CMU Project Report (Team6)

Table of Contents

[0. Introduction 3](#_Toc74329878)

[1. Schedule 4](#_Toc74329879)

[2. System Requirement 5](#_Toc74329880)

[3. Security Goals 8](#_Toc74329881)

[4. Assets 8](#_Toc74329882)

[5. Threat Modeling 9](#_Toc74329883)

[5.1. DFD 9](#_Toc74329884)

[5.2. STRIDE 9](#_Toc74329885)

[5.3. PnG 14](#_Toc74329886)

[5.4. Result of Threat Modeling 14](#_Toc74329887)

[6. Security Risk Assessment 17](#_Toc74329888)

[7. Security Requirements 18](#_Toc74329889)

[8. Mitigation 19](#_Toc74329890)

[9. Architecture 20](#_Toc74329891)

[9.1. Overall Architecture 20](#_Toc74329892)

[9.2. Terminology and Definitions 20](#_Toc74329893)

[9.3. Source Directory 21](#_Toc74329894)

[9.4. Setup Guide 21](#_Toc74329895)

[9.4.1. Server 21](#_Toc74329896)

[9.4.2. Client 21](#_Toc74329897)

[9.5. Crypto Algorithms 21](#_Toc74329898)

[9.5.1. Primitives and Algorithms 21](#_Toc74329899)

[9.5.2. Symmetric cipher algorithm 22](#_Toc74329900)

[9.5.3. Methods of Secret Hiding 22](#_Toc74329901)

[9.5.4. User Data Encryption/ Decryption 22](#_Toc74329902)

[9.5. Scenario 23](#_Toc74329903)

[10. Static Analysis 25](#_Toc74329904)

[11. Fuzz & Penetration Test 26](#_Toc74329905)

[12. Conclusion 27](#_Toc74329906)

# 0. Introduction

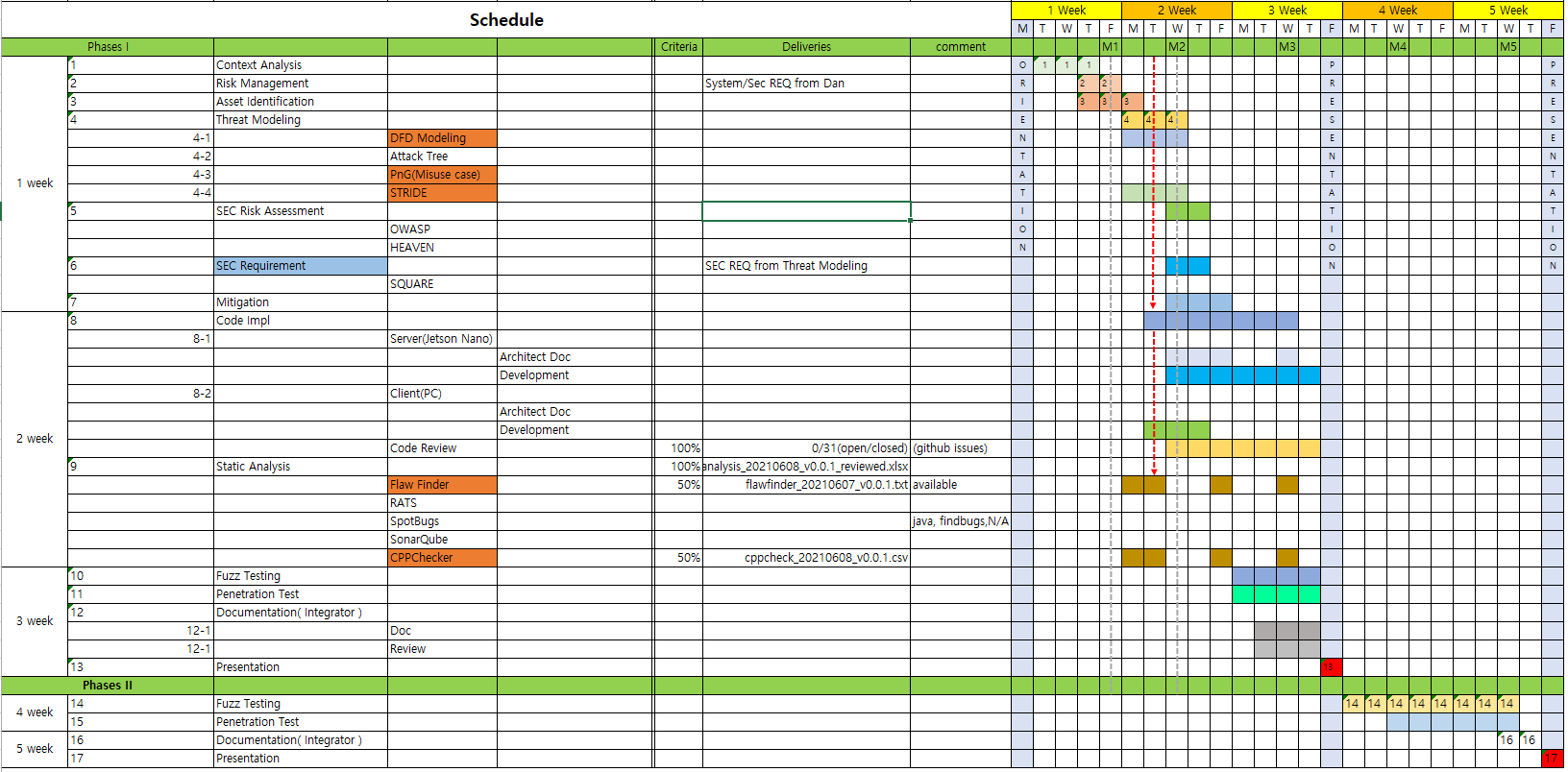
TODO: Introduce team member and role and project



