Water Gel blaster Cannon

**Security Specialist Team 4**

**“Introverts”**

About This Document

Document Information

|  |  |
| --- | --- |
| Issuing authority | Security Specialist Team 4 “Introverts” |
| **Status of document** | Done |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Comment | Author | Approver |
| 0.1 | 2024-06-16 | Initial Release | TEAM 4 |  |
| 0.2 | 2024-06-18 | Adding plan / role / DFD | TEAM 4 |  |
| 0.3 | 2024-06-20 | Adding Attack tree | TEAM 4 |  |
| 0.4 | 2024-06-21 | Adding SW Architect, Implemented list | TEAM 4 |  |
| 0.5 | 2024-06-23 | Adding Security Architecture | TEAM 4 |  |
| 1.0 | 2024-06-24 | Updating Implemented list | TEAM 4 |  |

Table of Contents

[1 Introduction 4](#_Toc170194269)

[1.1 Purpose 4](#_Toc170194270)

[1.2 Scope 4](#_Toc170194271)

[1.3 Audience 4](#_Toc170194272)

[1.4 Acronyms / Glossary 4](#_Toc170194273)

[1.5 Related Documents 4](#_Toc170194274)

[2 Team introduction 5](#_Toc170194275)

[2.1 4 Teams “Introverts” 5](#_Toc170194276)

[2.2 Development plan and milestones 5](#_Toc170194277)

[3 System Overview 6](#_Toc170194278)

[3.1 System Architecture (Native) 6](#_Toc170194279)

[4 Security Requirement 7](#_Toc170194280)

[4.1 Data Flow Diagram 7](#_Toc170194281)

[4.2 Attack Tree 7](#_Toc170194282)

[4.3 Requirement 8](#_Toc170194283)

[5 Security Architecture & Implementation 9](#_Toc170194284)

[5.1 Security Architecture 9](#_Toc170194285)

[5.2 Environment 10](#_Toc170194286)

[5.3 Features implemented based on Security requirement 10](#_Toc170194287)

Figures

[Figure 1 System Context Diagram for client 6](#_Toc170194668)

[Figure 2 System Context Diagram for server 6](#_Toc170194668)

[Figure 3 Data Flow Diagram 7](#_Toc170194668)

[Figure 4 Attack Tree 1 7](#_Toc170194668)

[Figure 5 Attack Tree 2 8](#_Toc170194668)

[Figure 6 Attack Tree 3 8](#_Toc170194668)

[Figure 7 Security Architecture 9](#_Toc170194668)

# Introduction

## Purpose

This document includes a team introduction (team formation and role) / development plans / strategies, as well as the SW architecture, DFD, requirements we have drawn.

And finally describe what we implemented according to the requirement

## Scope

* Schedule / Plan / Role
* DFD / SW Architecture
* Implemented list

## Audience

The target audience of this document is:

* Software architect and RED team who will evaluate the design of the software
* Component developer who will implement the design in actual code

## Acronyms / Glossary

|  |  |
| --- | --- |
| Acronym | Description |
| DFD | Data Flow Diagram |
|  |  |
|  |  |
|  |  |

## Related Documents

Documents related to this document include:

* 2024 LG Security Class Project Description.pdf

# Team introduction

## 4 Teams “Introverts”

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** |  |
| Jahoon Ku | Project Manager / Server developer |  |
| Jungsu Kim | Client Developer / Configuration Manager |  |
| Sungho Bae | Client Developer / Configuration Manager |  |
| Baekgeun Ji | Client Developer / Test Manager |  |
| Gayeon Kim | Server Developer / Test Manager |  |
| Jieon Kang | Server Developer / Test Manager |  |

## Development plan and milestones

From the investigation of the LgCannonDemo4 sources..

1. Eliciting requirement based on threat modeling of DFD (M/S STRIDE)

2. Implementation plaining with open sources (Server / Client)

3. Researching evaluation tool and application

4. Documentation of all artifact

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Title | 6/10 | 6/11 | 6/12 | 6/13 | 6/14 |
| Design /Document | Planning / Role | Investigate sources | Draw DFD | Draw DFD | Attack Tree |
| Develop Server | Impl. Server login | Impl. Server login | Impl. Server TLS | Impl. Server TLS | Impl. Server db |
| Develop Client | Impl. User login | Impl. User login | Impl. Client TLS | Impl. Client TLS | Impl. Client audit |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Title | 6/17 | 6/18 | 6/19 | 6/20 | 6/21 |
| Design /Document | Attack Tree | Elicit Requirement | Elicit Requirement | Implemented List | Implemented List |
| Develop Server | Impl. Server audit | Code review/fix | Impl. CAM on/off | Operation test | Operation test |
| Develop Client | Impl. Client audit | Code review/fix | Impl. CAM on/off | Operation test | Operation test |

|  |  |  |
| --- | --- | --- |
| Title | 6/24 | 6/25 |
| Design /Document | Finalize document | Presentation |
| Develop Server | Finalize server code |
| Develop Client | Finalize client code |

# System Overview

## System Architecture (Native)

Gel Water blaster Cannon consist of Client application and Server platform.

