INFORMATIC INSTITUE OF TECHNOLOGY

COMPUTER SCIENCE PRACTICE

4COSC008C

VULNARABILITIES AND THREATS OF IOT

Distributer denial of service/BotNet attacks: how can they be avoided? How can they help us learn lessons for better data protection? Does the Internet of Things pose new threats to our private data?

Module Leader's Name-Ms. Sulochana Rupasinghe

S.M.K.C. Wedage

Uow Number-w1742101

IIT Number-2018368

Group Members

1. S.M.K.C. Wedage 2018368

2. M.H.V. Sithum 2018369

3. K.V.H.C. Samaranayake 2018371

4. D.S. Sendanayaka 2018445

5. W.M.S. Perera 2018446

Table of Content

Table of Figures

Abstract

Simply IoT means Internet of Things. IoT is influencing our life styles from the way we react to the way we behave. IoT is a giant network with interconnected peripherals. IoT mainly depends upon the functionality.

This report is about how IoT affects to DDoS attacks. IoT ease our work. No doubt about that, but due some drawbacks it's a risk. Defiantly security of personal data is the issue. DDoS can be attacked in Network Layer and Application Layer, which can go through a victim's network and seize it and make it unavailable to the user. In this report I have showed couple of DDoS attacks.

Though technology grows up high and high still there is no proper way to get rid of this DDoS attack on Internet of Things. This is because of limited power of small IoT devices. We can assure that recently this problem will be solved.

1. Introduction

Today when we talk about personal data, security is the major aspect that we talk about. Technology is growing day by day which gives us more facilities to be interconnected. But now a days there are more threats that can harm our data rather than protect our data. DDOS and Botnet attacks are some attacks that can be a issue to our personal data.

Denial-of-Service (DoS) attacks are used to shutdown machines without the user authorization and make data and folders inaccessible. They generate data that cannot be bared by the data traffic. Most of these attacks target web servers and high profile organizations such as banking organizations, media companies, government organizations and trade organizations. When these same kind of attacks done by many nodes is called DDoS. Earlier these attacks were launched on the network layer. With the time passes these attacks became more sophisticated and efficient. Now it is also launched in application layer which attacks to the victim's web server.

There are many types DDoS attacks, PING flood, UDP Flood, Ping of Death, SYN Flood and Zero day DDoS are some of examples. Usually IoT runs in Application and Network layer. Application layer is the very first layer which has the user interface. In network layer, data processing and broadcasting is done from sender to receiver.

Technology developed the network protocols and operating systems. But because of using systems without security, results in providing hackers a lot of opportunities to misuse insecure computers on internet. In the network layer following attacks can be happened. Flooding attacks, Reflection-based flooding attacks, Protocol Exploitation flooding attacks, Amplification-based flooding attacks are some examples. Flooding is a type of attack which disturbs user's connectivity by exhausting victims network bandwidth. UDP flood, ICMP flood, DNS flood are some examples.

In application layer Reprogramming attack and Path based DoS can be faced. In reprogramming attack, the attacker can get the source code of a particular program and attacker can edit the source code as prefer. This may cause infinite loops and makes the user inaccessible to the program.

Ultimately, though IoT have some drawbacks IoT made our lives to a next level dimension. Some minor adjustment will be help to drop these drawbacks. Surely there is a risk.

2. Literature review

DDoS attacks have been increased rapidly throughout the years. It is said that 91% of DDoS have been in 2017. Roughly 50 million DDoS attacks occur annually and it is said that 17 million DDoS attacks will occur annually by 2020. For these numbers IoT is the major reason. This happens due to insecure IoT devices.

2.1 KrebsOnSecurity.com faced a massive attack.

(KrebsonSecurity, 2016)Since 2012, this site faced a load of DDoS attacks. On 20th September 2016 was dark day for KrebsOnSecurity.com as they faced a massive DDoS attack which made their whole site go down. This had a larger magnitude approximately 620Gbps. This was too large to bear my its own hand without affecting the customers. Akamai was the attacker and revealed that this attack got a weight of 24,000 systems. These systems were infected by mirai virus and mostly with hacked Internet of Things (IoT) devices such as video recorders and security cameras. This attack was massive no doubt about that, but the silly part was Akamai was a customer of KrebsOnSecurtity.

