Network Security, 2016.
[14] Y. Xie and S. Z. Yu, "Monitoring the application-layer DDoS attacks for popular websites." IEEE/ACM Transactions on Networking (TON), Vol. 17, no. 1, pp. 15-25, 2009.
[15] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEE Communications Surveys & Tutorials Vol. 15, no. 4, pp. 2046-2069, 2013.