Each part is working like below

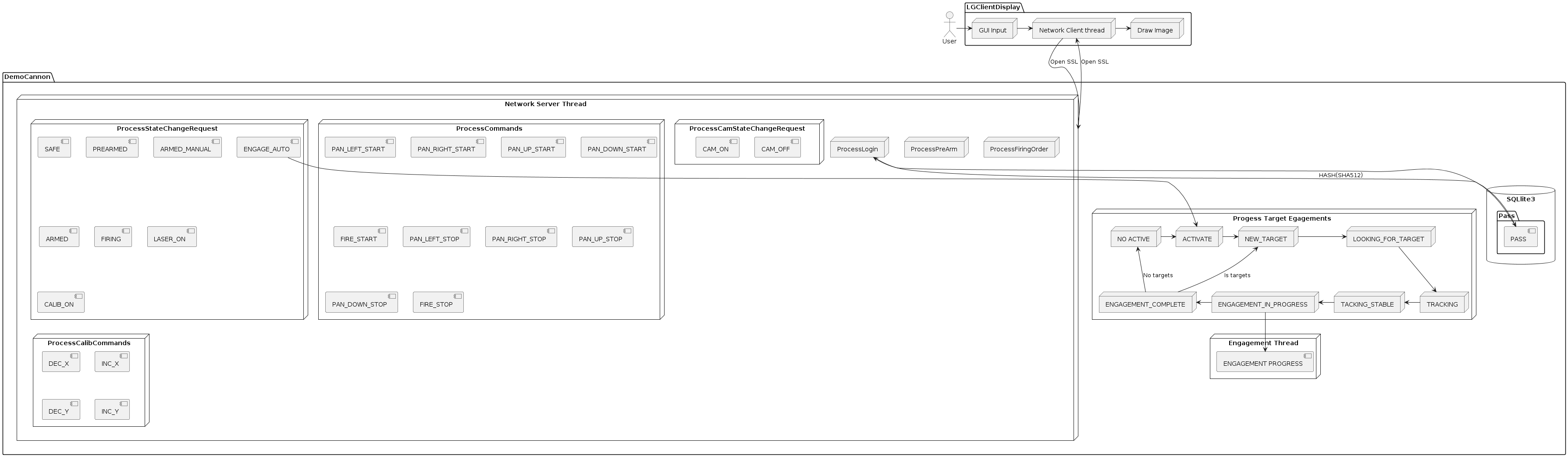


Figure 1 System Context Diagram for client

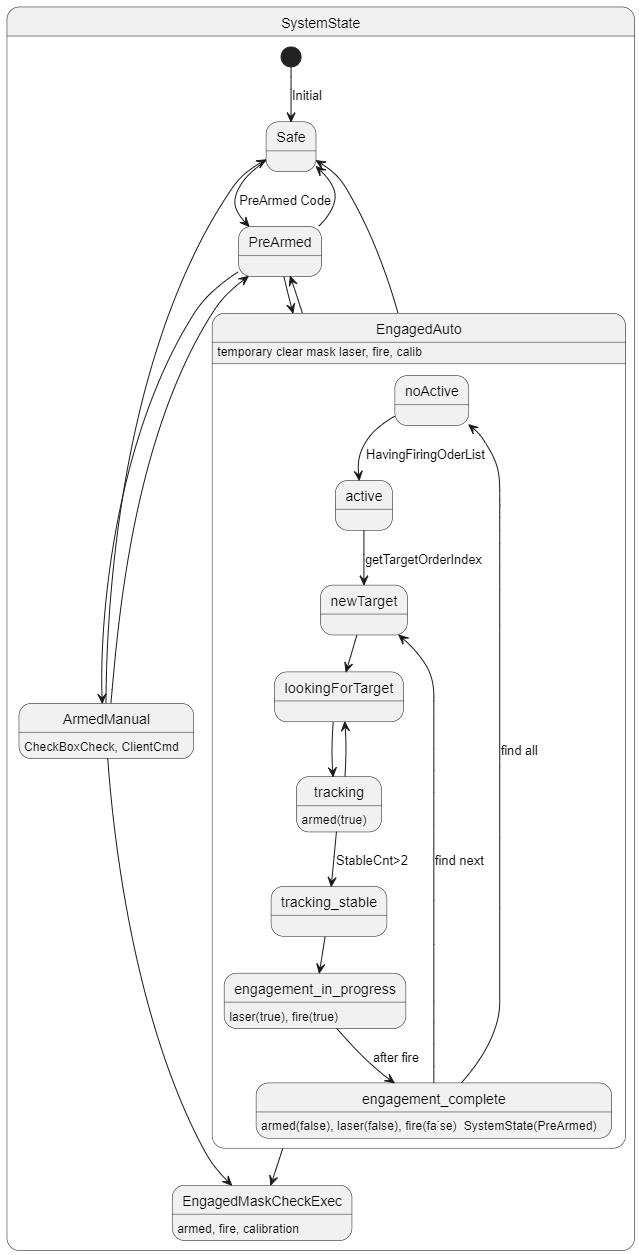


Figure 2 System Context Diagram for Server

