Appendix C:

Masters Project Research Log

Masters in Electronic and Computer Engineering 2019/2020

Student Name: Michael Lenehan
Student ID: 15410402
Project Title: An Evaluation of Distributed Denial of Service Attacks in IoT Networks

Please read before making entries in this log

The purpose of this Project Research Log is to capture concise, focused summaries of research materials you read, as you progress through your project. The emphasis is to record (i) how the material you have read will determine or influence your project solution approach and (ii) your assessment of the key strengths and weaknesses of the solutions, methods, technologies, etc. proposed in the material you have read.

In the first stage of your project, the literature review, use the Log to capture this information for the key papers you have read (for example, the three most important papers of your 10 literature review references). As your project progresses into the design and implementation phases, you will need to continue to search the literature so you can review, revise and refine your initial thinking and the details of your approach to a project solution. Use this Research Log to capture your continued research reading and its influence on your project design and implementation.

Be selective about what you record in this log. Do not use it as an informal notebook while you are reading a new paper. Only make an entry after you have read a paper that you consider important to the development of your project solution. It is expected that, by the end of the project, you will have made **between 10 and 20 entries (20 maximum)**.

Your log will be shared with your supervisor for viewing throughout the project and you will submit the final version of the log for grading, at the end of the project implementation period. It will be assessed on the basis of how well you have used your analysis of the literature to inform your project design, implementation and the evaluation of your project results. The Research Log contributes **5%** to the overall project mark.

Note: All entries you make in this log must use the prescribed format. A new entry with the correct format is generated using the “Research Log” menu above (it may take a minute for this menu to appear). Do not make any other entries or change the format of the generated tables. You will maintain other notes as you progress through your project but they should not be recorded here. Do not exceed the maximum word counts indicated.

Statement of project problem / research question
The aim of this project is to provide a comprehensive evaluation on the susceptibility of IoT devices to attack for the purposes of the execution of distributed denial of service attacks. This evaluation will take the form of a survey of current IoT security vulnerabilities, a comparison of the differences between IoT security implementations and desktop/server operating system security implementations, and a survey of currently proposed detection and mitigation techniques. Along with this survey, a simulation of a denial of service, and distributed denial of service attacks will be presented. This simulation will utilise some commonly available Linux packages to display the differences in attack volume, and complexity between a standard denial of service attack, and a distributed denial of service attack.

IoT Device security through dynamic hardware isolation with cloud-Based update
Hategekimana, F., Whitaker, T., Hossain Pantho, M. and Bobda, C., 2020. IoT Device security through dynamic hardware isolation with cloud-Based update. *Journal of Systems Architecture*, 109, p.101827.
https://doi.org/10.1016/j.sysarc.2020.101827
Summary of paper
This paper proposes a security device which can be connected between an IoT device and a network which monitors the traffic between the device and the network. In monitoring the traffic, security breaches can be detected, with reports sent to a centralised server, updating the security policies of other such security devices.
How is this paper relevant to solving your project problem or addressing your research question?
This paper examines a method of improving security on IoT devices. As DDoS attacks which make use of IoT botnets take advantage of the relatively poor security implementations on IoT devices, improving the security of these devices could greatly reduce the likelihood of these attacks.
What are the strengths and weaknesses of the solutions/methods/technologies proposed in this paper?
The proposed defense mechanism is placed between the IoT devices and the network. This would require device manufacturers to implement the SoC on their devices, which is an added cost to production. As a number of these manufacturers already do not implement basic security measures, the assumption that the added SoC would be used for their devices is not certain.
Log Entry Creation Date: Thu Feb 20 2020 11:05:08 GMT-0000 (GMT)

Distributed denial of service attacks and its defenses of IoT: a survey
Salim, M., Rathore, S. and Park, J., 2019. Distributed denial of service attacks and its defenses in IoT: a survey. *The Journal of Supercomputing*, 76(7), pp.5320-5363.
https://doi.org/10.1007/s11227-019-02945-z
Summary of paper
Acts as a survey of DDoS attack motivations and methods. Classifies attacks in terms of Iot devices and cloud layer. Presents defense and mitigation strategies. Paper gives a comprehensive overview of attack tools, various attack methods, defense and mitigation strategies.
How is this paper relevant to solving your project problem or addressing your research question?
This paper acts as a good starting point for the project. It presents an excellent baseline of knowledge in terms of DDoS attack types and the tools used by attackers.

What are the strengths and weaknesses of the solutions/methods/technologies proposed in this paper?

This paper provides a very in-depth survey into DDoS attack types, tools, and mitigation techniques. It does not however present any practical implementations of any of these.

Log Entry Creation Date: Thu Feb 20 2020 11:05:08 GMT-0000 (GMT)

Dyn DDoS Cyberattack - a case study

Sreekanth, A., Sri, P. and Vartiainen, T., 2020. Dyn DDOS Cyberattack - a case study. [online] Available at: <https://mycourses.aalto.fi/login/index.php>.

https://mycourses.aalto.fi/login/index.php

Summary of paper

This paper presents a case study of the Dyn DDoS attack. This attack took place in 2016, and at the time was the biggest DDoS attack ever launched. This paper delves into the Mirai malware which was used to launch the attack, the timeline of the attack, the DNS exhaustion attack method used, the effects of the attack, and the challenges faced in defending against these types of attack.

