# EE/CprE/SE 491 – sdmay26-08

# GridSAFE

# Week 6 Report

Start date - End date: 10/28/25 – 11/4/25
Client: Nellie Leaverton
Advisor: Julie Rursch

## Team Members:

Nellie Leaverton – Hardware & Architectural Design Lead
Jason Di Giovanni – Software and Security Lead
Brant Gicante – Software and Security Assistant
Evan Booze – Hardware & Architectural Design Assistant
Kyle Maloney – Testing Lead & Design Assistant
Anthony Nehring – Software and Security Assistant

**Weekly Summary:**

This week, the GridSAFE team printed their first prototype, and started the iterative process of printing different prototypes to fit their needs and project requirements. The hardware team advanced 3D design modeling by creating new buildings and preparing other 3D models for more prints. Additionally, the software team advanced development on multiple components, including a Python-based LED control system for visualizing node status changes, an AI output checker to validate model classifications against system logs, planned network configuration outlining vulnerable nodes and targeted attack scenarios, and finalizing host syntenic logs.

**Past week accomplishments:**

3D Modeling and Printing – Nellie Leaverton

- Printed first 3D prototype of Coin Building at SIC
    - Picked up 3D print
    - Broke off print supports
    - Marked print with new edits
- Printed second 3D prototype of Coin Building
    - Set up print at SIC
    - Picked up print from SIC
    - Broke off print supports
    - Verified print was visually appealing and met our requirements (visually, functionality, base board, dimensions)
- Started editing other 3D skyscraper models
    - Started cutting out holes in 3D models

Host log and MITRE Mapping – Anthony

- Created 22-field host log schema
- Generated synthetic events covering every MITRE ATTACK tactic (host relevant)
- Added process, pid/ppid, cmdline, file_path/action, network_dst/port, registry, service, auth, anomaly_score, label
- Simulated attack chain examples
    - Initial access -> execution -> persistence -> escalation -> lateral movement -> exfiltration -> impact
- Created full examples for also normal and anomalous

LED Controller - Kyle

- Started designing and implementing a Python library to control the state of the LEDs we display in our city
    - Displays time-based animations to show the transition of a powered node to an unpowered and under-attack node.
    - Receives a signal and updates to display either green or red or transition from one to the other to indicate its status.

AI Output Checker Prototype – Jason

- Completed initial implementation of the AI Output Checker script
    - Extracts AI classification results (e.g., normal, anomalous, malicious) from model output
    - Reads corresponding labeled entries from the system log file for comparison
    - Compares AI classifications to original labels to detect misclassifications
    - If classification is incorrect, transmits JSON data to the RPI for light change
        - Verified functionality using multiple test cases containing intentional misclassifications and incomplete outputs

Network Setup Practice – Brant Gicante

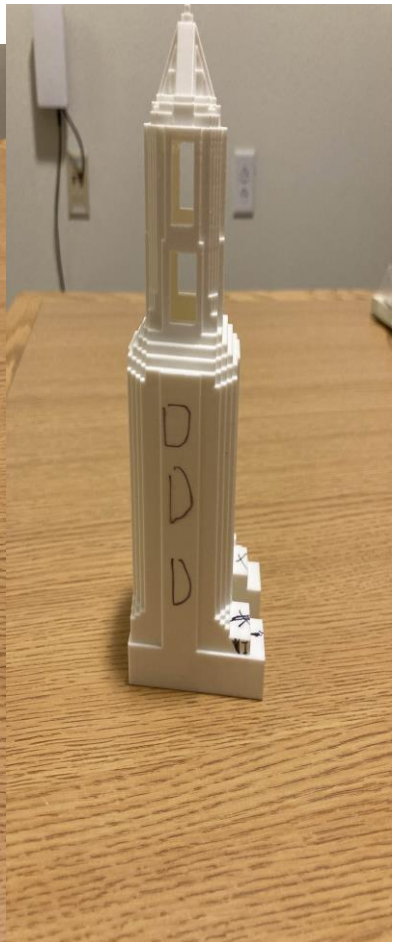
- Investigated and decided on a network map to draw up for setup of mail servers.
    - Specified configurations for network.
    - "vulnerable" and specific attacks which we will target.
        - Older version control
        - Open ports
        - Phishing example

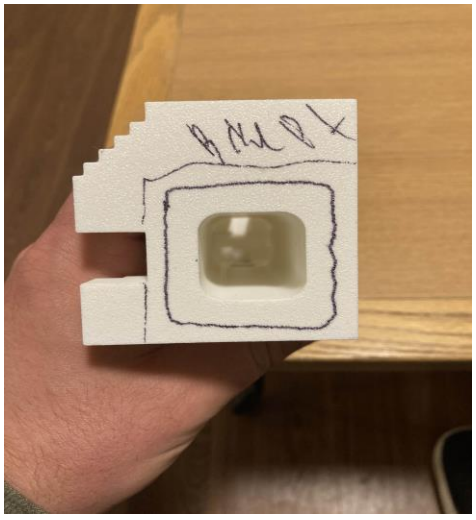
Structure Printing and Modification - Evan Booze