# Security Requirement

## Data Flow Diagram

Given information, team draws a DFD and analyze threat / requirements

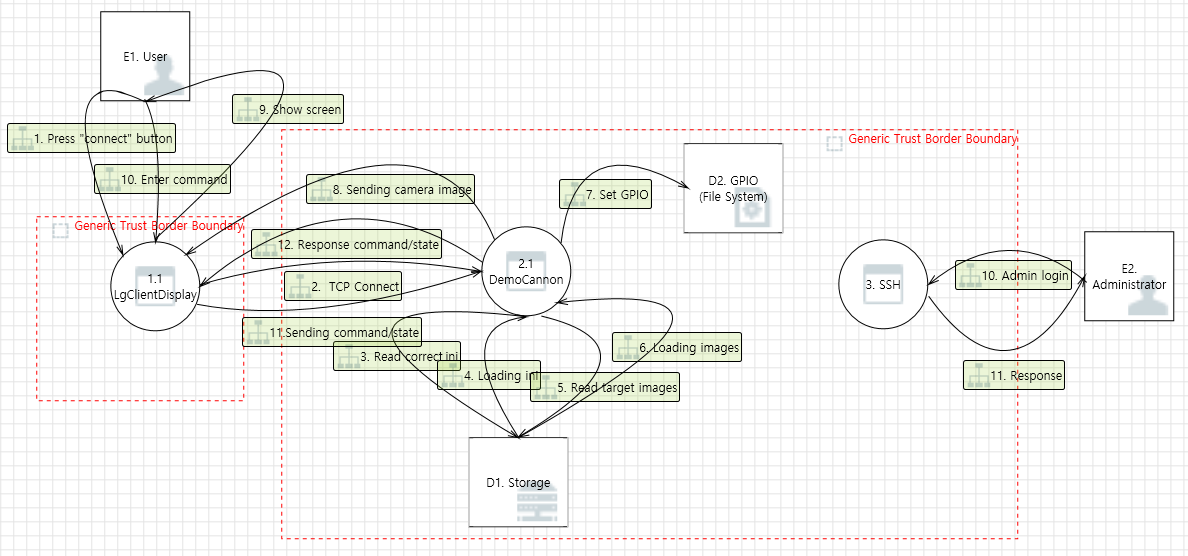
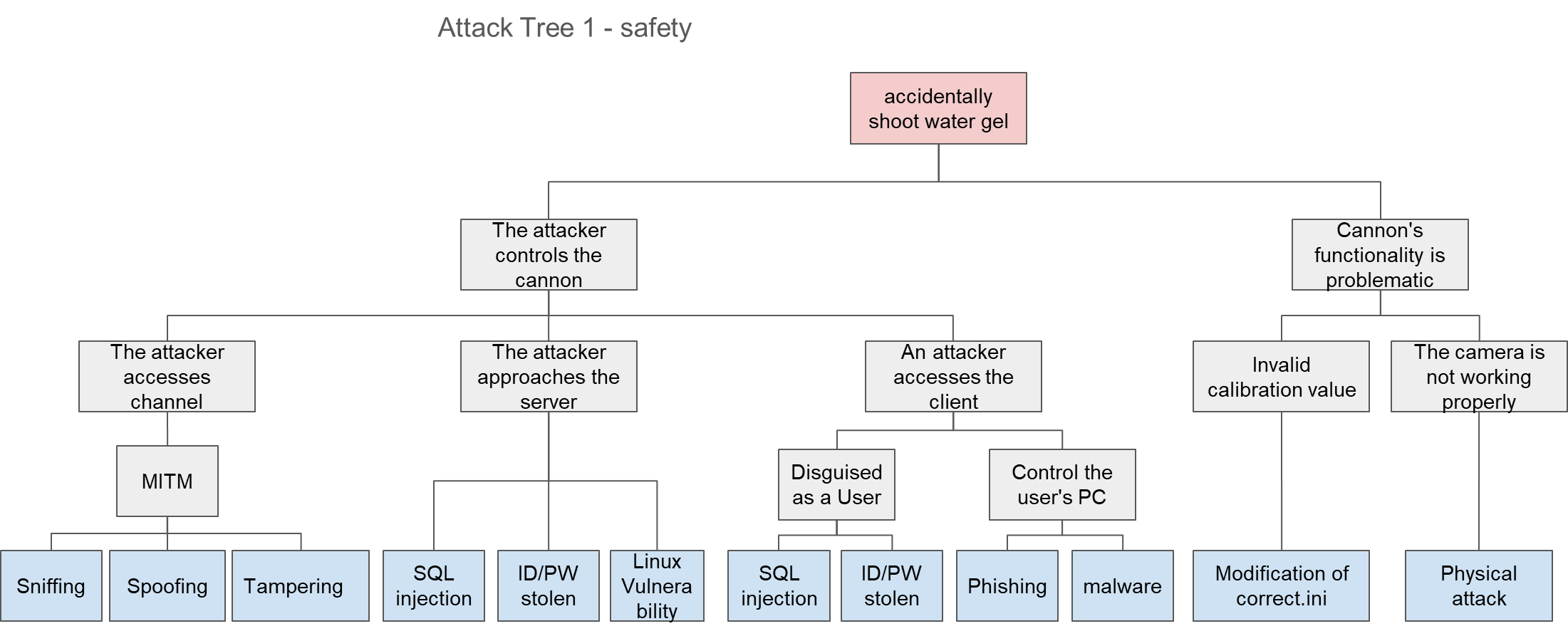


