Portcullis

Christopher Son, Aiden Seay, Preston Smith, and Ryan Todd

Faculty Mentor: Bailey Hall

Sponsored by: General Dynamics Mission Systems

NAU NORTHERN ARIZONA UNIVERSITY

Big Picture

Background

- Coast Guard critical infrastructure must remain secure and accessible
- Field personnel need **reliable** and **secure access** to sites
- Current systems are vulnerable to:
  - Break-ins & theft of equipment
  - Harsh weather conditions & connection issues

Our Project

- Build a new solution for remote site access with a **secure** and **resilient** door control system

Client Introduction

General Dynamics Mission Systems

- Deliver mission-critical systems and secure products for defense, intelligence, and cybersecurity customers
- Department of Defense contractor

Client Representatives

- **Benjamin Walker** - GD ~13 years, oversees the door systems
- **Alexander Gebhart** - GD ~1.5 years, mechanical engineer

GD Mission Systems

Business Process

General Dynamics Mission Systems Customer

- Coast Guard Rescue 21 (search & rescue command & control)
  - Direction-finding communications system

Current Workflow

- Personnel arrive onsite to fix issues
- Use RFID cards to enter the facility
- System monitors entry/exit

Problems

Current System Issues

- Updates to the system are difficult (network pushes are unreliable)
- High latency due to weather interference
- Security gaps (potential physical break-ins)
- Not reliable during power outages

Our task: find an innovative solution to solve these problems

Our Solution

Goal

- Develop robust software & hardware system for door access & monitoring

Core Functions

- Secure login & electronic lock control software
- Automated entry/exit logging
- Intrusion detection integration (motion sensors)
- Resilient communication (encrypted and reliable)
- Backup power support (battery powered)

Plan for Development

Design Requirements

- 16 Coast Guard requirements
- Develop two designs
- Trade study
    - Determine winning design

Technical Investigation

- Hardware interface (locks, sensors, monitors)
- Network resilience under poor conditions
- TLS encryption & secure communications
- Power backup strategies
- Lock types

Closing

Summary

- **Goal:** Developing a **secure**, **resilient**, remote door controller system fo GDMS
- **Challenge:** Accessibility, security, and reliability issues
- **Solution:** Prototype integrating secure access, intrusion monitoring, and reliable comms

Expected Benefits

- Faster, safer access for field engineers
- Stronger protection against intrusions and equipment theft

Broader Applications

- Scalable to other critical infrastructure (utilities and telephones)
- Adaptable for modern IoT access control systems

Thank you

NAU NORTHERN ARIZONA UNIVERSITY