Weapon Systems Cyber Protection

Felicia Ip, De’Shauna Downs, Nick Gould, Sumeet Ramani
George Mason University
4400 University Dr, Fairfax, VA 22030

Introduction

Modern weapon systems, software and data communication systems are inherently vulnerable to many different attack techniques due to the lack of cybersecurity prioritization. Until recently, cybersecurity has been non-existent or has been used as a “bolt-on” solution. Critical weapon systems have a higher impact if compromised, so it is imperative that these systems are protected. Our stakeholders include the United States government contractors, military, law enforcement, etc. Our system shall be used to help protect weapon systems from cyber attacks and ensure system resilience.Our project will utilize a raspberry pi that will transmit sensor data to be a representation of a weapon system by allowing us to understand the systematic architecture, demonstrate how to secure weapons and its data while using object and facial recognition. In the initial phase of our project, we have created a backlog of system tasks and capabilities. Within our backlog, we explicitly categorize our tasks as either process or product, where we focus perfecting all of the process tasks first. We developed a ConOps to describe our system from deploying and maintaining the devices through the lifecycle of the weapon’s system from the viewpoint of an individual who will be using the system. Our sponsor, Northrop Grumman, has required us to maintain a backlog of system tasks, capabilities, architectural diagrams, and key system information as well as completing new tasks in sprints. During this phase, we determined the best approach for our system through research of the different components such as hardware and software requirements. We then outline the approach to creating a small factor, low power, environmentally resilient network protection device. For our system, we have two raspberry pi’s represented as an AWS EC2 instance and physical development lab, serving as inflight and as a ground station. Our grounded pi is configured and maintained while the software from the development labs flow onto the pi or “weapon system” once it is “deployed”. The inflight pi produces the data and sends it back to the development labs to be further analyzed by AWS Rekognition. Based on the data, an action will trigger upon the existence of particular factors/objects. Through designing our solution, we verified our work by ensuring that we followed through with cyber security best practices such as identity and access management, secure coding practices, and security configurations on our device and platform. We also ensured that our customer’s expected deliverables were met. In order to validate that our solution meets requirements, it is necessary to demo points-of-entry by conducting vulnerability assessments and penetration testing to test our resilient system.