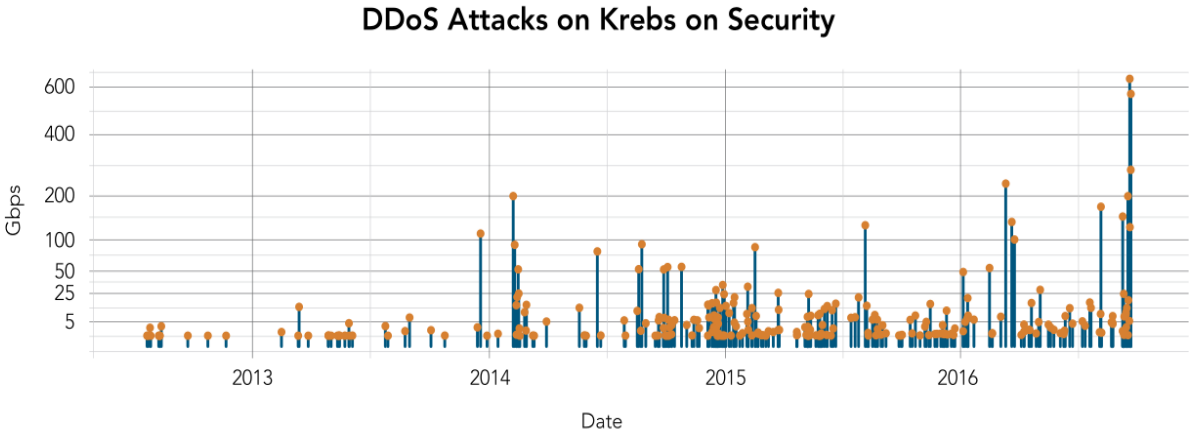

Figure 2.1.1: Attacks mitigated for Krebsonsecurity.com

2.2 DNS provider Dyn.

(Anon., 2016)One of the leading DNS provider, Dyn faced a massive DDoS attack on October 21 2016. This attack lasted for several hours damaging the access for some reputed companies like Twitter, GitHub and PayPal. For this attack mirai IoT botnet was used. Even this attack targeted the sites in DNS server the original sites were fully functional. But the browsers were unable to convert the domain names to IP address.

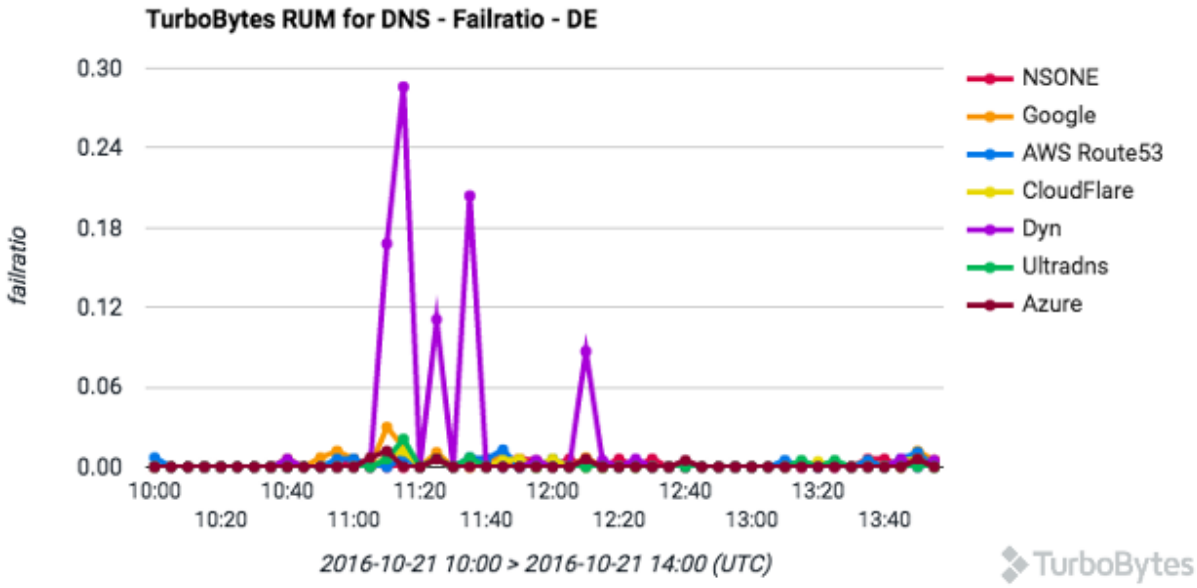

Figure 2.2.1: Real impact of DDoS to Dyn

For this attack no one found who is responsible. But Dyn says that, the person who attack KrebsOnSecurity.com is behind this. For this attack, attackers used the techniques that are widely known and the skill of the attacker was not great. But somehow the attacker is hidden.