Figure 3 Data Flow Diagram

## Attack Tree

Attack tree was configured to analyze threats in a different way



Hardware

RFQ.12

Platform

Platform

RFQ21

RFQ.19

RFQ20

Platform

RFQ.19

RFQ.04

RFQ.18

RFQ.05

Figure 4 Attack Tree 1

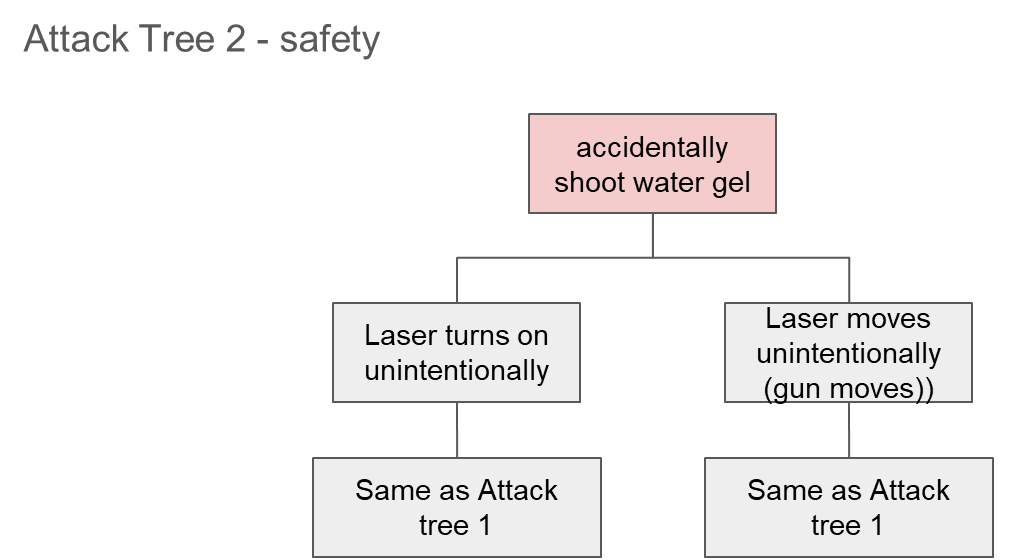
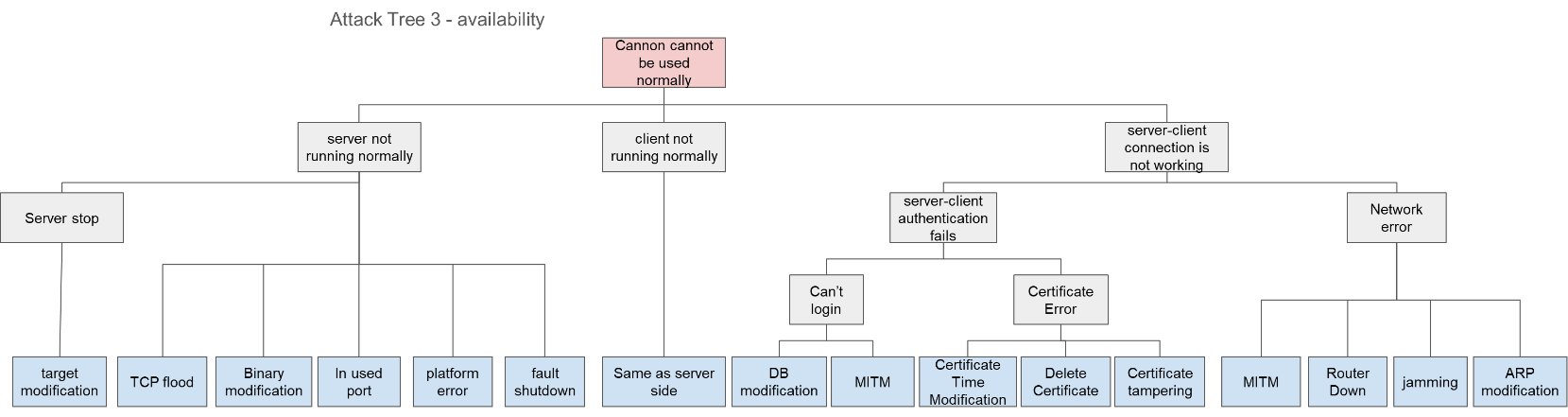