Stakeholder

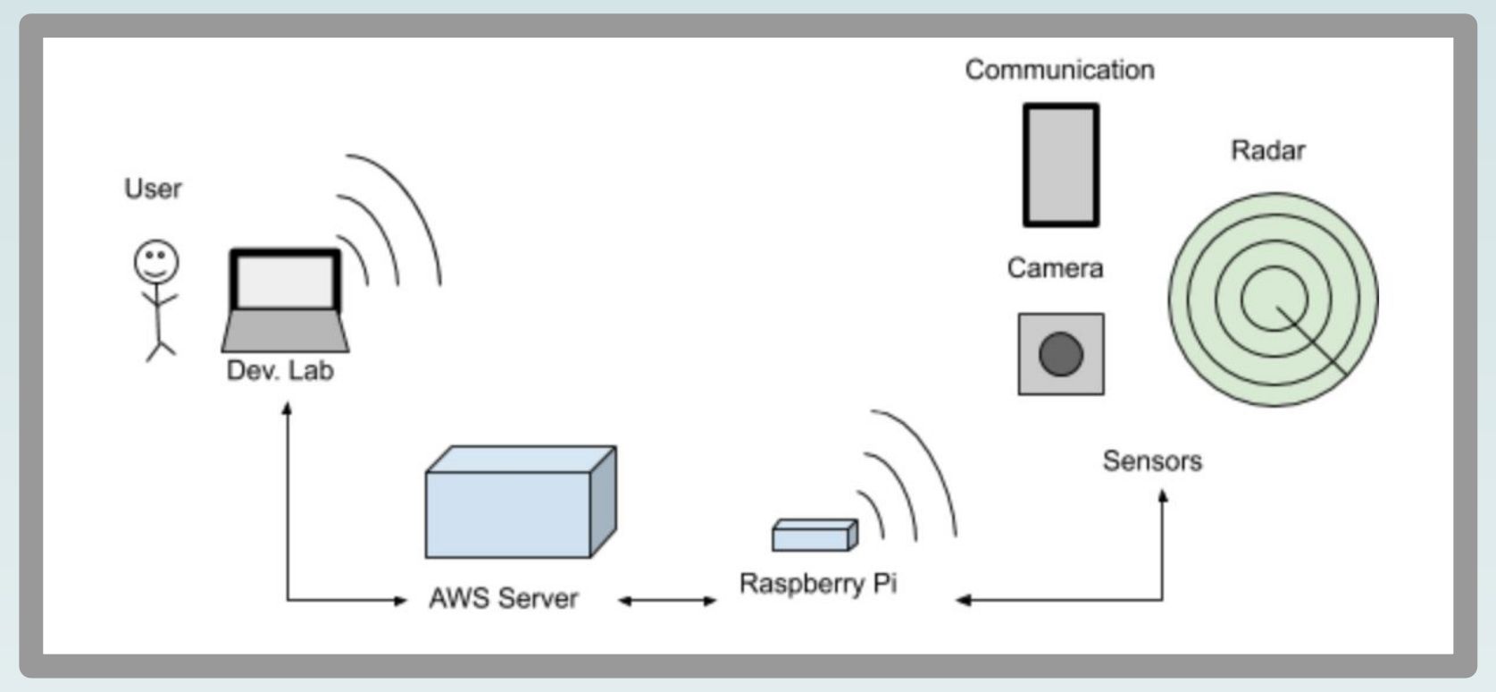
In order to identify the parties that will be affected by our project, we recognized our stakeholders to include Northrop Grumman, the U.S Government and George Mason University, using the power interest grid methodology. Within this approach, we make assumptions to individuals that hold high and low influence and high and low interest in our project as a whole. Next, we assessed the levels of interests and influence within our identified stakeholders. Since Northrop Grumman is the sponsor and the customer of our project, the level of interest and influence remain high as we must satisfy all requirements posed by the customer. Subsequently, George Mason University serves as the next stakeholder with as the next high power/high interest due to the nature of financial support and creation of the project as a whole. The university is responsible for the project; therefore, constant communication is maintained between both Northrop Grumman and George Mason University. Ultimately, we foresee the U.S Government as our final stakeholder considering our project involves weapon system improvement and the current customers of Northrop Grumman.

