Exploring Cybersecurity Vulnerabilities in IoT Devices

Julia Chaidez

PolySec Lab, Computer Science, Cal Poly Pomona

Faculty Advisor: Dr. Mohammad Husain, Cal Poly Pomona

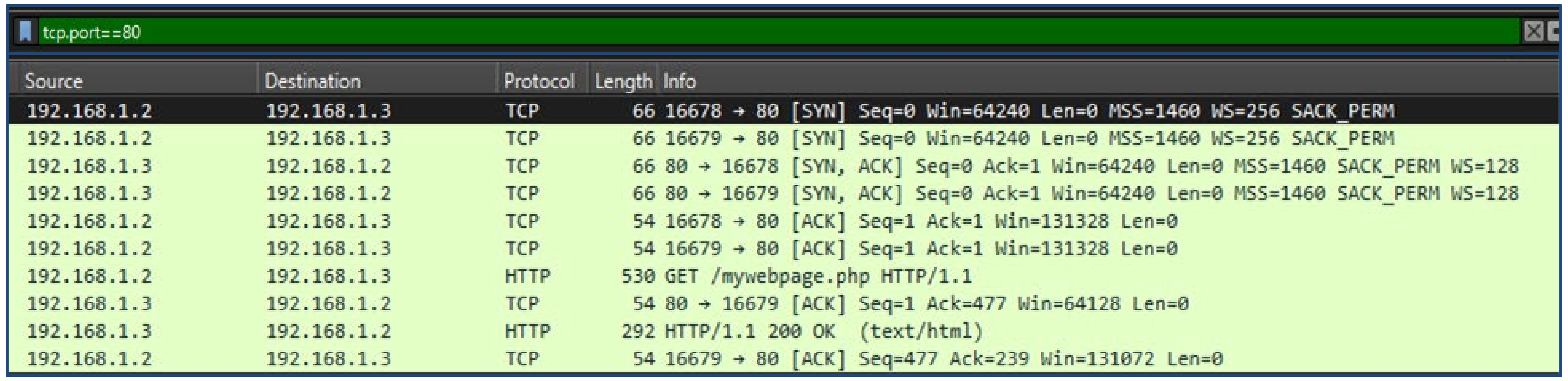
Problem

An Internet of Things (IoT) device is any device that communicates through a wireless network. Examples include your phone, smartwatch, smart light bulb, security camera, and even smart refrigerator. In recent years, the proliferation of IoT devices has surged due to consumer demand. They are highly attractive due to their potential to automate many daily tasks, making life more convenient and business operations more efficient, ultimately enhancing our lives. However, they remain vulnerable to cyberattacks. The goal of this project is to comprehend the TCP/IP model, explore the physical layer of wireless communication, and investigate vulnerabilities present in IoT devices utilizing tools such as Raspberry Pi and HackRF One.

Approach

Part A: I began by setting up a Raspberry Pi as a web server and hosting a basic website on it. Then, I used a router to connect the Raspberry Pi and my PC to the same network so I could access the website from my PC. Using Wireshark, I captured and analyzed the network traffic. This hands-on approach helped me to understand how data traverses across various network layers and provided practical insight into the transport layer of the TCP/IP model.

Part B: Transitioning to an exploration of the physical layer, I worked with HackRF One, a software-defined radio (SDR) capable of capturing radio frequency signals. Given that WiFi utilizes radio frequencies for data transmission, HackRF's functionality extends to capturing WiFi signals. However, due to its focus on the physical layer, HackRF alone cannot interpret TCP/IP packets. To overcome this limitation, I used Wireshark to demodulate and extract the packets needed for analysis.



```
tcp.port==80

Source          Destination     Protocol  Length Info
192.168.1.2     192.168.1.3     TCP          66 16678 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
192.168.1.2     192.168.1.3     TCP          66 16679 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
192.168.1.3     192.168.1.2     TCP          66 80 → 16678 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
192.168.1.3     192.168.1.2     TCP          66 80 → 16679 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
192.168.1.2     192.168.1.3     TCP          54 16678 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
192.168.1.2     192.168.1.3     TCP          54 16679 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
192.168.1.2     192.168.1.3     HTTP        530 GET /mywebpage.php HTTP/1.1
192.168.1.3     192.168.1.2     TCP          54 80 → 16679 [ACK] Seq=1 Ack=477 Win=64128 Len=0
192.168.1.3     192.168.1.2     HTTP        292 HTTP/1.1 200 OK  (text/html)
192.168.1.2     192.168.1.3     TCP          54 16679 → 80 [ACK] Seq=477 Ack=239 Win=131072 Len=0
```

Figure 1: Wireshark Packet Capture (Part A)

Challenges

The most challenging part of this project is bridging the gap between the transport and physical layer. While devices utilizing WiFi are easily accessible on the physical layer, the issue is translating the analog signals captured by the HackRF into analyzable data. Part B remains a work in progress, as I have yet to successfully analyze any packets on Wireshark. The need for additional processing of the analog signal to demodulate, filter, and decode the captured data presents a significant challenge. Additionally, factors such as the HackRF's constrained frequency bandwidth and potential noise within specific channels can further constrain its ability to capture WiFi signals effectively.

