Duck Defenders

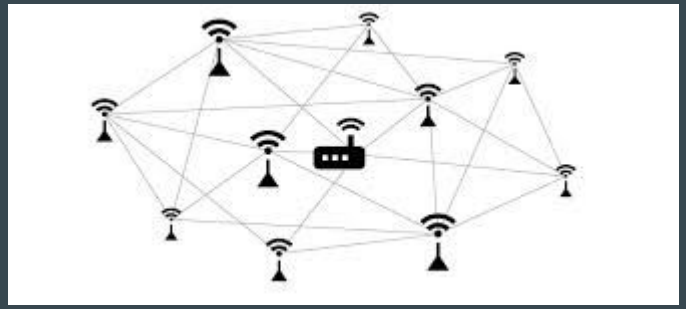
Team: Sam McKee, Sajan Johal, Jaime Rizo,
Cole Morrison, Tyler Herzog

Who is Project OWL?

- Develops devices that form a deployable mesh network.
- Devices called DuckLinks due to land, air, and sea capabilities, and can carry sensors for collecting data about their surroundings.
- These networks are designed to aid in communication.

Capstone summary

- We will develop a method of security analysis for mesh networks.
- The method will use a database of different attacks to use on the network.
- Based on the real world frequency and severity of each attack, and the metrics measured, the system will give an analysis for the security of the network.



Customers/clients

- Our client is Project OWL.
- Their original mission was to create a mesh network that could be used to aid communication between survivors of Hurricane Maria and first responders.
- Project OWL's products have expanded into fields such as military use and event set up.
- Our security analysis will give Project OWL's developers insight into security risks of the DuckLinks, which helps them make it a more secure product for their customers and users.

Stakeholders

- Communities affected by natural disasters and first responders
- The US Department of Defense and the people who may use DuckLinks in their field work
- Large public event planners (events such as large concerts and festivals)
- Energy and manufacturing companies

Project goals

- Curate a list of common mesh network attacks and a rubric to judge a network's security by.
- Conduct a security analysis on Project Owl's DuckLink network.

Project objectives

- Research security attack vectors commonly seen in mesh networks such as the DuckLink network.
- Develop a system of KPIs (Key Performance Indicators) that measure a system's security.
- Document needed security improvements in the DuckLink network for future development.
- Present security report to Project Owl and have them decide which attack vectors to patch.

Marketing requirements

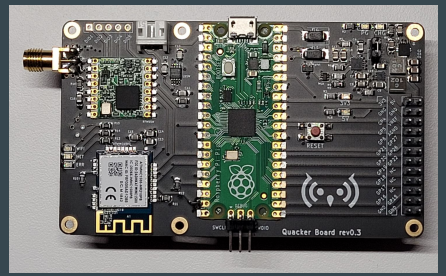
- Complying with DOD standards for encryption and security
  - AES 256
- Encryption is modular and can be rolled back to a lower standard for various clients
- Insight into potential attack vectors and mitigation tactics
  - Develop tools to mitigate harm from bad actors
  - Reporting any flaws in the network or source code
- Improving security without hurting performance
  - Encryption is fast and efficient
  - Any additional module draw minimal power
  - Self-Diagnostic tools are made to be lightweight

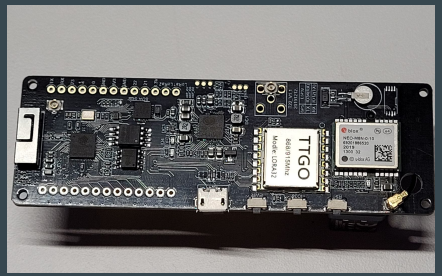
Engineering requirements

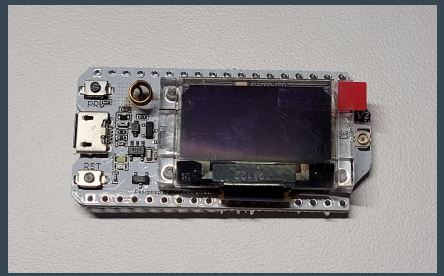
Spec. Number	Parameter	Target	Tolerance	Risk	Compliance
1	Encrypted messaging	AES-256, DoD standard	Max.	High	A, T, I
2	Power Usage	Low Power Modules and optimized lightweight code	Max.	High	A, I
3	Identification of many types of attacks (i.e. DOS, side-channel, external code injection)	Most to least common types	Min.	High	T, I
4	Malicious user identification	Mean time to detect	Min.	Medium	T, I
5	Recoverability from attacks	Time to remotely reset	Min.	Medium	T, I

Constraints

- Any additional hardware should be sourced from US or NATO based suppliers
- Opensource
- Ensuring that every library is up to date
- Flexible code that can be ported to any current CDP hardware (QuackerBoard, T-Beam, Heltec)







