Death Star Plans Radio Transmitter

Team Projects I

Group 10

Team Introduction

Zachary Leyes: CEG

Luke Kremer: CS

Jeremiah Hackman: ITC

Julie Peterson-Ramos: EE

Khiem Do: CS

JPR

Overview

- Common Terms
- Problem Statement
- History/Background
- Use Case
- Impact
- Technical Review
- Design Trades
- Design Components
- Component Trades
- Hardware Overview
- Software Overview
- Encrypt/Decrypt Breakdown
- Budget
- Risks and Mitigations
- Test Plan
- Timeline
- Milestones and Deliverables
- Questions/Contact Info

JPR

Common Terms

AES – Advanced Encryption Standard

IEEE – Institute of Electrical and Electronics Engineers

FCC Regulations – Rules established by the U.S. Federal Communications Commission that governs the legal use of frequency ranges.

JPR

Problem Statement

- The Rebellion needs to reveal the Death Star’s weaknesses.
  - The images are stored on a USB thumb drive
- An undercover engineer will access the images through a raspberry pi and send them to a Rebel Server.
  - The engineer can not use Wifi, Cellular, or Bluetooth to send the images
  - The transmission must be done under 10 minutes
  - The images need to be encrypted
- The raspberry pi also contains a message from Princess Leia
  - This message can be seen by everyone but the full message is only for Obi Wan

ZL

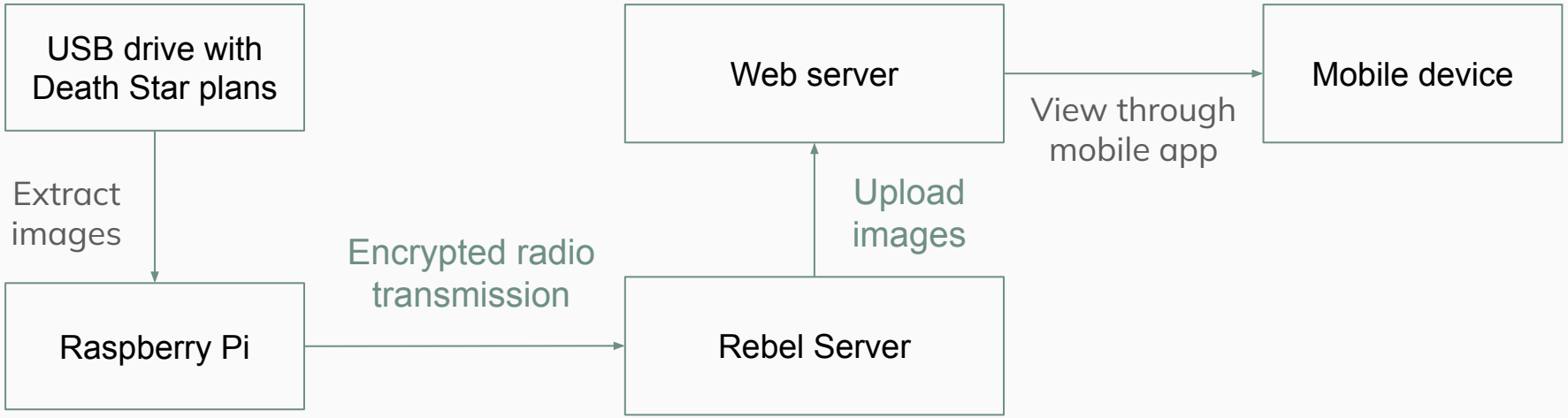
History/Background

- Origins: Rebel Intelligence recovered critical reconnaissance photos and a coded message from Princess Leia on a covert USB drive.
- Strategic context: The Death Star represents an existential threat, and its weaknesses must be identified and delivered to command before the Empire relocates or destroys evidence.
- Why it matters: Rapid, secure transfer preserves the tactical timeline for a coordinated strike, prevents enemy interception, and protects the identities of assets and informants.
- Mission impact: Successful transmission shortens decision time for fleet command, increases survivability of Rebel units, and directly enables planning to exploit identified Death Star vulnerabilities.

LK

Use Case

The Death Star plans are stored on a USB drive. The system will extract the plans, encrypt them, transmit them with radio waves to a Rebel Server, decrypt them, and upload them to a web server so Rebels can view the plans with a mobile app.



ZL

Impact

- **Cultural**
  - Stealing data violates cultural norms
- **Economic**
  - Inexpensive components
  - Financial costs on victims
- **Environmental**
  - Small impact - small amounts of electricity, processing power, and low frequency radio waves
- **Global**
  - Stealing the plans contributes to the collaborative fight against the Empire
- **Public health**
  - No effect on public health: - low frequency em waves
- **Public safety**
  - No effect on public safety - no moving parts, sharp edges, or emissions
- **Public welfare**
  - Disclosing the plans exposes the empire's militaristic ambitions

JMH

Technical Review: **Requirements**

Requirement 1: The Raspberry Pi shall load images from the USB drive.
Requirement 2: The Raspberry Pi shall identify images with red circles.
Requirement 3: The Raspberry Pi shall have the ability to encrypt images.
Requirement 4: The Rebel Server shall have the ability to decrypt images.
Requirement 5: The Raspberry Pi shall have the ability to transmit and receive data with radio frequency waves.
Requirement 6: The Rebel Server shall have the ability to transmit and receive data with radio frequency waves.
Requirement 7: After receiving a transmission, the Rebel Server shall perform error checking.
Requirement 8: In the case of an error, the Rebel Server shall send a transmission to the Raspberry Pi requesting to resend the data.