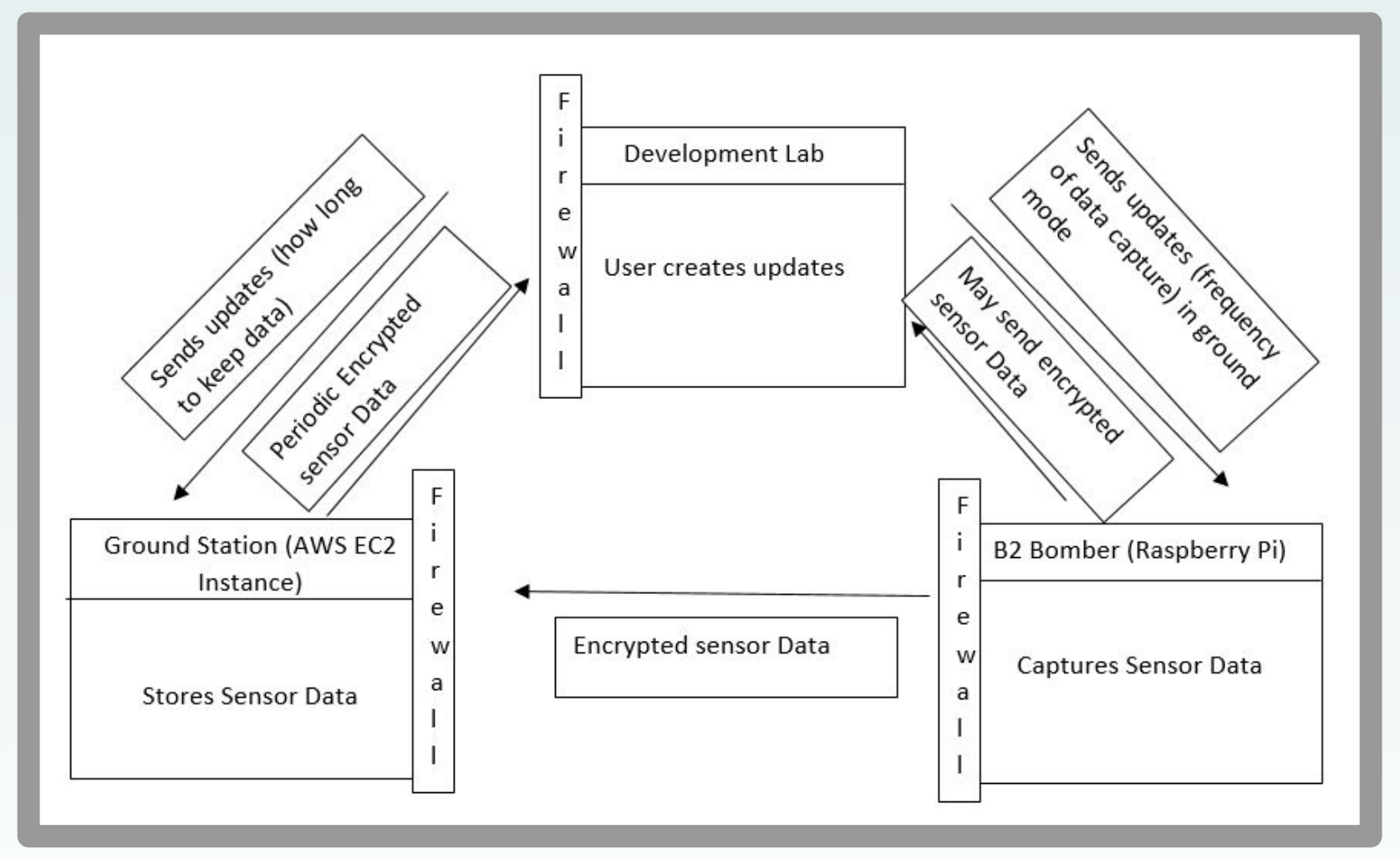
Problem Statement

Modern weapon systems are vulnerable to many different attack techniques due to not prioritizing cybersecurity. These attack techniques are not limited to but include: EM/signal and sensor spoofing, EM/signal and sensor jamming, data injection, malicious software updates either via usb or by SOTA, hardware attacks via supply chain or physical attacks and access control to name a few. Until recently, they have been nonexistent or have been using a “bolt on” cyber system. These critical weapon systems have a high impact if compromised, so it is imperative that they are protected. A real-world example that demonstrates this is the Iran-U.S. RQ-170 Incident. In 2011, an unmanned U.S. UAV was captured by Iran. They did this by first jamming the drones connection back home base. This caused the Drone autopilot to kick in and return back to base. From there, Iran spoofed telemetry data to the drone to make it think it was back at base, which caused the drone to ‘crash’ land. Yes, the signals were encrypted; however, this is an example of how cyberware was used to get around a weapons system that had little protections against it. Another example is dated even further back to the Kosovo War in 1999. The Yugoslavian army used EM waves emitted by magatrons found in microwave ovens to spoof targets and fool billion dollar NATO missile systems. This greatly affected the reliability and accuracy of these missile systems. This is just another example of real life events where cybersecurity was used to attack and disrupt weapon systems. Examples such as these demonstrate the importance and necessity for weapons systems to have substantial safeguards against cyber security attacks. This project utilizes a raspberry pi that transmits sensor data to be representative of a weapon system. This allows us to demonstrate a broad example of how to secure a weapon system and its data and to address the cybersecurity concerns that come with this system and how to safeguard against cybersecurity attacks.

