Final Project Phase 1

Group 5 - Adrion Thomas, Ian Scheetz

9/22/25

1. Project Overview

Our application will generate a secure log of the state of an art gallery. Users will be able to use queries to search for employees or guests, when they entered or left a room, and how long they spent in each room. The application will be made of two programs, logappend and logread. Logappend will securely write updates to the log, while logread will return information from the log to the user based on the queries they input. Both programs will use an authentication token to verify each other.

2. Functional Security Requirements

- Authentication: An authentication token will be required in both programs to authenticate each other.
- Authorization: Login credentials will be required to access the readlog program.
- Data Protection: The log file will only be able to be read via the logread program. Examining the log file directly will not provide any useful information. Also, while the logappend program is running, it will write to a temp file and create the secure log upon completion in order to protect the integrity of the log file.
- Input Validation: The user can input queries into the logread program. This input will need to be sanitized with an allowlist to make sure the user does not input malicious code.

- Logging and Monitoring: All queries that are input into the logread program will be documented in a separate userlog file. In the case that a malicious user gains access to the logread program, their queries will be logged and can be inspected later.

3. Security Goals
    - Assume Breach - If information about the guests or employees get compromised, it would be hard for the person breaching to get information and we could detect it easily.
    - Threat Modeling
    - Confidentiality - Contents of the logs cannot be released to unrelated parties.
    - Ensuring that the entries entered follow correct procedures -> A person cannot leave a room they didn’t enter, etc.
    - Integrity - Log entries can’t be edited once entered.
    - Availability - The information is only available to authorized users with the correct authorization tokens.