JMH

Technical Review: **Requirements**

Requirement 9: If the Raspberry Pi receives a request to resend a transmission, then it will send the image again.
Requirement 10: The system shall complete all transmissions in 600 seconds or less.
Requirement 11: Any user shall have access to the first video.
Requirement 12: Authorized users shall have exclusive access to the second video.
Requirement 13: The mobile app shall use a secure method of authentication to identify authorized users.
Requirement 14: The mobile app shall display images in a scrollable table.
Requirement 15: The mobile app shall display up to 10 images.
Requirement 16: The scrollable table shall display the contents of each red circle exactly once.

JMH

Technical Review: Assumptions

Assumption 1: The provided room will have a standard 120 V and 60 Hz power supply.

Assumption 2: The Rebel Server will be placed 5 to 10 meters from the lab window.

Assumption 3: Obi-wan will have access to an email account as well as an account on the Rebel website.

Assumption 4: Princess Leia’s messages will be in a video format.

Assumption 5: Ambient noise and interference in the radio frequency band chosen will remain low enough for successful communication.

Assumption 6: The Rebel Server can communicate via Wi-Fi with the WSU_EZ network.

JMH

Technical Review: Constraints

Constraint 1: The total cost of the project shall not exceed $300 without Faculty Advisor approval.

Constraint 2: The solution shall use only the provided equipment plus additional components purchased within the budget; a personal mobile application host device is required.

Constraint 3: The Raspberry Pi and all equipment connected to it must fit within the provided box.

Constraint 4: The Raspberry Pi and Rebel server shall not communicate with each other using Wi-Fi, Bluetooth, cellular communication, or a wired connection.

Constraint 5: The Rebel Server and all its components shall be placed at least 5 meters from the Raspberry Pi.

Constraint 6: The range of frequencies used shall be compliant with FCC regulations.

JMH

Technical Review: **Standards**

1. The solution shall comply with AES FIPS 197-upd1 for encryption.
2. The solution shall comply with C95.3-2021 for radio frequencies.
3. The mobile application shall comply with IEEE 23026-2023 for website design.
4. All Python code shall comply with PEP 8 for coding style.

LK

Design trades

Radio frequency:

- Easy to set up
- High transmission speed
- Requires radio transceiver
- Can transmit through wall

Infrared:

- Difficult to set up
- Half the transmission speed of RF

QR codes:

- Designed to transmit hyperlinks, not images
- Requires camera

LK

Design components

Microcontroller

- Processing power
- Cost
- Size

RF transceiver module

- Frequency
- Transmission speed
- Bidirectional transmission
- Error correction
- Cost
- Range
- Power supply

Design components

Image processing

- Cost
- Compatibility
- Ease of implementation

Encryption

- Encryption algorithm
- FIPS certified
- Cost
- Language compatibility

LK

Design components

Mobile app framework

- Scrollable table
- Two-factor authentication
- Cost
- Development Time

Web server architecture

- Cost
- Hosting
- Customization
- Performance
- Support

LK

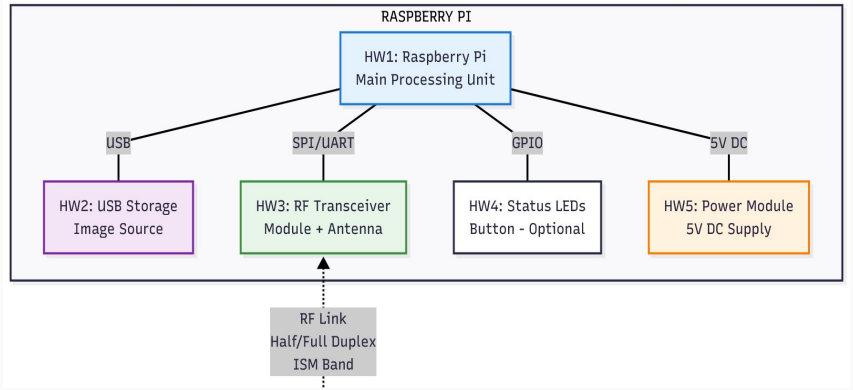
Component trades

- Raspberry PI - Raspberry Pi 4 (Broadcom BCM2711)
- RF Transceiver - NRF24L01+ (Nordic Semiconductor)
- Website - Local Server
- Encryption Library - OpenSSL (FIPS)
- Image Processing Algorithm - OpenCV (Hough Circles)
- Mobile App Framework - Flutter
- Coding Language - Python