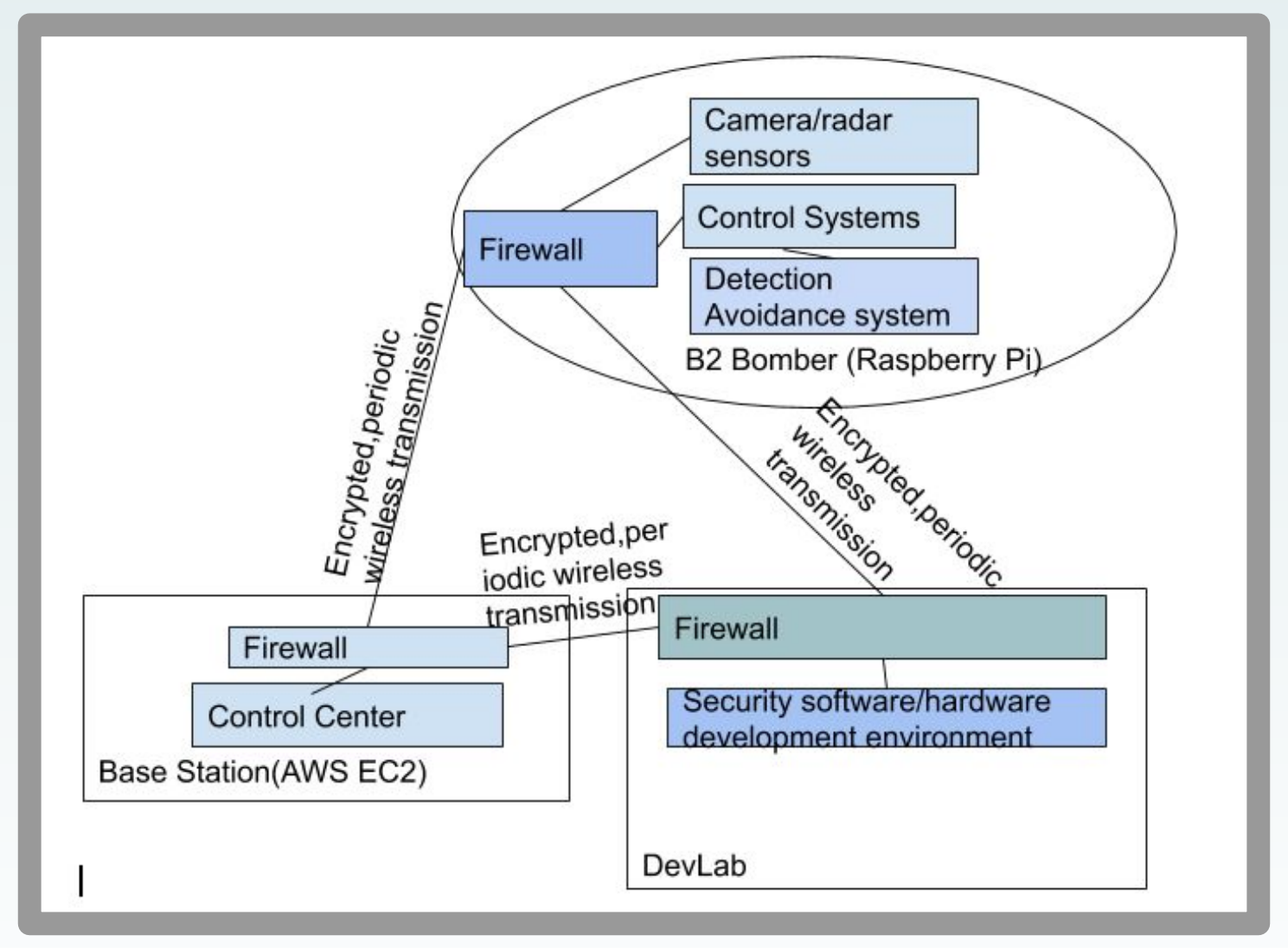
Con-Ops

For our ConOps, our system starts from deploying and maintaining the devices through the lifecycle of the weapon’s system from the viewpoint of an individual who will be using the system. During this phase, we determined the best approach for our system through research of the different components such as hardware and software requirements. Our approach is to create a small factor, low power, environmentally resilient network protection device. For our system, we have two raspberry pi’s represented as an AWS EC2 instance and physical development lab, serving as inflight and as a ground station. Our grounded pi is configured and maintained while the software from the development labs flow onto the pi or “weapon system” once it is “deployed”. The inflight pi produces the data and sends it back to the development labs to be further analyzed by AWS Rekognition.