Figure 5 Attack Tree 2



Hardware

Hardware

Hardware

RFQ.18

Platform

Platform

Platform

RFQ.18

RFQ19

Duplicated

RFQ22

RFQ22

RFQ22

Platform

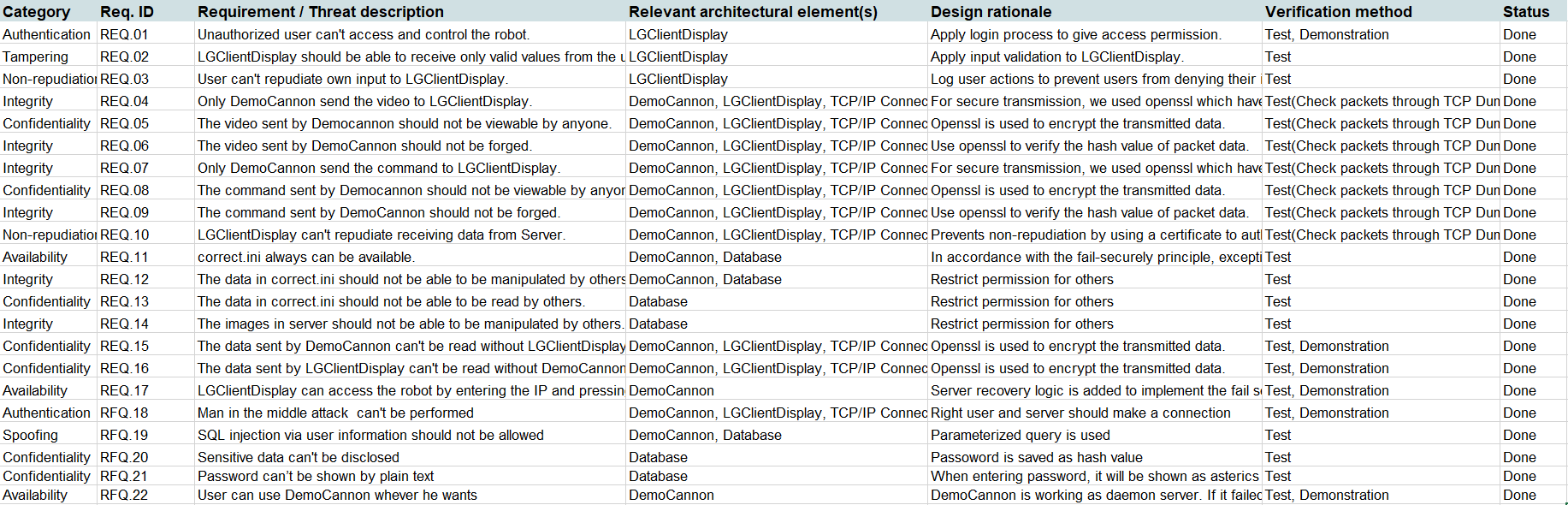
Platform

RFQ.22

Figure 6 Attack Tree 3

## Requirement

22 requirements derived through threat analysis were summarized





# Security Architecture & Implementation

## Security Architecture

1. Client

- TLS Wrapper for stable connection with OpenSSL

- Authenticating proper user and verifying password configuration

- Heartbeat control with Timer call back

- Generating log data for user input and server notification

2. Server

- TLS Wrapper for stable connection with OpenSSL

- Sending heatbeat

- User information control with SQLite

- Logging for server activity

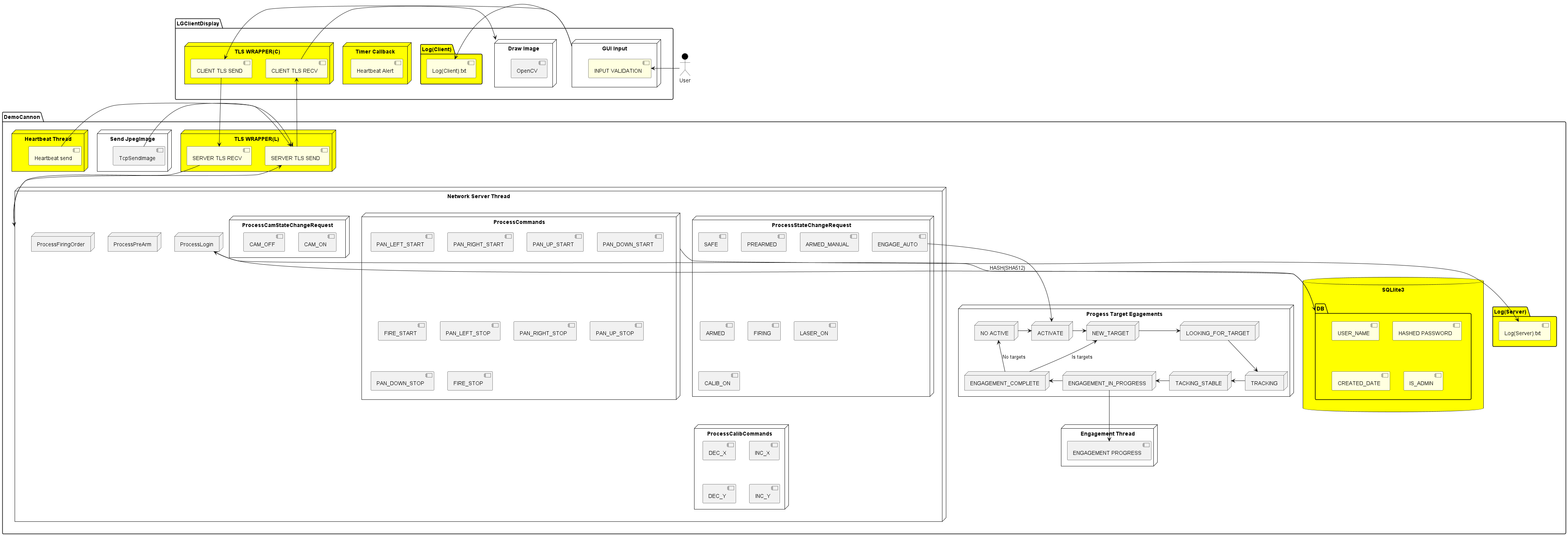


Figure 7 Security Architecture

## Environment

github : https://github.com/baverbae/LgCannonDemo4\_RELEASE

Libraries : OpenSSL 3.0.11 19 Sep 2023 (TLS )

Sqlite3 3.40.1 2022-12-28 14:03:47 ( Database )

logrotate 3.21.03.21.0 (Saving logs)

tools (staticanalysis / Fuzz)

cppchecker (<https://cppcheck.sourceforge.io/>)

snyx (<https://snyk.io/lp/snyk-code-checker/> )

zzuf (<https://github.com/samhocevar/zzuf> )

sonarqube (<https://docs.sonarsource.com/> )

## Features implemented based on Security requirement

1. User logging process

RFQ.01, 02, 19, 20, 21

- Fixed users can log in the remote client application with ID / Password

: ID / Password are stored in sqlite3 database

: sqlite3 database has 4 field ( ID / PW / last date of PW setting / Admin or not )