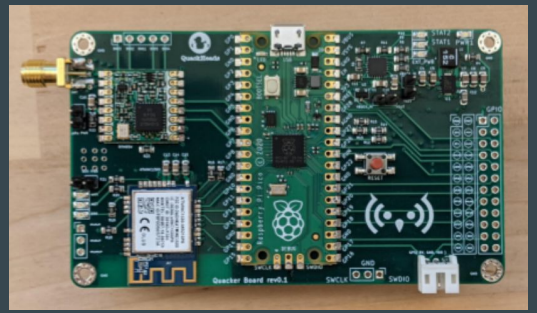
Criteria

- Access Gained
- Information Gained
- Frequency
- Time to Attack
- Complexity

Related work

- Project OWL is not the only current mesh network
  - Meshtastic, Disaster Radio, etc.
  - Project OWL is more sensor focused
  - Helpful in comparing security approaches

- Previous Capstone projects
  - QuackHeads - Hardware redesign
  - R.A.F.T - Hardware design



Project outcomes and deliverables

- Research common and possible attacks
  - Condense research into deliverable paper with possible attacks
  - Evaluate attacks based on severity and frequency

- Create threat assessment report
  - Document all findings in a report with information about attacks
  - Include specific information about attacks (ex. Does the attack disclose any confidential info?)

- Present Duck Link vulnerabilities
  - Deliver report to Project OWL with findings and attacks listed

Concept generation and evaluations

- Three main ideas (along with many others)
  - Security
  - Porting source code from Arduino
  - Shrinking last years board into more compact package
  - Additional ideas include sending Ducks into orbit and making Ducks monkey proof

- The importance of security with a mesh-network
  - Project OWL emphasized this across our meetings
  - As a group we wanted to do something beneficial to the project long-term
- Final decision was a combination of motivators
  - Importance to the project
  - How our skill sets applied (and what we wanted to learn)
  - What seemed most interesting

Design description

- Research common mesh-network threat vectors
  - Include both hardware and software security issues
  - Put together analysis of most common flaws
  - Add helpful data such as risk and frequency

- Deliver threat assessment of Project OWL's current infrastructure
  - Include criteria to judge threat vectors
  - Examples include risk, frequency, ease of attack, etc.

Attack	Risk	Frequency	Ease of Attack
DOS	Medium	High	Very Easy
etc...			

Mission and objective

Mission:

- Effectively communicate with each other.
- Be transparent.
- Stay organized & have proper documentation.

Objective:

- Learn how to effectively conduct a security threat analysis.
- Become more familiar with mesh-network technology and how to keep it secure from intruders.

