Denial of Service (DoS) Attacks Against An Internet of Things (IoT) Security Camera

Yocelyne Hernandez, MiraCosta College
Ian Harris, P.h.D
Donald Bren School of Information and Computer Sciences, University of California, Irvine
NSF REU IoT-SITY Summer Research Program

INTRODUCTION

- Denial of Service (DOS) attacks are attacks meant to shutdown a machine or network, making it inaccessible to intended users
- IoT devices come with immense ricks on our security and privacy because they collect personal information and monitor user activity
- Research has been conducted to evaluate the security of IoT devices to find better ways to design them and eliminate or lessen any harmful effects done on them

Objectives:
- Review literature on DoS and DDos attacks and defenses
- Install OpenCV on Raspberry Pi 3 and access webserver

Challenges:
- Installing OpenCV on the Raspberry Pi 3
- Accurate algorithm to differentiate legitimate requests from malicious ones

BACKGROUND

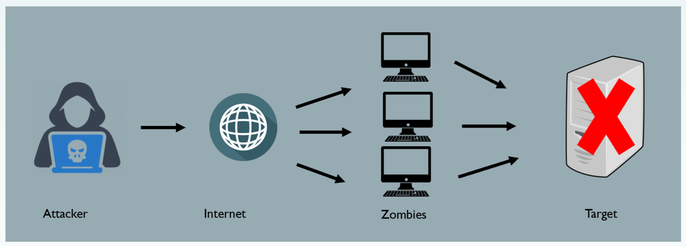

Figure 1. This diagram shows the typical structure of a DoS attack.

- The attacker will use the “zombies” and send attack commands though the zombies towards the target
- The Internet Protocol (IP) is based on packet-switching and supports ease of attachment of hosts to networks
- Little support for verifying the source address of packets thus making it difficult to identify the source of traffic
- Protocol-based bandwidth attacks gain their attack power based on the specific weaknesses of the Internet protocol

SYN FLOOD ATTACKS:

- Exploits a vulnerability of the TCP three-way handshake
- The attacker sends SYN packets with fake source IP addresses
- The server will store the requested information in a memory stack and wait to receive confirmation packets
- Since the IP addresses are nonexistent, the server will not receive the packets and half-open connections will start to accumulate and fill up the memory stack
- No legitimate requests will be able to be processed and the resources and services of the system will be disabled

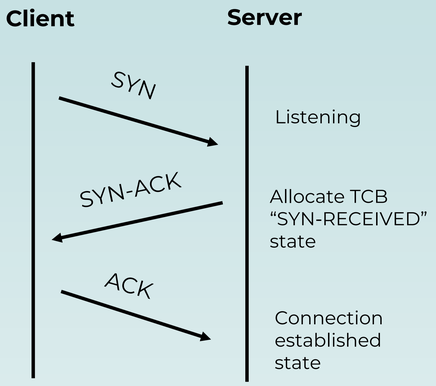

Figure 2. TCP Connection

METHODOLOGY

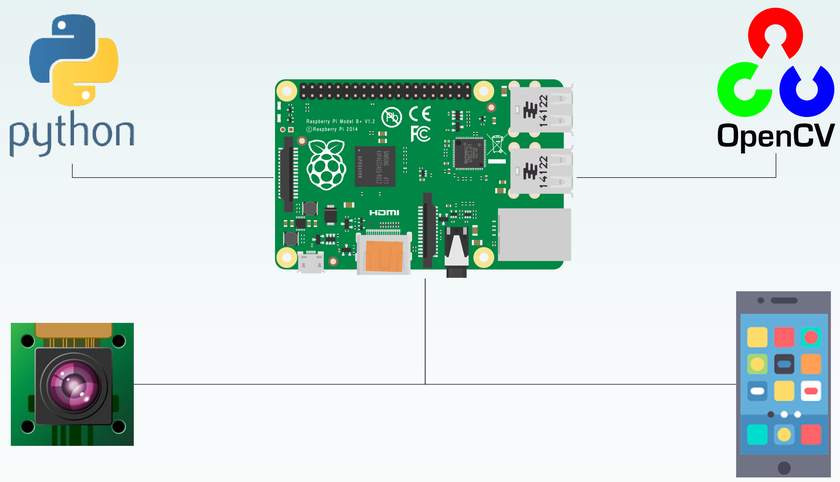

Figure 3. Architecture of the IoT security camera

After testing multiple systems such as the Arduino, ESP8266, and Raspberry Pi 4, we found that the Raspberry Pi 3 was the best system to use for designing the IoT camera.

REFERENCES

Peng, T., Leckie, C., and Ramamohanarao, K.2007. Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Comput. Surv. 39,* 1, Article 3 (April 2007), 42 pages DOI = 10.1145/1216370.1216373 http://doi.acm.org/10.1145/1216370.1216373

OUTCOMES

Figure 4. IoT Security Camera made using the Raspberry Pi 3.

Advantages of using the Raspberry Pi 3:
- Features can be added smoothly
- Webserver based

Challenges with IoT security camera:
- Installing OpenCV - a open source library for computer vision, image processing and machine learning

CONCLUSION

- Potential solutions to combating Denial of Service attacks successfully come with a long and difficult path to achieve
- A key challenges for defense is how to discriminate legitimate requests for service from malicious attacks
- The most effective DoS defense scheme is to detect and block attack traffic close to the source
- Defense schemes that follow such implementation are highly costly due to the difficulty of discriminating between legitimate and malicious traffic
- It is expensive and at times impossible to eliminate DoS attack problems entirely.

Future work for this project consists of:
- Writing attack scripts against the IoT camera
- Evaluating the security of the camera
- Designing defense mechanisms that are resistant to such attacks

ACKNOWLEDGEMENTS

I would like to thank my mentor, Dr. Ian Harris, for his support and guidance throughout this research. I am grateful for Dr. Nalini Venkatasubramanian valuable advice throughout this project. I would also like to thank Dr. Sharnnia Artis for organizing and facilitating the REU program and for Ernest Garrison's guided help in developing the security camera. I would also like to acknowledge NSF for sponsoring and funding the REU program.