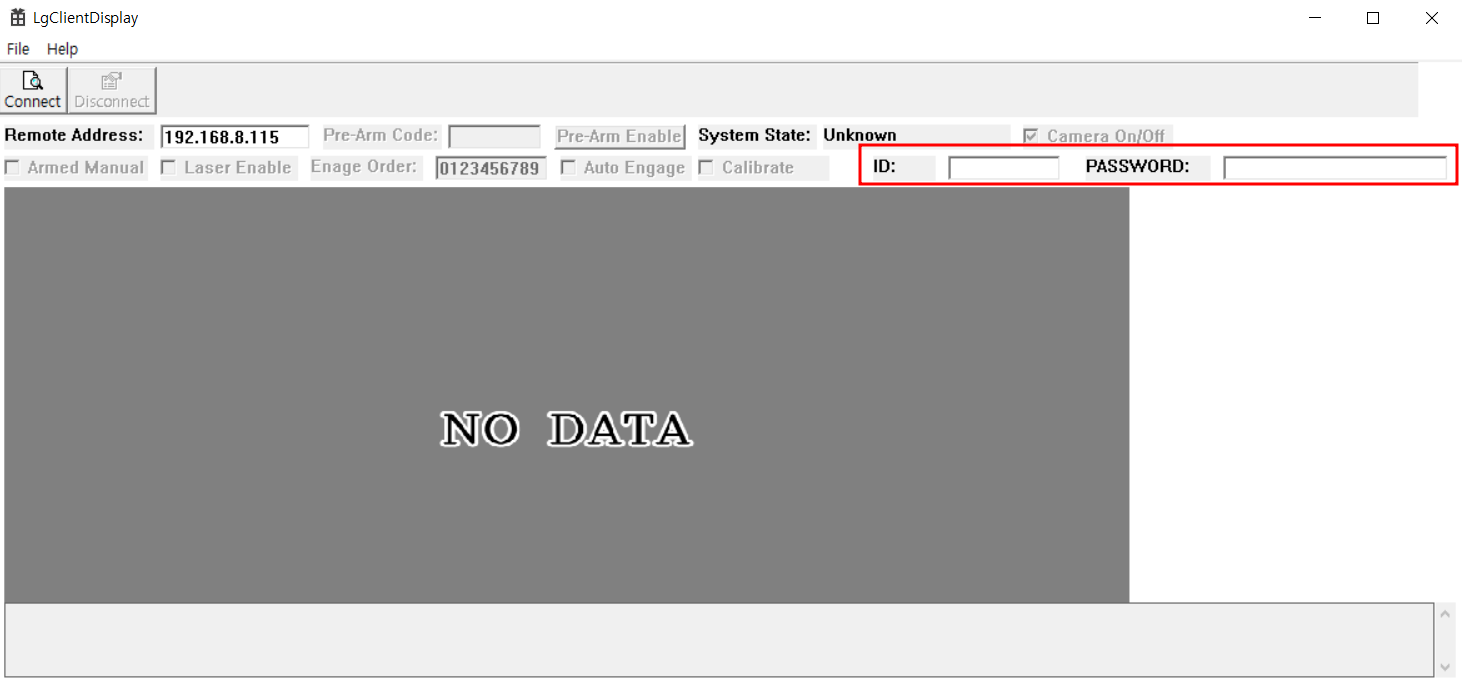


Figure 8 Remote Client application

- Input data is validated with length (over 10) and special character

- If PW setting date is expired, new setting screen will appear

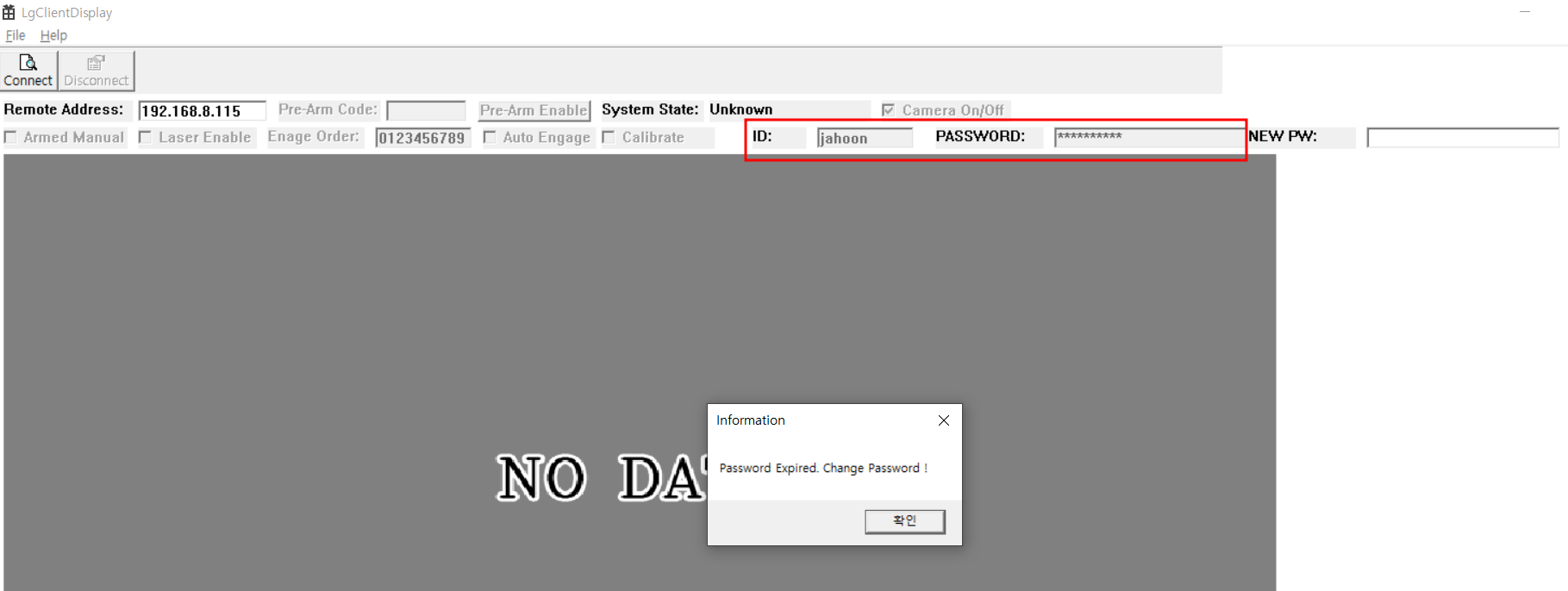


Figure 9 Remote Client application

- If wrong PW are inputted, connection will fail.

