DETECTING SPOOFING ATTACK IN CYBER-PHYSICAL SYSTEMS

Team Members

- Samuel Gross
- Michaela Walker
- Ashley Vanaman
- Logan Parker
- Leah Casey

Client Information

- Pierce Aerospace

  CEO - Aaron

  CTO - Gary

  Back-End Coder – Chris - He’s our primary point of contact in the project

Business Requirements

- <u>Business Requirement 1</u>

  Develop a data curation framework for forensic users that can identify potential spoofing attacks within certain cyber-physical systems.

- <u>Business Requirement 2</u>

  Display ‘clean’ drone information to end-users

Use Cases

- Use Case 1 – Connected to business requirement 1
- Actors: Government officials, law enforcement, government agencies, clients, and the public
- Flow:

-User access the framework through an app.

-User inputs or uploads drone flight information into the system.

-System processes the data and identifies information from the flight data.

-Application analyses for potential spoofing

-Application validates the data.

-If spoofing is found, data is returned as bad, and a report is made. If no spoofing is present, data is returned as good.

-User can view results and identify potential security threads.

Use Cases

- Use Case 2 – Connected to business requirement 2
- Actors: Government officials, law enforcement, government agencies, clients, and the public
- Flow:

  -User access the framework through an app.

  -Application shows real-time drone data for the area.

  -Application analyzes the drone data for possible spoofing and anomalies.

  -If 'clean', that is showed in displayed information.

  -If 'bad', that information is not shown on the user interface.

  -Users will be able to view 'clean' drone information which will ensure reliable data is present.

Requirements

- Functional Requirements

  FR1: The System shall use attribute data to detect for spoofing. BR1, HIGH

  FR2: The system shall differentiate between spoofers and drone anomalies. BR1, HIGH

  FR3: The system shall exclude drones with spoofed Remote ID from being displayed to end-users. BR2, MEDIUM

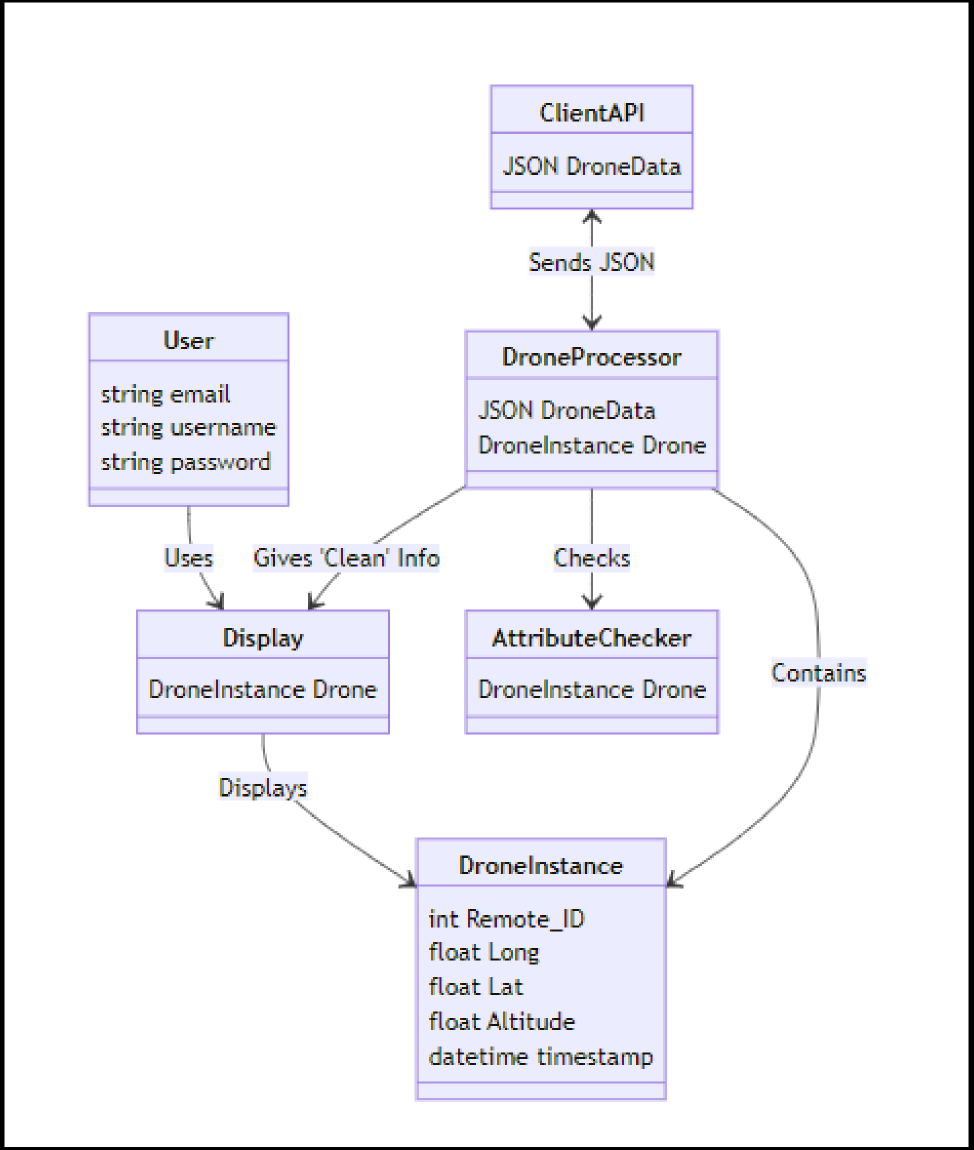
- Non-Functional Requirements

  NR1: Application prioritizes and enforces sign-in security measures and data protection. BR1, HIGH