Development Lab
User creates updates
Firewall
Sends updates (how long to keep data)
Periodic Encrypted sensor Data
Sends updates (frequency of data capture) in ground mode
May send encrypted sensor Data
Ground Station (AWS EC2 Instance)
Stores Sensor Data
Firewall
Encrypted sensor Data
Firewall
B2 Bomber (Raspberry Pi)
Captures Sensor Data



Camera/radar sensors
Control Systems
Firewall
Detection Avoidance system
B2 Bomber (Raspberry Pi)
Encrypted,periodic wireless transmission
Encrypted,periodic wireless transmission
Encrypted,per iodic wireless transmission
Firewall
Control Center
Base Station(AWS EC2)
Firewall
Security software/hardware development environment
DevLab

Implementation As Prototype

Since we do not have access to an actual bomber, we have to emulate the system as best we could. Our ground station is a virtual machine (called EC2) and a storage device (called S3) in AWS. The S3 is exposed to the internet for incoming data, but has a basic firewall in place, so that only allowed connections can connect to it [2]. The bomber is being modeled by a raspberry pi with a camera attachment to it. The testing lab stations are our personal laptops. The EC2 instance and our personal laptops can connect directly to the pi via ssh to either give commands or push updates. The pi captures data in the form of pictures and sends them to the S3. from there the pictures get sent to the ground station (EC2) and also gets sent to AWS Rekognition service to help use machine learning to identify objects and help the ground station make decisions that will tell the pi what to do. Each part of this overall system communicates using ssh or amazons boto3 sdk which uses https. If communication between the pi and the ground station is interrupted then the pi stores the pictures it takes onboard and then once connection is reestablished to the ground station it will send the stored pictures.Therefore, a somewhat secure data gathering,data transmitting, decision making, and somewhat securely communicating weapons system that is somewhat resilient is being emulated.

Verification

To verify our work, we are ensuring that we follow through with cyber security best practices such as identity and access management, secure coding practices, and security configurations on our devices and platform [4]. We also ensured that our customer’s expected deliverables were met. As we had planned for further testing, an unforeseeable issue has risen. There has been a global pandemic that forced our team to delay our project resulting in the lack of concrete results to provide.

Validation

To validate the requirements of our system, we will demonstrate the resilience of our weapon system. To do this, we will perform different types of cyber attacks based on our vulnerability assessment and penetration testing. An example would be testing an injection attack to make sure that there aren't any vulnerabilities to allow the attack to succeed. Our system will be set up and deployed in other various conditions to see the results and progressively create a resilient system. As the device is hardened against different attacks it will continuously be tested by the group or other class members. Due to unfortunate circumstances, validation has been delayed and there are no results as of yet.

Test Plans / Results

The validation will be accepted if the attacks against the PI are unsuccessful in compromising the device. If the attack is successful, the team will go back and evaluate how the attacker was able to compromise a vulnerability and develop a solution. Due to unfortunate circumstances, acceptance has been delayed and there are no results as of yet.

References

[1]Product Plane. “Project Management - Stakeholder Analysis”, Accessed on Oct. 16, 2019. [Website]. Available: https://www.productplan.com/glossary/stakeholder-analysis/

[2]Amazon Web Services. “Amazon EC2 Instance Types”, Accessed on Sept. 12, 2019. [Website]. Available: https://aws.amazon.com/ec2/instance-types/

[3]Northrop Grumman Corporation, “B-2 Stealth Bomber”, Accessed on Sept. 12, 2019. [Website]. Available: https://www.northropgrumman.com/air/b-2-spirit-stealth-bomber/

[4]C. Segal. “8 Cyber Security Best Practices For Your Small Business To Medium-Sized Business.” Cox Blue. Accessed on Mar. 23 2020. [Website]. Available: https://www.coxblue.com/8-cyber-security-best-practices-for-your-small-to-medium-size-business-smb/

[5]A.Mishra, “Machine learning in the AWS Cloud: Add Intelligence to Applications with Amazon SageMaker and Amazon Rekognition,” *Amazon*, 2019. [Website]. Available: https://aws.amazon.com/rekgnition/.[Accessed: 24-Mar-2020].

[6]“B-2 Stealth Bomber,” *Northrop Grumman*. [Online]. Available: https://www.northropgrumman.com/air/b-2-spirit-stealth-bomber/. [Accessed: 24-Mar-2020].