|  |  |
| --- | --- |
| Name | Role |
| Jeonghwan.Ahn | Implement TLS, Crypto, … |
| Jinmo.Kim | Requirement Analysis, Static Analysis, Threat Modeling, Schedule, … |
| Kyungnam.Bae | Implement Client, Contact Point, … |
| Seongju.Moon | Static Analysis, Threat Modeling, … |
| Byungchul.Park | Implement Server, … |

# 1. Schedule

Note: This is our rough schedule that’s set-up in the first week so it will be updated periodically.



# 2. System Requirement

We’ve analyzed the requirement documents that was given by Professor Dan and Professor Jeff. The name of the first document is **LG May 2021 Lecture Secure Coding Project Intro V1.1.pptx.pdf** and the second is **LG Security Class Project Description.pdf.**

We’re struggling to find and extract our system requirement from these documents.

Here is our first artifact from the first, Project Description-1, 2, 3.



But, we needed to compare another document below because it (the second) was also describing system requirements of Jetson Nano system. The second document says requirements of Tartan Secure Camera Application.



Those made us confused. Therefore, we should clarify and draw the requirement for our system after discussing with Professor DAN.

|  |
| --- |
| Summary of meeting with Professor DAN |
| Mandatory requirements described in the "LG May 2021 Lecture Secure Coding Project Intro V1.1.pptx.pdf" document.  - no vulnerability in the system  - secure architecture  - implement 5 modes (run, test run, learning, secure, non-secure)  - Jetson Nano sends the Camera Image and Face Recognized information. It should be separated.  - Client receives the data above, and displays it after combining it |

We’ve extracted our requirements from the list above and attached the result.





# 3. Security Goals

Protecting the user privacy information in our system.

# 4. Assets

|  |  |  |  |
| --- | --- | --- | --- |
| # | Items | Items to manage | Comment |
| 1 | Images for transmission over camera cable | X | Out of S/W boundary |
| 2 | Images for transmission over network | O |  |
| 3 | The Friends video file | O |  |
| 4 | Client program itself | O |  |
| 5 | Client program hash code on server side | O |  |
| 6 | User info. data (ID, type, password) | O |  |