3. Methodology

This report mainly focuses on how IoT aids on DDoS attacks. This was a brand new topic to our team that we never heard. So we spent so many hours to gather information and sort them out. After dividing the topic into subtopics, we started our mission on gathering information related to work break down structure. I had to gather information about the history and the current situation of this problem.

3.1 Online resources

To gather information, I referred lots of research papers and some of recent projects. But I didn't get valuable information. So I referred online articles. Articles drove me to a much better understanding. It wasn't enough, so to get a fine understanding about my topic, I watched some of YouTube videos. But, to be true I didn't get cutting edge information. Because currently there is no proper solution to this problem

3.2 Human resources

As I mentioned above I didn't get the information I needed. So, to sort out my problem I got helped from a software engineer who is my roommate. He clearly explained me about problem and drove through some current issues in IoT.

4. Results and discussion

IoT is a cutting edge technology which helps us in day to day lives. But due to IoT vulnerabilities people are scared to use IoT devices. Because IoT has the potential to provide huge and large amounts of personal information. Even in the latest devices, there are security vulnerabilities.

4.1 IoT vulnerabilities

DDoS attack is mainly focused on Network layer and Application layer. Due to poor mainatainence in these layers insecure network services are being served. In IoT devices unexpectedly firmware failures are been occurred. So its insecure to transfer or store personal data in IoT devices.

(Bhattacharya, 2018)But in these devices there are user authentication processers. User might think nothing could go wrong. But sometimes these too fails. Because of that privacy protection is insufficient. In IoT devices, data is send and retrieve through the transport layer. All the sensitive data goes through this transport layer. But the fact to be amazed is still there is no proper encryption to the transport layer.

Ultimately, I would say that if we use proper encryption methods and proper user authentication methods we could minimize the data loss.

4.2 IoT Threats

If there are vulnerabilities surely there are threats. The threat can be affected for a individual person, or a group of people or a country. Threats cannot be neglected when it is considered as national security. Due to poor usability and sloppy handling IoT devices suddenly fails. The bad practice could be done by the user or the developer.

Another threat is, sensitive cloud information could be leaked. And this is also could be affected to several people.

To solve these kind of threats first of all we should solve the basic vulnerabilities. When data is transferred data encryption methods can be used. To ensure more security we could use independent encryption methods to the OSI layers. If IoT fails unexpectedly we could use an auto system backup process as currently it is not available. Just in case a secondary memory can be used to ensure that the user data is not loosed.

If developers, consider the above facts, they could make IoT devices which are safer . So people might tent to use more IoT devices. So the whole word is connected to a one place.

5. Conclusion

In this paper I focused about the vulnerabilities and threats of IoT. Now a days It is impossible to prevent IoT from DDoS attacks because of above mentioned vulnerabilities. (Rayome, 2017)It is said that in 2017, 91% of DDoS attacks was caused by poor maintenance of IoT devices. But technology develops day by day. So we can assure that engineers will work on these vulnerabilities because IoT will play an important role in future. In here IOT devices work as a system with many sub systems. Because of this, security is the main issue caused by this of interconnection. So we should identify and mitigate the DDoS attacks on IoT.

6. REFERENCES

Anon., 2016. *enisa.* [Online]
Available at: https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices
[Accessed 14 March 2019].

Bhattacharya, S., 2018. *INFOSEC.* [Online]
Available at: https://resources.infosecinstitute.com/the-top-ten-iot-vulnerabilities/#gref
[Accessed March 2019].

CYBERPEDIA, n.d. *CYBERPEDIA.* [Online]
Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos
[Accessed 18 March 2019].

KrebsonSecurity, 2016. *KrebsonSecurity.* [Online]
Available at: https://krebsonsecurity.com/2016/11/akamai-on-the-record-krebsonsecurity-attack/
[Accessed 19 March 2019].

Rayome, A. D., 2017. *TechRepublic.* [Online]
Available at: https://www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/
[Accessed 17 March 2019].

7. Bibliograpy

https://www.a10networks.com/resources/articles/iot-and-ddos-cyberattacks-rise

https://www.bleepingcomputer.com/news/security/dramatic-increase-of-ddos-attack-sizes-attributed-to-iot-devices/

https://www.bitdefender.com/box/blog/iot-news/iot-botnets-responsible-powerful-ddos-attacks/

https://www.darkreading.com/iot/7-serious-iot-vulnerabilities/d/d-id/1332616?image_number=5

https://resources.infosecinstitute.com/the-top-ten-iot-vulnerabilities/#gref

https://www.networkworld.com/article/3332032/top-10-iot-vulnerabilities.html