IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-9, Sept 2019 E-ISSN: 2347-2693

IoT Devices are Being Weaponized for DDoS Attacks

Sapna Rawat[1*], Md Tabrez Nafis[2]

[1,2]Department of Computer Science JAMIA HAMDARD, Delhi, India

[*]*Corresponding Author: certinsapna@gmail.com, Tel.: +90-9891099380*

DOI: https://doi.org/10.26438/ijcse/v7i9.2225 | Available online at: www.ijcseonline.org

Accepted: 02/Sept/2019, Published: 30/Sept/2019

***Abstract*—** The Internet of Things revolutions have made our live stress-free and better by giving us economical services. It always keeps us connected to the embedded system and provides value added services to humans as per their requirements. As per the research, 5 billion devices are already connected with the internet and these numbers will increase to 20 billion in few years. As we know that every cloud has a silver lining, same goes for Internet of Things. IoT devices are becoming a primary object for hacker, it is continuously alluring the attacker or intruder who tries to harness and exploit the devices. Top security concerns of IoT devices are Sensitive information disclosure, Denial of service attack, Tampering of Data and privilege escalation. Internet of Things use cloud servers to exchange information from one device to another device. But if an attacker successfully exploits the vulnerability, it could easily access, read or modify the data while performing the men in middle attack. Moreover malicious user can use this data that can cause potential damage to the targeted organization and can use it for their personal financial gain. This article provides the guidance for best practices to mitigate the DDOS attack and examine their interrelationships.

***Keywords*—** Internet of Things (IoT), Denial of Service(DOS), Distributed Denial of Service(DDOS), Internet Security, Wireless Security, Spoofing, Secure Routing, IoT Security, Controller, Secure Forwarding Cloud, Device, Sensor, Encrypted session key, Firewall, HTTP/S, Filtering, DNS, BGP, Null routing, BIG-IP server, VoIP or FTP.

I. INTRODUCTION

Internets of Things (IoT) devices are most prominent platform for cyberattacks and it has become the most vulnerable way to perform the attack. Millions of devices remain unmonitored for a very long period of time, such as CCTV Camera, mobile phones, routers, AC, automatic, car, hospital appliances or fridges [1]. Unfortunately numbers of IoT devices have very low building cost as a result of which they have poor design and configuration.

Variants of DDOS are raising alarm for the industry to secure the IOT devices and act to reduce the risk exposing the Internet infrastructure. As per the predictions by several consultancy firms (like Google, McKinsey and UHG) on IoT clearly shows that market will increase in next 15 years.

IoT Devices are Being Weaponized for DDoS Attacks

The Internet of Things (IoT) revolution is not only interconnecting the entire generation of "dumb" devices at the same time it also provides revolutionary promises to make our lives easier. The Internet of Things (IoT) is the network of physical devices that are embedded with electronic sensors, software and network connectivity that permit these objects to collect and exchange data over the cloud network. The data that is been traversed over cloud network can be compromised or breached by intruder for their potential gain [2].

DDoS (Distributed Denial of Service) is the most prominent attack. This vulnerability can be exploited by sending crafted data packets to the targeted device. Successful exploitation of this vulnerability will allow the attacker to execute the multiple requests on the vulnerable system to cause the denial of service condition on the target device. Conjunction of DDOS with other vulnerabilities could lead to successful execution of arbitrary code and compromise the targeted device.

II. RELATED WORK

This study was focused on previous DDoS detection and defence algorithms to mitigate the DDOS attack. The proposed algorithm, it focuses on three important parts: (DDR) Detection, Defence and Report of attacks as shown [5].

Algorithm: QVMMA stands for Qualified Vector Match and Merge Algorithm that can be used for DDoS detection and mitigation in real time.

Brief description of steps of QVMMA for Binder Detection shown in Fig.2 is provided as follows:

Figure 1. QVMMA for Binder Detection

1. Qualify: Check the Suspicious Records using Qualifiers Q= {OQ1, OQ2}

   If it is satisfies the given conditions. Qualifiers are generated as first value of Attack Signature Qualifier Components.