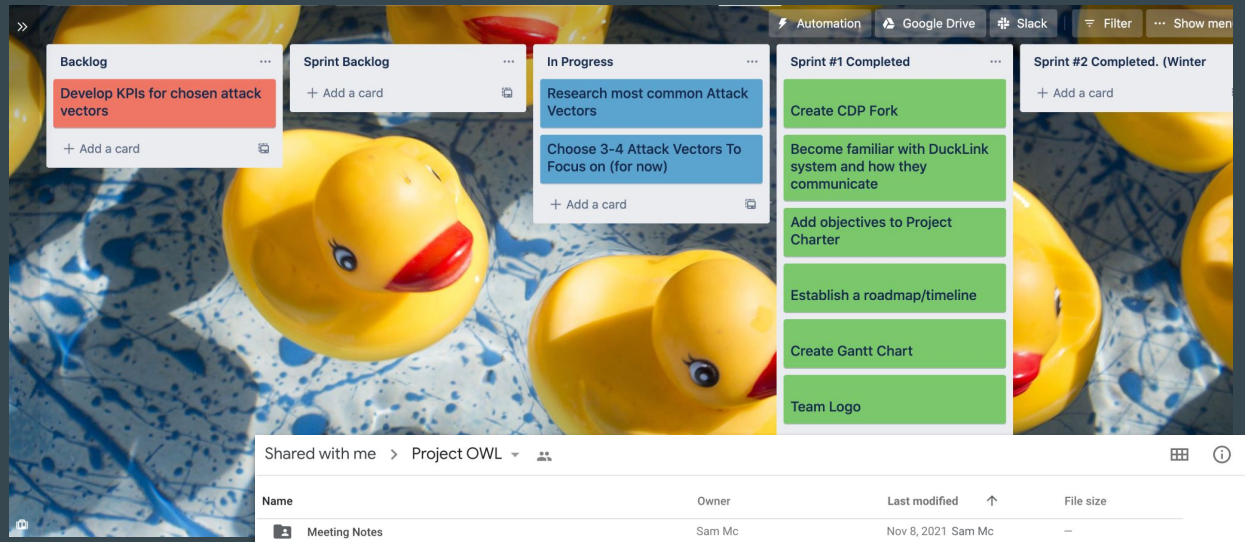
Members & Roles

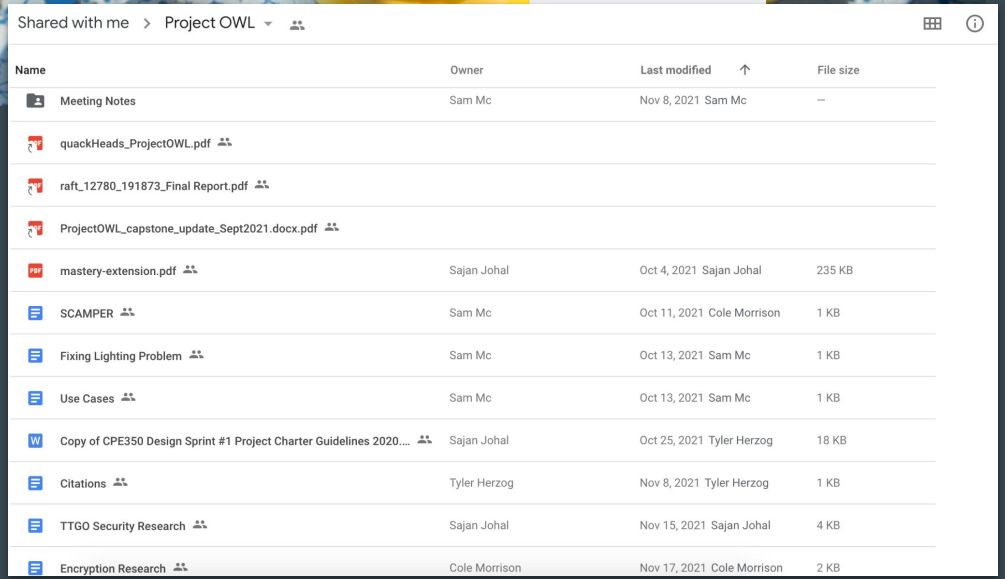
- **Tyler Herzog**
  - Hardware Reliability
- **Sajan Johal**
  - Hardware Security
- **Cole Morrison**
  - Software Encryption
- **Jaime Rizo**
  - Software Security Risks/User Impact
- **Sam McKee**
  - Software Security Risk Mitigation

Planning Information

Collaboration

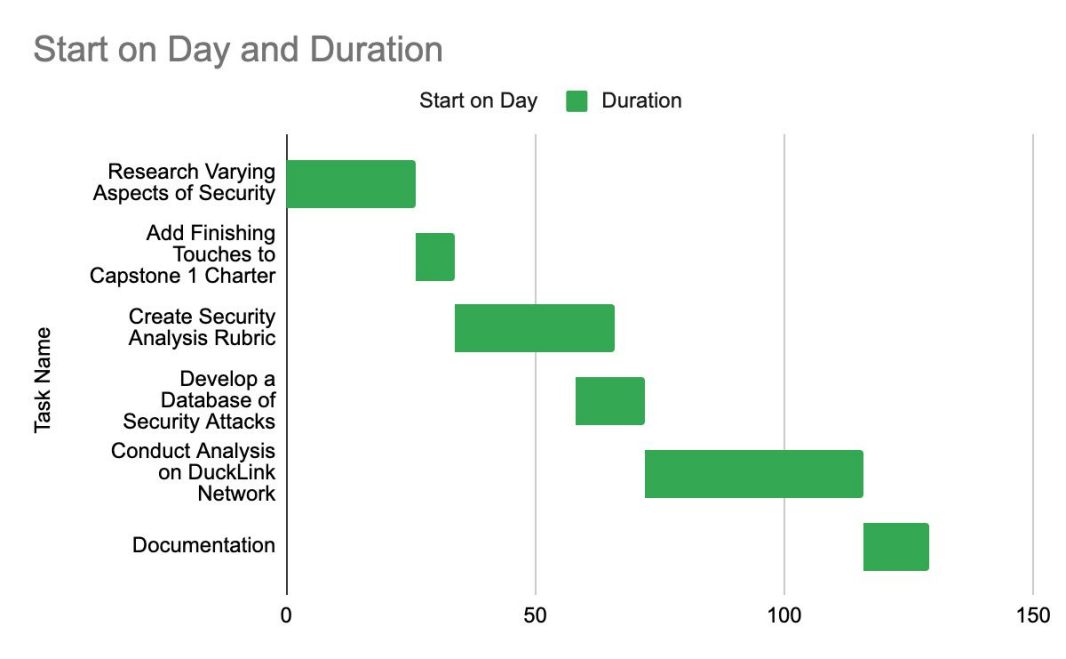
- Slack
- Zoom
- Trello
- Google Docs/Spreadsheets
- Group Text





Planning Information

Gantt Chart



DEMO

QUESTIONS