JPR

Hardware Overview

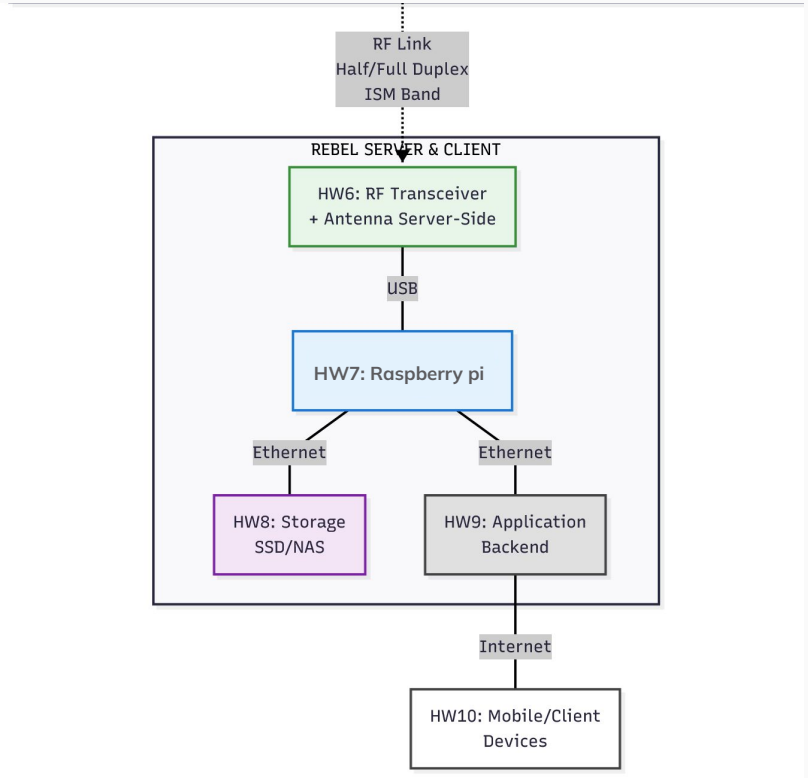
1. HW1 Raspberry Pi – Single-board computer executing image selection, encryption, packetization and retransmission logic.
2. HW2 USB Storage – Local mass storage holding the input images set to be scanned/selected.
3. HW3 RF Transceiver Module (Pi-side) – ISM-band transceiver, provides non-Wi-Fi/BT/cellular wireless transport.
4. HW4 Status I/O (optional)
5. HW5 Power Module – 5V DC supply for the Pi and RF module



JPR

Hardware Overview

1. HW6 RF Transceiver (Server-side)
2. HW7 Raspberry Pi – Receives RF packets, verifies integrity, issues ACK/NACK, also performs decryption
3. HW8 Storage (SSD/NAS) – Persistent storage for received files, logs, and metadata
4. HW9 Application Backend – APIs, authentications, and content services that the are hosted on local computer
5. HW10 Mobile/Client Devices – User devices that browse images and play videos per access policy

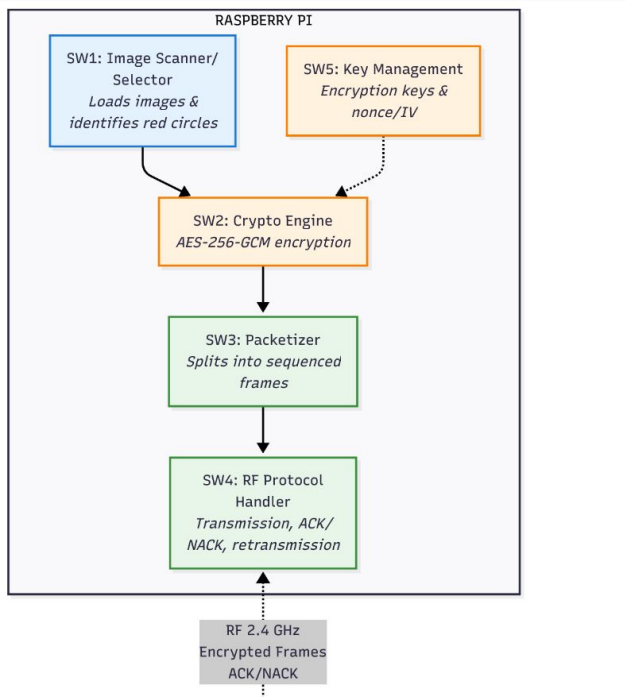


LK

Software Overview

Raspberry Pi Software:

- SW1 Image Scanner/Selector
- SW2 Crypto Engine
- SW3 Packetizer
- SW4 RF Protocol Handler
- SW5 Key Management