2. Vectorization: Generate the vectors FV for suspicious records.

3. Match: Match the vectors with the General Attack Vector Value (GAVv).

   If (Match vector value! = GAVv)
   {
   Print (If condition is not matched, then attack is not performed)
   }
   Else
   {
   (Attack is performed)
   }

4. Merge: Merge is the feature vectors or signatures generated at Stage 2 Filter run at different routers inside the network to measure the overall impact of attacker on the victim.

III. METHODOLOGY

This study will focus on "Mitigation of DDOS attacks in context of IOT devices"

Step 1: Prerequisites for proposed secured algorithms:
1. IOT Devices
2. Cloud Server
3. 3 Way handshake approach
4. Cryptography
5. Traffic Analyser Tool

Step 2: IOT devices are communicated with cloud server using 3 way handshake approach.

Below is the screenshot, how it works.

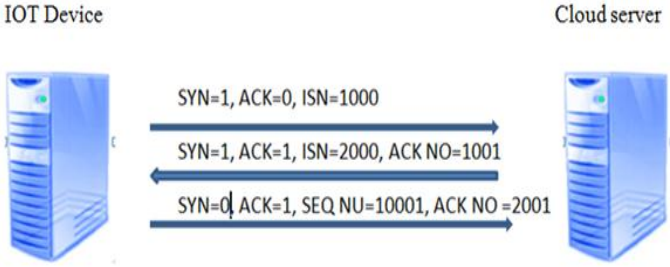

Figure 2. 3 Way Handshake

Step 3: IOT DEVICE communicates with cloud server using SYN = 1, ACK = 0, ISN = 1000.
Step 4: Cloud server receives the IOT Device request and acknowledge with SYN = 1, ACK = 1, ISN = 2000, ACK NO=1001.
Step 5: IOT Device sends an acknowledgement to Cloud server, with SYN = 0,
ACK =1, SEQ NU=1001, ACK NO=2001
After the secure connection is established, now the connection is reliable and open for both the devices.
Step 6: IOT Device ID request is encrypted using encryption algorithm
Step7: Key was generated on authentication server with the help of super secrete key algorithm.
Step8: Session key generated for IOTdevice ID and embedded with IOT Device ID.
Step9: Now the request is send it to cloud server with the combination of Input request, session key and super-secret key
Step10: Traffic analyser tool analyze the IOT Device ID request before reaching to the cloud server.
SPLUNK, Network Performance Monitor (NPM), Wireshark or FIRWALL.
Step11: If traffic is legitimate then CLOUD SERVER validates the data or session value.
Step: 12: Post that CLOUD SERVER decrypt the IOT Device data with secrete key and send acknowledgement to the client.
Step 13: In the 12th step we concluded that the IOT device is now secure.

The below mitigation algorithm focuses mainly on three important parts:
1. Detection
2. Defence
3. Report

Algorithm refers to the process of successfully protecting the targeted servers and network from distributed denial-of-service (DDoS) attack [7].

A cyber-attack is a persistent threat to businesses and organizations by hostile performance of service or by completely shutting down a website.
Mitigation process is broadly defined as below:

Figure 3. DDoS Mitigation life cyle

Detection – Identify the abnormal traffic flow that may trigger the DDoS attack.

Diversion – Diversion includes either rerouting of traffic, filtering out the abnormal flow or the traffic will be discarded.
Filtering – DDoS traffic is eradicated by analyzing and then identifying the patterns, whether they are legitimate or malicious traffic.

Analysis – Reviewing of security logs to collect information about the attack for identifying the attackers and to minimize the future incidents.

DDOS mitigation techniques:
1. DIVERSION TECHNIQUES: DNS VS BGP ROUTING
DNS ROUTING: It reroutes all incoming traffic through the scrubbing servers, where scrubbing server eradicate malicious traffic and forward legitimate traffic to the servers.
BGP ROUTING: It redirects all network layer packets from the targeted IP addresses to the scrubbing servers. And then they filter out malicious packet along with sending the alert to the systems via secure GRE tunnel. At the same time it reduces latency and accelerates the content delivery.
BGP routing is extensively used as traffic diversion method and since it offers protection to all type network and application layer attacks thus it is effective across all protocols.