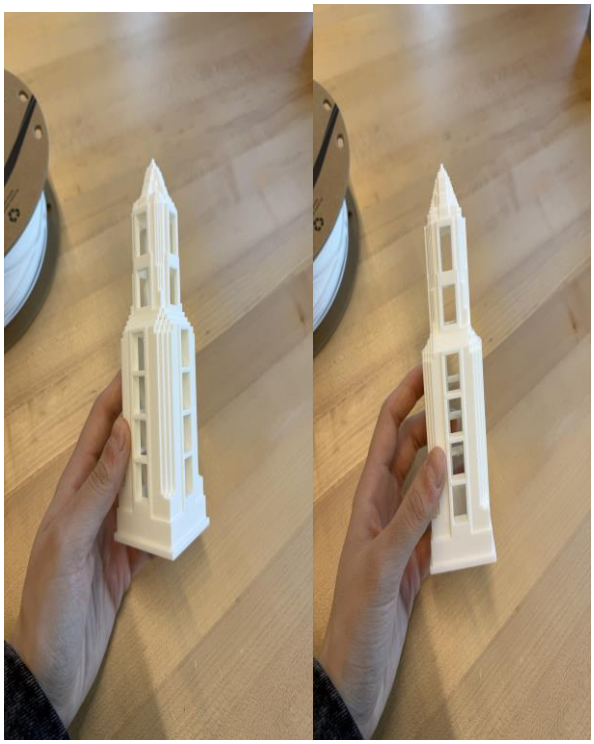
- Completed print of initial prototype structure
- Made modifications to initial protype structure in Autodesk Fusion
    - Added a 0.5-inch base plate
    - Added additional windows to the structure
    - Widened interior of the structure to facilitate LED installation
    - Removed extraneous bits around the base of the structure to reduce base thickness

**Citations/Research:**

Log examples for malware, DNS, and OT devices:
https://www.unb.ca/cic/datasets/index.html







**Pending issues:**

**Individual contributions:**

| NAME | Individual Contributions | Hours this week | HOURS cumulative |
|---|---|---|---|
| Nellie Leaverton | • Created Meeting Notes for weekly meeting<br>• Printed first and second 3D prototype at SIC<br>• Started making modeling edits (extrusions, adding windows, adding base plate) to new 3D skyscraper models. | 6 | 38 |
| Brant Gicante | • Network Design drawing<br>• Network vulnerability configuration<br>• Learned about our current AI model | 4 | 27 |
| Evan Booze | • Printed initial prototype structure for testing<br>• Made modifications to prototype structure in Autodesk Fusion | 6 | 21 |
| Jason Di Giovanni | • AI Output Checker<br>• Research for OT and other log datasets | 4 | 27 |
| Kyle Maloney | • Continued prototyping Proxmox server<br>• Researched MITRE attacks and XGBoost to prepare for training with our generated logs<br>• Continue designing the LED library to use in our city structure | 6 | 20 |
| Anthony Nehring | • Created host log schema<br>• Created full coverage logs for normal, anomalous, and malicious host logs<br>• Developed host log attack chains | 6 | 24 |

**Plans for the upcoming week:**

- **Brant Gicante:**
  - Put the network map into a real setting/environment
  - Make a communication between our AI and a raspberry pi, or at least configure what it will look like when available
  - Attempt making a checker for the AI and raspberry pi to compare to (assuming supplies have arrived) otherwise investigate a simulation or environment to make it realistic.
- **Evan Booze:**
  - Continue making edits to other structures with Nellie to be ready for splicing and printing.
  - Help Nellie make modifications to LED wires, so the LEDs are ready to be installed for testing.
  - Secure materials for the model city base plate.
  - Print more structures at SIC.
- **Nellie Leaverton:**
  - Continue to print more 3D models, different types of skyscrapers
  - Work on setting up a simple circuit to test lighting (LEDS) we bought.
  - If lighting works and looks visually appealing in prototype, start setting up the lights with the raspberry pi.
- **Kyle Maloney:**
  - Meet with the software team to discuss MITRE attacks to analyze and create logs.
  - Finish designing the LED library we will use for our physical city
  - Continue setting up Proxmox server if we receive the resources we need
- **Jason Di Giovanni:**
  - Discuss use case for datasets regarding attacks and OT devices with software team
  - Set training environment up and begin training AI
- **Anthony Nehring:**
  - Get input on the host logs made, and with this feedback use this to help finalize the network and host synthetic logs.
  - Furthermore, discussing the current state of synthetic logs in general to thus make sure the network and host logs are up to standard on what we want from the two.