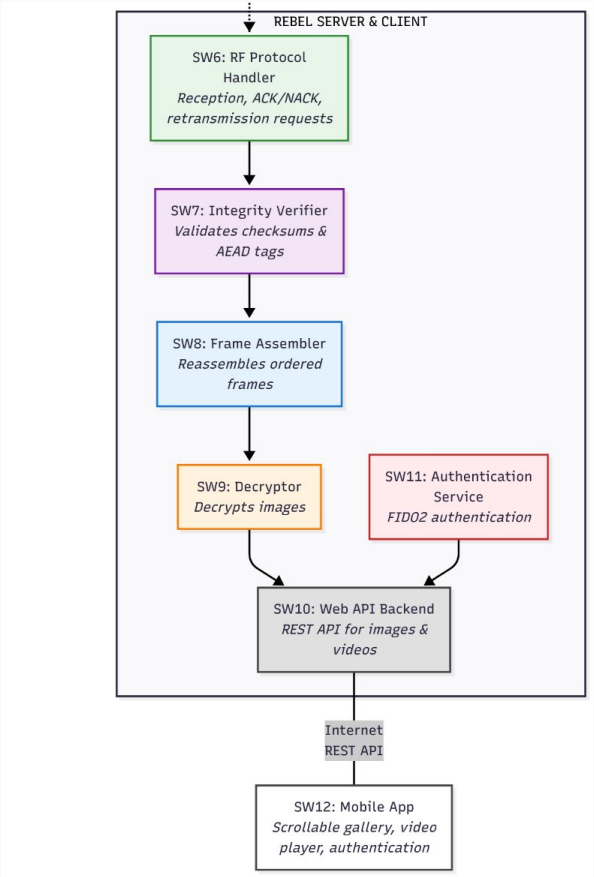
Software Overview

Rebel Server Software:

- SW6 RF Protocol Handler
- SW7 Integrity Verifier
- SW8 Frame Assembler
- SW9 Decryptor
- SW10 Web API Backend
- SW11 Authentication Service

Mobile app:

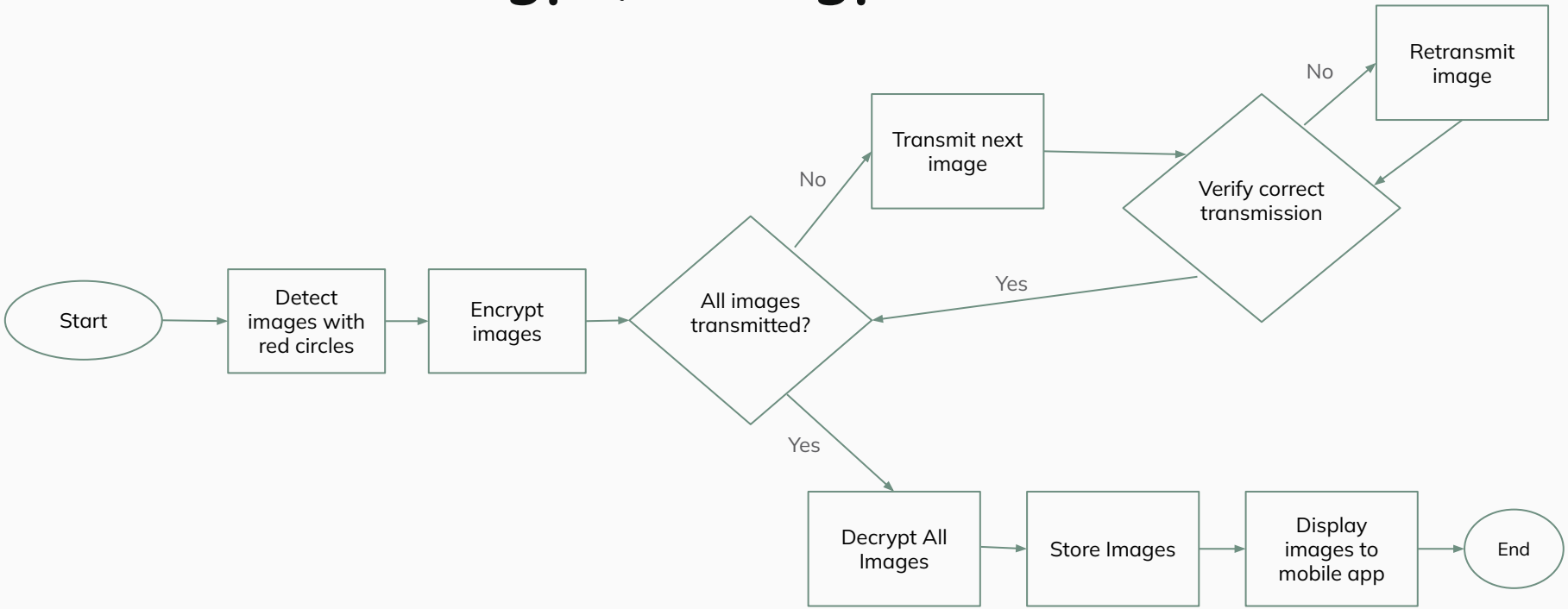
- SW12 Mobile App



LK

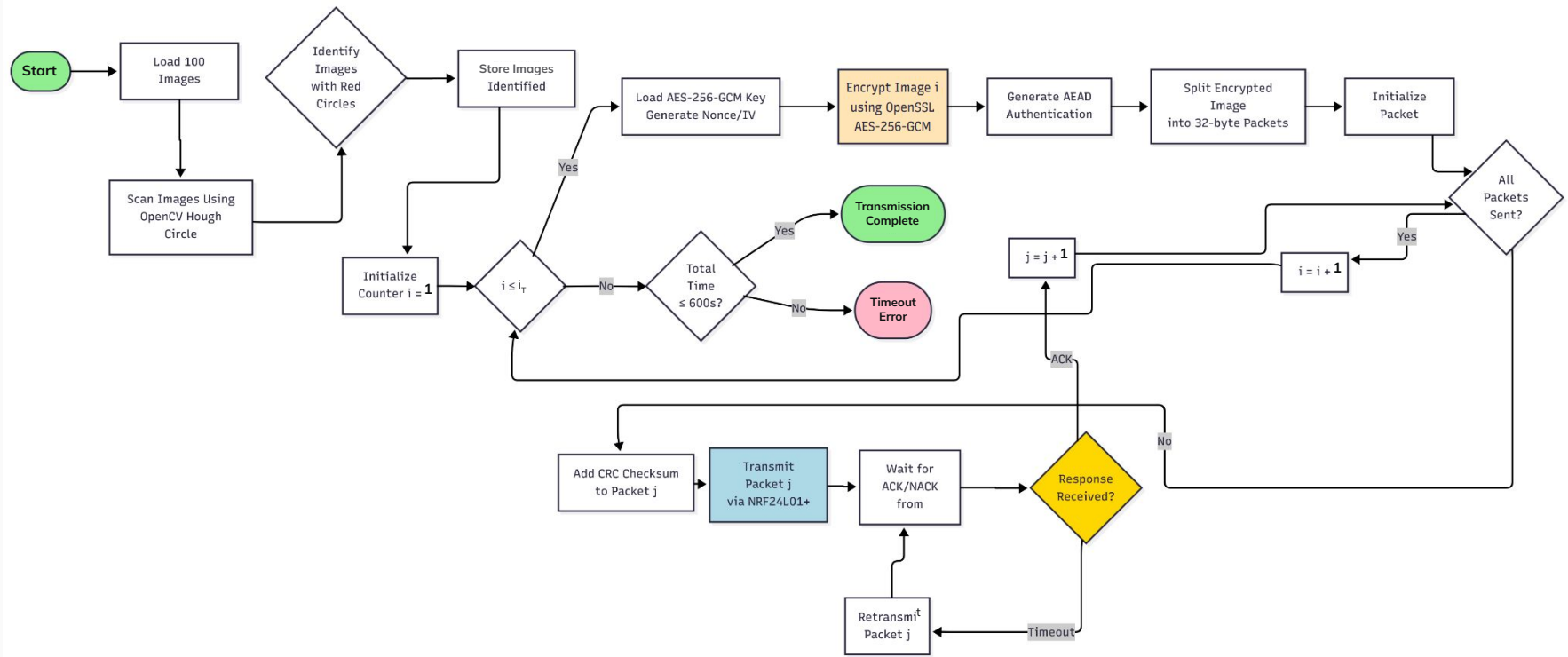
KD

Overall Encrypt/Decrypt Breakdown



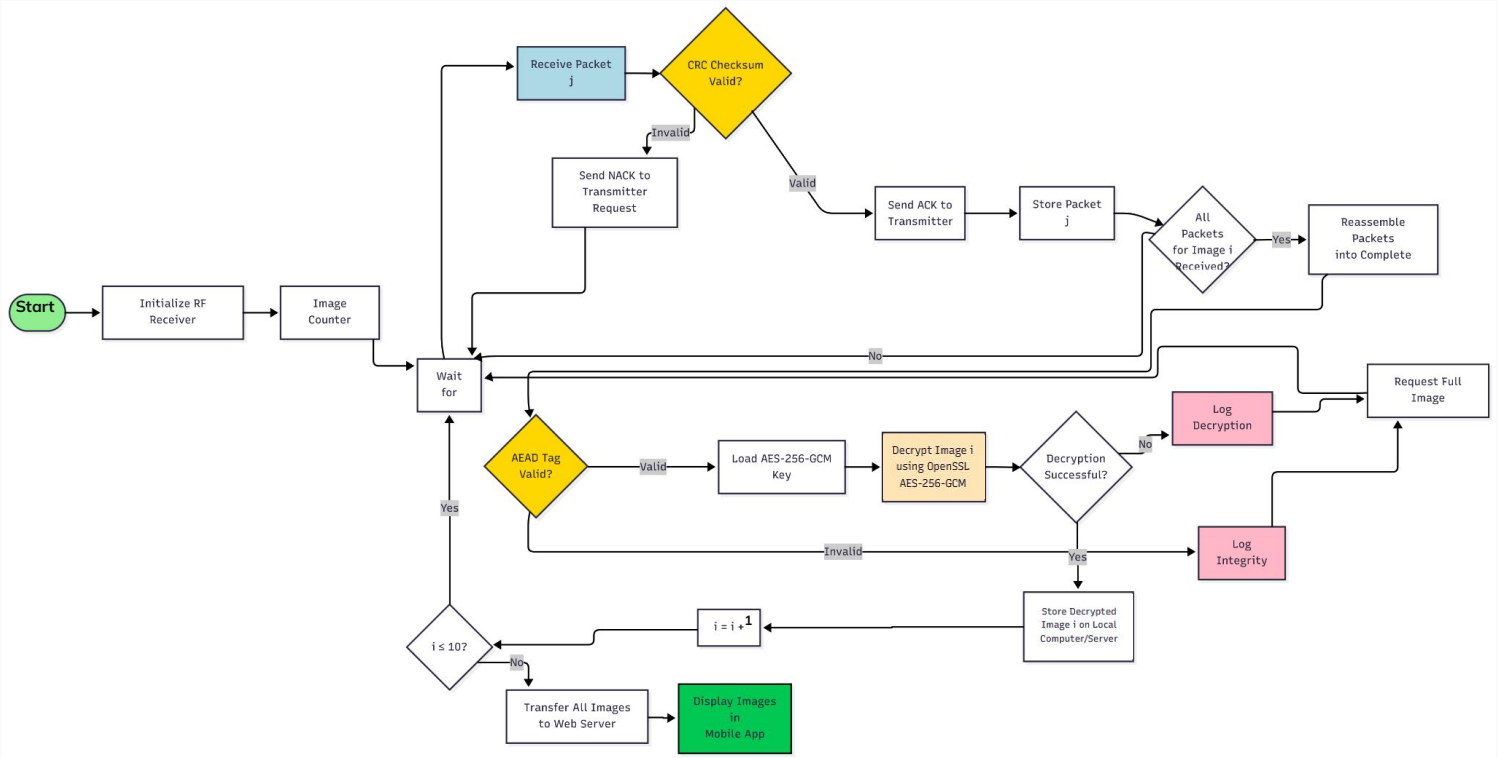
KD

Encryption Breakdown



KD

Decryption Breakdown



JPR

Budget

Bill of Materials:

1. Raspberry Pi 4B
   $30.00
2. Raspberry Pi 4 (Broadcom BCM2711)
   $67.99
3. NRF24L01+ Transceivers
   $13.99
4. Jumper Wires
   $5.97
5. 2 Power Cord
   $10.00

Total:
$127.95 out of the given $300

Vendor	Item #	Description	Qty	Price	Total
Amazon	BC22523	NRF24L01+ Transceivers	1	$13.99	$13.99
Amazon	765756931182	Raspberry Pi 4B 4GB	1	$67.99	$67.99

Risks and Mitigations

LK

- Risk of late/damaged parts. Likelihood is low but the severity of the impact is high.
- Mitigation: minimize the likelihood by ordering parts as early as possible and inspecting them as soon as received.

- Risk of incorrect parts being ordered. Likelihood is low and severity is moderate.
- Mitigation: there is still money left in our budget if we need to order another part.

- Risk of insufficient radio bandwidth. Likelihood is moderate and severity is moderate.
- Mitigation: order and test radio early to ensure bandwidth will be high enough to transmit images in time limit.

- Risk of violating the FCC regulations. Likelihood is low and severity is high.
- Mitigation: minimize the likelihood by constantly checking the guidelines and ensuring the frequencies do not violate them.

LK

Risks and Mitigations

- Risk of electrocution. Likelihood is low and severity is high.