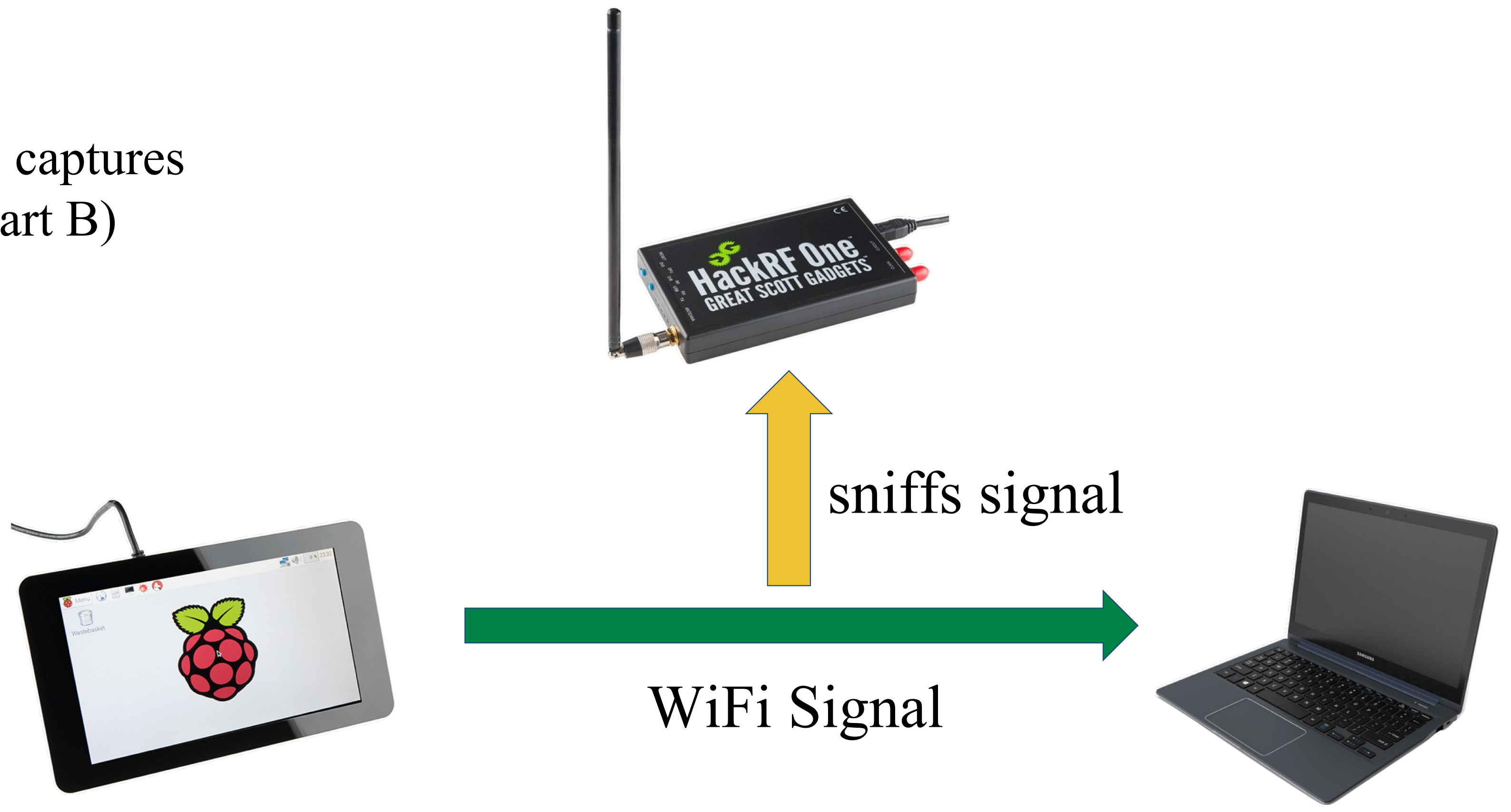


Figure 2: HackRF captures WiFi signal (Part B)

Future Work

Through intercepting and analyzing WiFi signals, I recognized the susceptibility of IoT devices to unauthorized access, highlighting the critical need for strong cybersecurity measures in a time of increased connectivity. Future direction may include exploring the use of machine learning algorithms to help with network traffic detection. This may be an interesting route for researching how to improve the resilience of IoT devices.

References and Acknowledgements

Shuler, R. (2002). *How the Internet works* – https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm

Hung, P. D., & Vinh, B. T. (2019). *Vulnerabilities in IoT devices with software-defined radio. IEEE Xplore*. doi:10.1109/CCOMS.2019.8821711

This project was funded, in part, by the SPIRES program (NSF grant 1834186) and the CSU-LSAMP program (NSF grant HRD-1826490) at Cal Poly Pomona