2. NETWORK CAPACITY
Network capacity is one of the best ways to mitigate DDoS attack. The greater the network capacity, lesser will be the influence of DDoS attack.

3. NETWORK LAYER MITIGATION TECHNIQUES
Null routing – It directs all traffic to a non-existent IP address.
Sinkholing – This method diverts malicious traffic away from its target by scanning the list of known malicious IP addresses.

BIG-IP server - Load balancer divided the network and application traffic across the number of servers. It is used to increase the reliability and capacity of applications.

Below are the points that should also be considered to avoid DDOS attack:

- Monitoring the traffic to look for abnormal activity, always keep an eye on public wastebins (Pastebin), anonymous site (DB hacker) and social media (Twitter) for threats.
- Pastebin is used for storing and sharing stolen data. It is commonly used for distributing legitimate data into networks, like application, network configuration details and authentication records.
- Build a cyber response plan document and a rapid response team. Place all the procedures in one centralize database for your customer support security teams and communication teams.
- To prioritize your concerns, examine several DDoS mitigation techniques and prepare the advisory and vulnerability note.

IV. RESULTS AND DISCUSSION

Find the below DDoS attacks and Global IoT Installed base devices in the last few years [8].

Table 1. Global IoT Installed Base (In billion units)

Category	2017	2018	2019
Consumer	5.2	7	12.8
Business	1.2	1.4	7.6
Total	6.4	8.4	20.4

Table 2 . DDoS attacks in the last few years

Name	Year	Source Code	Agent CPU	Architecture Model	Possible Attacks
Chuck Norris	2010	Reverse Eng.	MIPS	IRC-Based	UDP Flood, SYN Flood, ACK Flood
Aidra, LightAidra, Zendran	2012	Open Source	MIPS, ARM ,MIPSEL, SuperH, PPC	IRC-Based	SYN Flood, ACK Flood
XOR.DdoS	2015	Reverse Eng.	MIPS, PPC, SuperH, ARM	Agent-Handler	DNS Query, Other TCP Floods, ACK Flood SYN Flood.
Mirai	2016	Open Source	MIPS, MIPSEL, ARM, PPC, SuperH,	Agent-Handler	SYN Flood, GET Flood, GRE Protocol flood, ACK Flood, UDP Flood, DNS Water Torture GRE IP, Flood, VSE Query Flood, HTTP Layer 7 Flood.

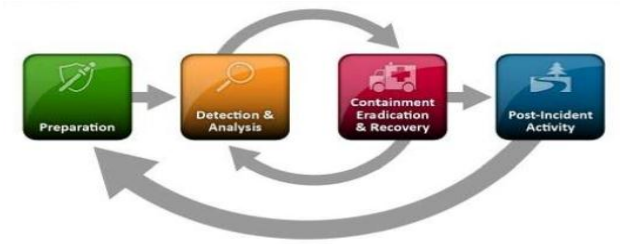

Figure 4. How DDoS Mitigation life cyle work

V. CONCLUSION AND FUTURE SCOPE

IoT as a "Land of Opportunity" for DDoS Hackers, with flooded numerous number of poorly configured secure devices that can be controlled by intruder for highly disruptive attacks by gaining access of targeted system. Successful exploitation of this vulnerability could allow the attackers to execute multiple requests on targeted system with elevated privileges. This vulnerability in conjunction with other vulnerabilities could lead to execution of arbitrary code and compromise the targeted system.

Implementation is carried out to establish "device connection" with "cloud component for authenticating devices" to prevent DDOS attack, create the emergency response plan team to mitigating network layer attacks, all software must be updated with the latest patches. Follow the security guidelines to avoid the DDoS attack.