- Mitigation: follow proper safety precautions when handling all electronic components.

- Risk of mobile application not being fully functional. Likelihood is low and severity is high.
- Mitigation: minimize likelihood by creating the application to do the bare minimum to meet requirements before adding anything else.

- Risk of leaked AES key. Likelihood is low and severity is high.
- Mitigation: minimize likelihood by replacing compromised keys and ensuring there is another form of encryption and decryption that can be used.

ZL

Test Plan - Requirements

Req No.	Test Method	Evaluation Method	Threshold	Objective
10	Raspberry Pi will be provided with USB drive containing 100 test images	Direct observation that images are loaded into memory without errors	100% of images loaded successfully	The Raspberry Pi shall load images from the USB drive.
20	Run OpenCV Hough Circle detection algorithm on all 100 images	Compare identified images against ground truth list of 10 images with red circles	100% accuracy (all 10 identified, 0 false positives)	The Raspberry Pi shall identify images with red circles.
30	Apply AES-256-GCM encryption to test image using OpenSSL	Verify ciphertext differs from plaintext; measure encryption time	Successful encryption with valid AEAD tag	The Raspberry Pi shall have the ability to encrypt images.
40	Receive encrypted test image and decrypt using matching key	Binary comparison of decrypted image against original plaintext	100% match (bit-for-bit identical)	The Rebel Server shall have the ability to decrypt images.