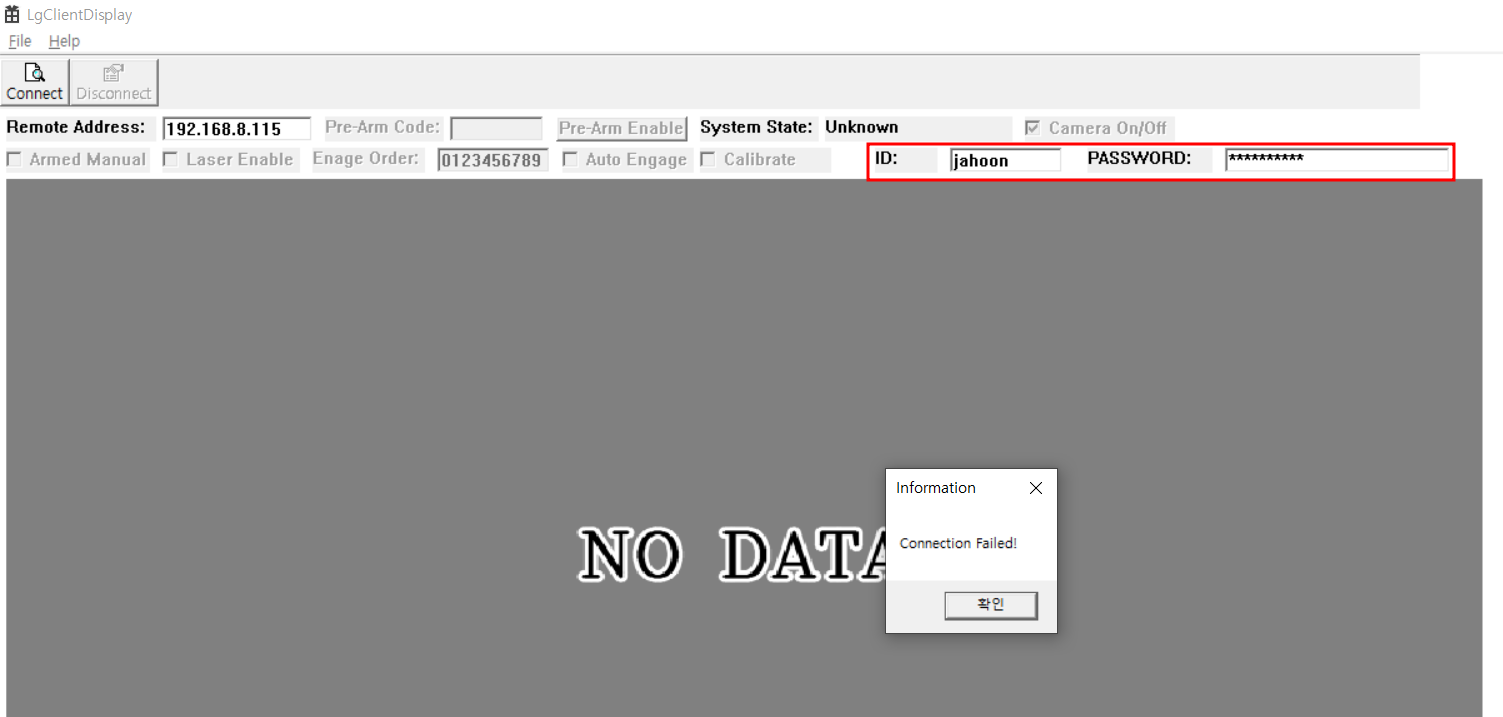


Figure 10 Remote Client application

RFQ.04, 05, 06, 07, 08, 09, 10, 15, 16, 18

2. TCP connection is replaced to TLS connection

- Openssl is imported for server & client

(Rationale : OpenSSL is one of the most widely used open-source TLS and

cryptographic libraries. It is available for both Windows and Linux operating systems

and provides a C language-based API)

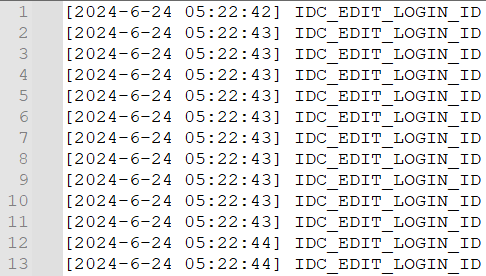
- SSL context / SSL connection is generated and SSL\_read / SSL\_write function is

used for communicating with each other

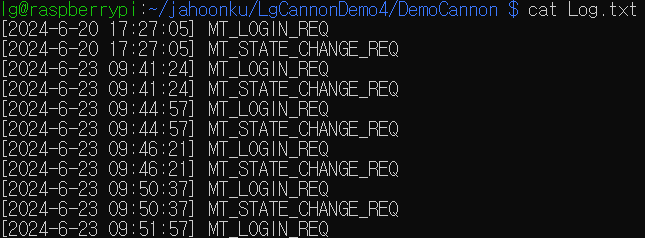
3. Audit system

RFQ.03, 10, 14

- All of user input to remote client application saved to Log.txt



- All of user input from remote client application to server saved to Log.txt



4. Unsafe Mode Control

a. When connection is not established, client application will show warning message

to user

b. If the network connection to the remote interface is lost, warning message

will be showing up (Heartbeat)

c. If the barbette traverses more than 15 degrees left or right of the center aim

line, robot will skip that target

d. If the barbette traverses more than 15 degrees up or down in elevation of the

center aim line, robot will skip that target

e. If the system is in an Unknown, Safe, or Pre-Arm state, the robot shall not

fire the cannon

5. Platform

- Check validation of the important file (ex, correct.ini )

RFQ.11

- Setting access rights for critical files

RFQ.12, 13, 14

- DemoCannon is configured to work as daemon server to provide service

all the time.

RFQ.12, 13, 14, 17, 22