How is this paper relevant to solving your project problem or addressing your research question?

The Dyn attack is infamous due to the scale of the botnet used to launch the attack. By presenting a case study of this attack, we get a better understanding of the real-world impact of these large scale attacks. Having a real-world example to refer to, rather than a conceptual, or theoretical threat proves the need for further understanding of the causes of these attacks along with the security measures which can be taken to avoid these attacks.

What are the strengths and weaknesses of the solutions/methods/technologies proposed in this paper?

This paper presents an in-depth case study of the Dyn attack, with focus on the attack and the challenges faced in mitigating the attack. However, as this is just a case study, there is not as much of a focus on the current state of mitigation techniques, or

Log Entry Creation Date: Thu Feb 20 2020 11:05:08 GMT-0000 (GMT)

Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes

Ali, B. and Awad, A., 2018. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors*, [online] 18(3), p.817. Available at: <https://www.mdpi.com/1424-8220/18/3/817>.

https://www.mdpi.com/1424-8220/18/3/817

Summary of paper

This paper proposes a security device which can be connected between an IoT device and a network which monitors the traffic between the device and the network. In monitoring the traffic, security breaches can be detected, with reports sent to a centralised server, updating the security policies of other such security devices.

How is this paper relevant to solving your project problem or addressing your research question?

This paper examines a method of improving security on IoT devices. As DDoS attacks which make use of IoT botnets take advantage of the relatively poor security implementations on IoT devices, improving the security of these devices could greatly reduce the likelihood of these attacks.

What are the strengths and weaknesses of the solutions/methods/technologies proposed in this paper?

Log Entry Creation Date: Thu Feb 20 2020 11:05:08 GMT-0000 (GMT)

Standardizing IoT Network Security Policy Enforcement

Barrera, D., Molloy, I. and Huang, H., 2018. Standardizing IoT Network Security Policy Enforcement. *Workshop on Decentralized IoT Security and Standards (DISS) 2018*,.

https://dx.doi.org/10.14722/diss.2018.23007

Summary of paper

This paper looks into the predictability of IoT security implementations, and proposes a secure architecture for protecting networks of IoT devices. This architecture is independent of device manufacturers and aims to protect devices from being compromised by attackers.

How is this paper relevant to solving your project problem or addressing your research question?

The “security policy enforcement architecture” aims to protect devices and mitigate the impact of attacks by providing a whitelist of expected network activity, such as metadata - packet size etc. -, content - protocol -, and application - HTTP requests. The paper also provides insight into the need for this type of architecture, looking at attacks and similar architectures.

What are the strengths and weaknesses of the solutions/methods/technologies proposed in this paper?

The proposed solution aims to be independent of device vendors, increasing the probability of success for the method. Also the method uses the “principle of least privilege” to limit the exposure of the devices.
One listed limitation of the proposed policies is increased latency. It was noted that the LIFX smart bulb used for testing faced a delay between commands sent from the smartphone and the action of the bulb, as devices were isolated from one another on the

network, meaning all packets sent had to make a connection to the LIFX cloud servers to be rerouted to the bulb.

Log Entry Creation Date: Thu Feb 20 2020 11:05:08 GMT-0000 (GMT)

Facing DDoS bandwidth flooding attacks

Furfaro, A., Pace, P. and Parise, A., 2020. Facing DDoS bandwidth flooding attacks. *Simulation Modelling Practice and Theory*, 98, p.101984.

https://doi.org/10.1016/j.simpat.2019.101984

Summary of paper

This paper gives a scalable filtering mitigation technique for bandwidth flooding attacks. This technique builds on the StopIt mechanism, adding the ability to deal with indirect flooding attacks.

How is this paper relevant to solving your project problem or addressing your research question?

Flooding attacks are a common use-case for IoT botnets. The large number of devices means that high volumes of data can be used to exhaust the available resources for a web server/service. The proposed filtering technique could be applied to an IoT network, mitigating the risk of a denial of service.

What are the strengths and weaknesses of the solutions/methods/technologies proposed in this paper?

The proposed defense mechanism can reduce packet loss in a network undergoing an attack from 95.15% (without any defense mechanism) to 0.07% packet loss. This paper presents a simulation model for the proposed mechanism, developed in ns-3, which experimentally shows it's benefits.
The simulations use a network of 20 nodes, which includes hosts and switches. This is much lower than the number of hosts used in botnet DDiS attacks. Also, ns-3 does not provide any information on the impact of the defense mechanism on the system, in terms of performance.