  NR2: Displayed UAS information shall be accessible on a smart device. BR2, MEDIUM

  NR3: User interface allows for customization of the types of UAS data displayed. BR2, LOW

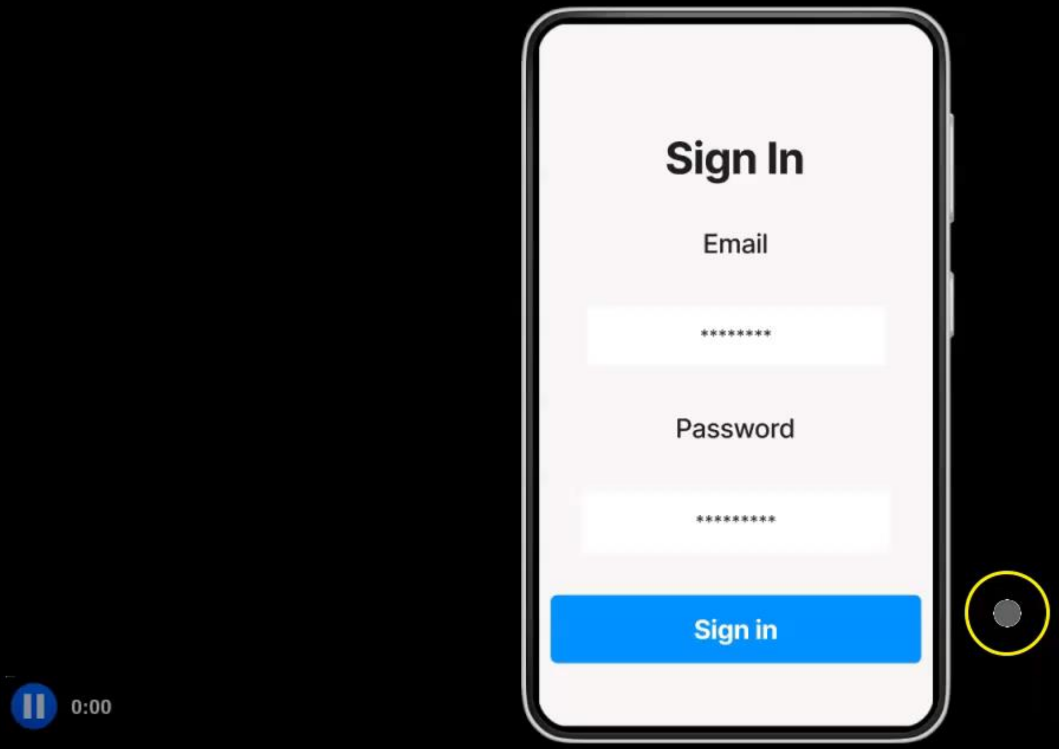
Domain Model



TechStack

- We are using Java and Unreal

Prototype



Sign In

Email

****

Password

****

First Iteration Features

- Text Based Output
- Import JSON Files
- Process JSON Files
- Put JSON file information back into the database
- Create User Sign in

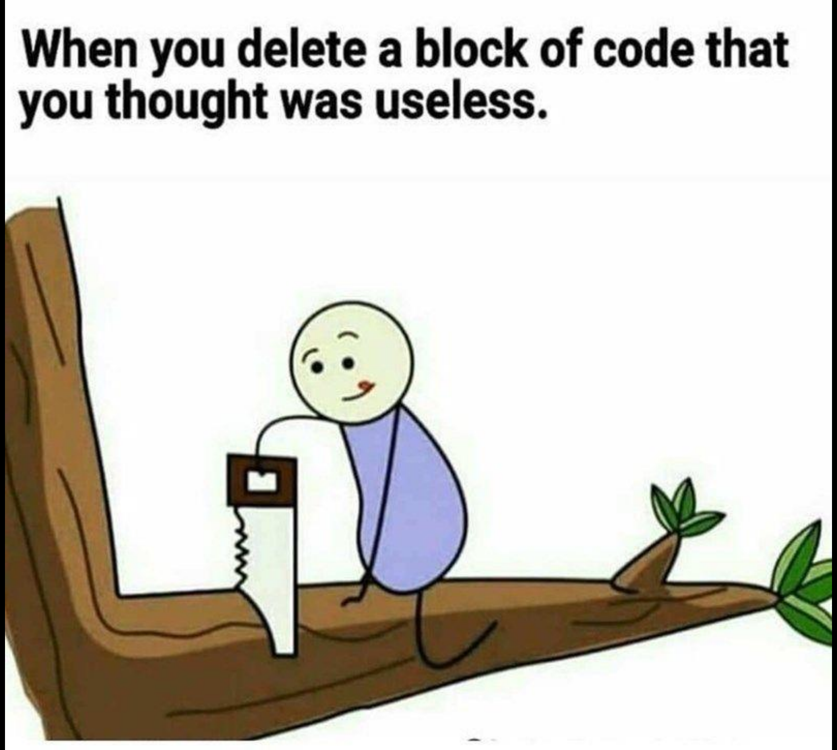
Mentor Feedback

- Everything looks good.
- Putting in work to ensure all requirements are met will help benefit us in the future which we have set ourselves up for.
- Expectations should be low for first iteration.
- Project looks good.
- Project is comprehensive, visualizing how software will be used is extremely beneficial and our project is.

Client Feedback

- Don’t mention company architecture.
- Business requirements are good.
- Use Cases are good.
- Focus on Attribute data for requirements, what we had was too specific for the first iteration.
- Wanted only real-time data on screen of prototype, did not want the drone information to have to be typed in.
- Simplified out first iteration requirements, with what we had there was a concern we were doing too much for the first iteration, too much detail.

Interesting Slide


When you delete a block of code that you thought was useless.