In context of this paper I would like to share my analysis of IoT devices exposing DDoS capabilities and this study will raise awareness among the research community and implement capabilities to respond to cyber crisis before it happens.

REFERENCES

[1] Constantinos Kolias, Georgios Kambourakis, and Angelos Stavrou *"DDoS in the IoT: Mirai and Other Botnets"*, **07 July 2017**, IEEE, INSPEC Accession Number: **17012613**. For Journal

[2] Linux/AES. DDoS: "*Router Malware Warning - Reversing an AR March ELF*," MalwareMustDie! Blog, **2014**.

[3] Danny Palme, *IoT security warning: Cyber-attacks on medical devices could put patients at risk*, DOI: **10.1145/2667218**, Communications of the ACM 58(4):**74-82 · April 2015.**

[4] D. Bekerman, "New Mirai Variant Launches 54 Hour DDoS Attack against US College," blog, Imperva Incapsula, **29 Mar. 2017**.

[5] SoniaLaskara, DhirendraMishra "*Qualified Vector Match andMerge Algorithm (QVMMA) for DDoS Prevention and Mitigation*". **ELSEVIER**, India, Volume **79, 2016**.

[6] S. Edwards and I. Profetis, "*Hajime: Analysis of a Decentralized Internet Worm for IoT Devices*," Rapidity Networks; **16Oct.2016.**

[7] Prabhakaran Kasinathan; Claudio Pastrone; Maurizio A.Spirito; Mark Vinkovits, *Denial-of-Service detection in 6LoWPAN based Internet of Things.*

[8] Georgios Kambourakis, Constantinos Kolias, Angelos Stavrou *"The Mirai botnet and the IoT Zombie Armies"*,MILCOM- **2017 IEEE** Military Communications Conference (**MILCOM**).

[9] Michele De Donno, Nicola Dragoni, Alberto Giaretta, "*Analysis of DDoS-capable IoT malwares*", **2017** Federated Conference on Computer Science and Information Systems (**FedCSIS**).

[10] Natalija Vlajic, Daiwei Zhou "*IoT as a Land of Opportunity for DDoS Hackers*" C. Kolias et al. Published in: Computer Volume: 51, Issue: 7, July 2018.

[11] M Devendra Prasad1, Prasanta Babu V2, C Amarnath3 *"Machine Learning DDoS Detection Using Stochastic Gradient Boosting" Volume*-**7, Issue-4, Page no. 157-166, Apr-2019.**

[12] Michele De Donno, 1 Nicola Dragoni, 1, 2 Alberto Giaretta, 2 and Angelo Spognardi3 "*DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation"* Volume **2018, Article ID 7178164.**

[13] Swaroop P T1, Mrs. Chaitra H K "*Internet of Things: Smart*" College, Volume-**4, Special Issue-3, May 2016.**

Authors Profile

Sapna Rawat in pursed Bachelors of Engineering (B.E) in Computer Engineering from The Institution of Electronics Telecommunication Engineers (AMIETE), India in 2011, Post-graduation diploma in Information security from Indira Gandhi National Open University Delhi in 2014 and currently pursuing Master of Technology (M. Tech) in Computer Science from Jamia Hamdard, India. She is currently working as Information Security Engineer in United Health Group. Prior to United health group she worked with Indian Computer Emergency Response Team (ICERT) under the ministry on IT as Junior Cyber Security Consultant, where she was resposnible for making cyber security policies, track and manage the cyber security threats, Performed Security audits of web application on government projects, vulnerability Tracking, Preparation of Vulnerability notes and advisories published on "ICERT" Websites.Her main research work focuses on Cyber security, Cryptography Algorithms, Application Security, Cloud Security and Privacy, Data Analytics, IoT and Computational Intelligence based education. She has overall 6.5 years of cybr security consultatnt experience.

MD TABREZ NAFIS in pursed Bachelor of Science, Master of Science and Ph.D. He is currently working as Assistant Professor in Jamia Hamdard, India published more than 15 research papers in reputed international journals.