ZL

Test Plan - Requirements

Req No.	Test Method	Evaluation Method	Threshold	Objective
50	Transmit test packet via NRF24L01+ at 2.4 GHz	Use spectrum analyzer to verify RF transmission and RF24 library to confirm data sent	Successful transmission detected on correct frequency	The Raspberry Pi shall have the ability to transmit and receive data with radio frequency waves.
60	Configure Rebel Server with matching NRF24L01+ module	Receive test transmission and verify payload integrity	Successful reception with 0 bit errors	The Rebel Server shall have the ability to transmit and receive data with radio frequency waves.
70	Transmit frame with known checksum; intentionally corrupt packet	Verify server detects corruption via CRC mismatch	100% error detection rate	After receiving a transmission, the Rebel Server shall perform error checking.
80	Inject transmission error and verify NACK sent	Monitor RF channel for NACK packet and verify contents	NACK transmitted correctly with frame ID	In the case of an error, the Rebel Server shall send a transmission to the Raspberry Pi requesting to resend the data.

ZL

Test Plan - Requirements

Req No.	Test Method	Evaluation Method	Threshold	Objective
90	Simulate NACK reception at Raspberry Pi	Verify Pi retransmits the requested frame	Correct frame retransmitted	If the Raspberry Pi receives a request to resend a transmission, then it will send the image again.
100	Time complete transmission cycle with stopwatch	Record elapsed time from start to completion	≤ 600 seconds total transmission time	It shall transmit in 600 seconds or less.
110	Access public video URL without authentication	Verify video loads and plays from multiple devices	Video accessible without login	Any user shall have access to the first video.
120	Attempt to access authenticated video without credentials	Verify access denied; then authenticate and verify access granted	Unauthorized users blocked; authorized users granted access	Authorized users shall have exclusive access to the second video.

ZL

Test Plan - Requirements

Req No.	Test Method	Evaluation Method	Threshold	Objective
130	Implement FIDO2 two-factor authentication	Test authentication flow with security key and verify non-password based access	FIDO2 authentication successful without password	The mobile app shall use a secure method of authentication to identify authorized users.
140	Load mobile application on mobile device	Verify images displayed in scrollable format	Images displayed in scrollable table	The mobile app shall display images in a scrollable table.
150	Count number of images displayed in gallery	Manual count and comparison to expected value	Exactly 10 images displayed	The mobile app shall display up to 10 images.
160	Verify each red circle content appears once	Manual inspection to confirm no duplicates	Each red circle image appears exactly once	The scrollable table shall display the contents of each red circle exactly once.

ZL

Test Plan - Constraints

Req No.	Test Method	Evaluation Method	Threshold	Objective
10	The budget spreadsheet will be analyzed to ensure the total cost is $300 or less.	Manual inspection of budget	Total cost no more than $300	The total cost of the project shall not exceed $300 without Faculty Advisor approval.
20	Ensure only appropriate equipment is used.	Documenting of all equipment used	Only provided equipment or components purchased within the budget are used	The solution shall use only the provided equipment plus additional components purchased within the budget; a personal mobile application host device is required.
30	Place the Raspberry Pi and all equipment connected to it into the box.	Visual inspection of equipment	All equipment fits within the box	The Raspberry Pi and all equipment connected to it must fit within the provided box.

ZL

Test Plan - Constraints

Req No.	Test Method	Evaluation Method	Threshold	Objective
40	Confirm that all Wi-Fi, Bluetooth, and cellular functionalities are disabled, and no wires directly connect the Raspberry Pi to the Rebel Server.	Visual inspection of computer settings	No Wi-Fi, Bluetooth, cellular communication, or wired connections are used.	The Raspberry Pi and Rebel server shall not communicate with each other using Wi-Fi, Bluetooth, cellular communication, or a wired connection.
50	Use a tape measure or other measuring device to determine the distance.	Visual inspection of distance	The Rebel Server is at least 5 meters from the Raspberry Pi.	The Rebel Server and all its components shall be placed at least 5 meters from the Raspberry Pi.
60	Use the transceivers to receive and send test data, and mark the signals that were used during transportation.	Documentation of the signals that were sent and received.	Following the standards set by the FCC, without breaking the said set standards.	The range of frequencies used shall be compliant with FCC regulations.