Log Entry Creation Date: Thu Feb 20 2020 11:05:08 GMT-0000 (GMT)

A novel approach for detecting vulnerable IoT devices connected behind a home NAT

Meidan, Y., Sachidananda, V., Peng, H., Sagron, R., Elovici, Y. and Shabtai, A., 2020. A novel approach for detecting vulnerable IoT devices connected behind a home NAT. *Computers & Security*, 97, p.101968.

https://doi.org/10.1016/j.cose.2020.101968

Summary of paper

This paper proposes a machine learning based mitigation technique for defending a network from the level of the NAT. The proposed method can identify IoT devices on a

users home network with known vulnerabilities and perform a number of actions, such as patching the device, rerouting packets from the device, or notifying the user of any vulnerabilities.

How is this paper relevant to solving your project problem or addressing your research question?

Home IoT devices have been used in past large scale DDoS attacks, and as such, a mechanism which can defend the network from the level of the attack source would prove efficient and beneficial.

What are the strengths and weaknesses of the solutions/methods/technologies proposed in this paper?

The proposed method was extensively tested, using a network containing 13 IoT devices. Performance metrics including training time and classifier size, were used for the selection of the machine learning algorithm. The presented results are in depth.
As noted in the study, the method may not be scalable due to the amount of time required to collect data from the IoT devices on the home network. Also the proposal to patch vulnerable devices is purely dependent on the device manufacturers cooperation and willingness to release firmware updates for the devices.

Log Entry Creation Date: Thu Feb 20 2020 11:05:08 GMT-0000 (GMT)

A Simulation Analysis of Flooding Attack in MANET using NS-3

Bandyopadhyay, A., Vuppala, S. and Choudhury, P., 2011. A Simulation Analysis of Flooding Attack in MANET using NS-3.

https://doi.org/10.1016/j.sysarc.2020.101827

Summary of paper

This paper presents an ns-3 based simulation of flooding attacks using MANETs. The paper discusses how the mobile aspect of a MANET increases the susceptibility to compromise, and shows how flooding in the network can lead to a denial of service.

How is this paper relevant to solving your project problem or addressing your research question?

While this paper focuses on MANETs, these types of networks can still be considered under the umbrella of connected devices that is the Internet of Things. The detailed simulation setup section also gives a good insight into the parameters and metrics which could be monitored during a DDoS simulation.

What are the strengths and weaknesses of the solutions/methods/technologies proposed in this paper?

This paper provides detailed setup and results information for the simulations which were run.

Log Entry Creation Date: Thu Feb 20 2020 11:05:08 GMT-0000 (GMT)

Software Defined Network Defense
Sathyanarayana, S., 2012. Software Defined Network Defense. [online] Available at: <https://www.academia.edu/1833986/Software_defined_network_defense>.
https://www.academia.edu/1833986/Software_defined_network_defense
Summary of paper
This paper demonstrates the Pushback Scheme DDoS defense mechanism, which uses the OpenFlow Software Defined Networking architecture for it's implementation. The paper evaluates Frenetic, the python based network programming language, in terms of efficiency and speed of attack detection and mitigation.
How is this paper relevant to solving your project problem or addressing your research question?
This paper presents a simulation, implemented using the Mininet simulator, which shows how mitigation and defense techniques can be introduced in SDN. As the Mininet simulator is being used, and the benefits of SDN being investigated, this paper shows how this defense strategy can be implemented using both.
What are the strengths and weaknesses of the solutions/methods/technologies proposed in this paper?
This paper uses Mininet to implement it's simulations, and gives some useful information for setting up and testing networks using Mininet. Due to the age of the paper, a number of features were missing from Mininet, such as the ability to limit link bandwidth, which means assumptions had to be made to determine when a denial of service had occurred.
Log Entry Creation Date: Thu Feb 20 2020 11:05:08 GMT-0000 (GMT)

Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics
Mahbub, M., 2020. Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. *Journal of Network and Computer Applications*, 168, p.102761.
https://doi.org/10.1016/j.jcna.2020.102761
Summary of paper
This paper presents a survey of the application areas of IoT devices, the architectures these devices use for communications, and a comprehensive review of the types of attacks which these devices are susceptible to. The presented information covers the area of IoT security from the level of infrastructure and protocols, to attack and defense techniques.
How is this paper relevant to solving your project problem or addressing your research question?

The first number of sections of this paper offers a lot of background information about the standards and networking protocols used by IoT devices and the areas in which these devices are used. Section 6, “Layers in IoT architecture”, breaks these networks down, comparing them to the equivalent OSI model layers. The last sections, 7 through 9, offer a lot of relevant information about the threats facing network connected devices.
What are the strengths and weaknesses of the solutions/methods/technologies proposed in this paper?
This paper presents an in-depth look at the vulnerabilities of IoT devices to attack, with information about the network protocols, and common attack types used on these devices. The strengths of this paper lie in the breadth of the information presented. The weaknesses of this paper, for the purpose of addressing my research question, are in the lack of practical demonstration of attacks, or of mitigation techniques.
Log Entry Creation Date: Thu Feb 20 2020 11:05:08 GMT-0000 (GMT)