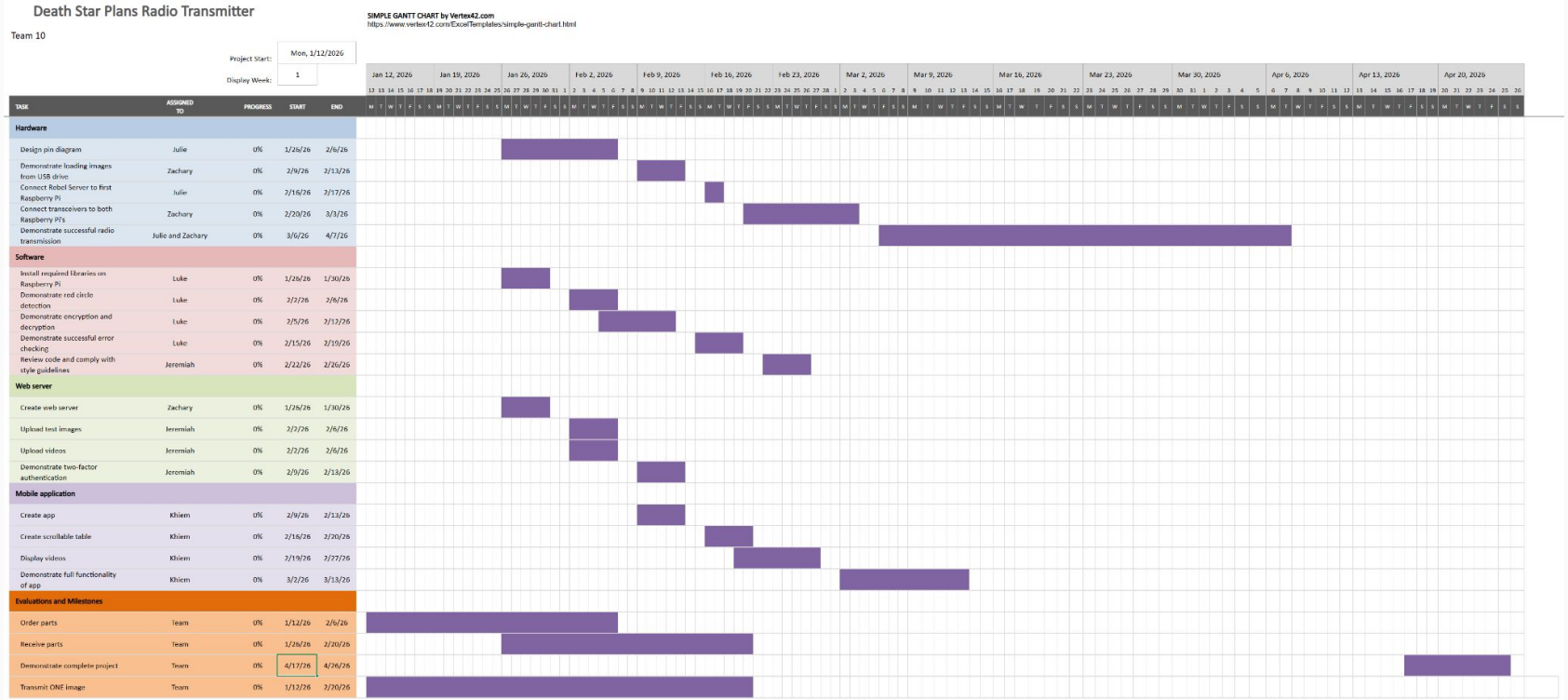
ZL

Test Plan - Standards

Req No.	Test Method	Evaluation Method	Threshold	Objective
10	Encrypt and decrypt data using OpenSSL's AES encryption.	Inspection of encrypted and decrypted data	Ciphertext differs from plaintext, and data can be accurately decrypted	The solution shall comply with AES FIPS 197-upd1 for encryption.
20	Use the transceivers to receive and send test data, and mark the signals that were used during transportation.	Documentation of the signals that were sent and received.	Following the standards set by the FCC, without breaking the said set standards.	The solution shall comply with C95.3-2021: Standard for Radio Frequencies
30	Ensure that mobile application follows all appropriate guidelines	Visual inspection of application	The application functions correctly and can display images and videos	The mobile application shall comply with the IEEE/ISO/IEC 23026-2023 standard for website design.
40	Inspect code and ensure it complies with all style guidelines	Review code and verify compliance	All written Python code complies with PEP 8.	All Python code shall comply with PEP 8 for coding style.

JMH

Timeline



JMH

Milestones and Deliverables

- Design pin diagram
- Demonstrate loading images from USB drive
- Connect Rebel Server to first Raspberry Pi
- Connect transceivers to both Raspberry Pi's
- Transmit one image
- Demonstrate successful radio transmission
- Install required libraries on Raspberry Pi
- Demonstrate red circle detection
- Demonstrate encryption and decryption
- Demonstrate successful error checking
- Review code and comply with style guidelines
- Create web server
- Upload test images
- Upload videos
- Demonstrate two-factor authentication
- Create app
- Create scrollable table
- Display videos
- Demonstrate full functionality of app
- Order parts
- Receive parts
- Demonstrate complete project

Contact Info/Questions?

Zachary Leyes: leyes.4@wright.edu

Luke Kremer: kremer.76@wright.edu

Jeremiah Hackman: hackman.10@wright.edu

Julie Peterson-Ramos: peterson-ramos.2@wright.edu

Khiem Do: do.21@wright.edu