# 5. Threat Modeling

## 5.1. DFD



## 5.2. STRIDE

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Category | Interaction | Description | Justification |
| 1 | Information Disclosure | DF4.2 Load Login Credential / Learning Data ... | Improper data protection of S1. User Credential Data File System can allow an attacker to read information not intended for disclosure. Review authorization settings. | [Threat] If the user credential data is stored as plain text, it can be disclosed.  [Review] Use data encryption |
| 2 | Tampering | DF4.2 Load Login Credential / Learning Data ... | Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources. | [Threat] An attacker modify user credential data. [Review] Use hashing |
| 3 | Spoofing | DF4.2 Load Login Credential / Learning Data ... | S1. User Credential Data File System may be spoofed by an attacker and this may lead to incorrect data delivered to 2.1 Server (Jetson). Consider using a standard authentication mechanism to identify the source data store. | [Threat] An attacker modify user credential data and then server can use it without checking. [Review] Use hashing |
| 4 | Spoofing | DF2.1 Request (Login / Mode Ctrl..) | 2.1 Server (Jetson) may be spoofed by an attacker and this may lead to information disclosure by 1.1 Client (PC). Consider using a standard authentication mechanism to identify the destination process. | [Threat] An attacker spoof the user (Client) [Review] use 2FA |
| 5 | Tampering | DF2.1 Request (Login / Mode Ctrl..) | Data flowing across DF2.1 Request (Login / Mode Ctrl..) may be tampered with by an attacker. This may lead to a denial of service attack against 2.1 Server (Jetson) or an elevation of privilege attack against 2.1 Server (Jetson) or an information disclosure by 2.1 Server (Jetson). Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach. | [Threat] An attacker tampers data to server in order to get information. [Review] use TLS |
| 6 | Repudiation | DF2.1 Request (Login / Mode Ctrl..) | 2.1 Server (Jetson) claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. | [Threat] Clients can repudiate the actions they have performed. [Review] Use mutual authentication |
| 7 | Information Disclosure | DF2.1 Request (Login / Mode Ctrl..) | Data flowing across DF2.1 Request (Login / Mode Ctrl..) may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow. | [Threat] An attack can sniff the data on the connection. [Review] Use TLS Encrypted Communication channel, mTLS (mutual Auth) may be implemented. |
| 8 | Information Disclosure | DF2.1 Request (Login / Mode Ctrl..) | Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme. | [Threat] Weak Authentication may lead to disclose information [Review] Need to more stronger authentication process. Use 2FA |
| 9 | Denial Of Service | DF2.1 Request (Login / Mode Ctrl..) | 2.1 Server (Jetson) crashes, halts, stops or runs slowly; in all cases violating an availability metric. | [Review] Server is simple then there is no way to detect that symptoms. |
| 10 | Denial Of Service | DF2.1 Request (Login / Mode Ctrl..) | An external agent interrupts data flowing across a trust boundary in either direction. | [Threat] the information of the communication between client and server is interrupted by attackers. [Review] using TLS |
| 11 | Elevation Of Privilege | DF2.1 Request (Login / Mode Ctrl..) | 2.1 Server (Jetson) may be able to impersonate the context of 1.1 Client (PC) in order to gain additional privilege. | [Review] Server doesn't need to impersonate in order to gain additional privilege. |
| 12 | Elevation Of Privilege | DF2.1 Request (Login / Mode Ctrl..) | 1.1 Client (PC) may be able to remotely execute code for 2.1 Server (Jetson). | [Review] Client cannot execute code in Server remotely. |
| 13 | Elevation Of Privilege | DF2.1 Request (Login / Mode Ctrl..) | An attacker may pass data into 2.1 Server (Jetson) in order to change the flow of program execution within 2.1 Server (Jetson) to the attacker's choosing. | [Threat] An attacker sends a malicious data to server in order to change the flow of program execution. [Review] need input sanitization |
| 14 | Spoofing | DF3.2 Sensor Data | 3.1 Camera Unit may be spoofed by an attacker and this may lead to unauthorized access to 2.1 Server (Jetson). Consider using a standard authentication mechanism to identify the source process. | [Review] Camera unit can get information only about Camera control signal, cable is dedicated for that. |
| 15 | Spoofing | DF3.2 Sensor Data | 2.1 Server (Jetson) may be spoofed by an attacker and this may lead to information disclosure by 3.1 Camera Unit. Consider using a standard authentication mechanism to identify the destination process. | [Review] Camera is just simple unit, so no threat is expected to arise. |
| 16 | Tampering | DF3.2 Sensor Data | Data flowing across DF3.2 Sensor Data may be tampered with by an attacker. This may lead to a denial of service attack against 2.1 Server (Jetson) or an elevation of privilege attack against 2.1 Server (Jetson) or an information disclosure by 2.1 Server (Jetson). Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach. | [Review] Since it is connected with a physical dedicated cable, it is difficult to interrupts and tamper data from the outside. |
| 17 | Repudiation | DF3.2 Sensor Data | 2.1 Server (Jetson) claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. | [Review] Camera Unit cannot claims the receive data from a source outside. |
| 18 | Information Disclosure | DF3.2 Sensor Data | Data flowing across DF3.2 Sensor Data may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow. | [Review] The camera unit can only do very simple things, and that threat is unlikely to arise. |
| 19 | Denial Of Service | DF3.2 Sensor Data | 2.1 Server (Jetson) crashes, halts, stops or runs slowly; in all cases violating an availability metric. | [Review] Server is simple then there is no way to detect that symptoms. |
| 20 | Denial Of Service | DF3.2 Sensor Data | An external agent interrupts data flowing across a trust boundary in either direction. | [Review] Since they are connected by physical cables, it is difficult to interrupt with data. |
| 21 | Elevation Of Privilege | DF3.2 Sensor Data | 2.1 Server (Jetson) may be able to impersonate the context of 3.1 Camera Unit in order to gain additional privilege. | [Review] Even if the camera unit acquires additional privileges, It just send Sensor Data, so no threat is expected to arise. |
| 22 | Elevation Of Privilege | DF3.2 Sensor Data | 3.1 Camera Unit may be able to remotely execute code for 2.1 Server (Jetson). | [Review] Camera is just simple unit, so no threat is expected to arise. |
| 23 | Elevation Of Privilege | DF3.2 Sensor Data | An attacker may pass data into 2.1 Server (Jetson) in order to change the flow of program execution within 2.1 Server (Jetson) to the attacker's choosing. | [Review] Camera is just simple unit, so no threat is expected to arise. |
| 24 | Spoofing | DF3.1 Camera Ctrl | 2.1 Server (Jetson) may be spoofed by an attacker and this may lead to unauthorized access to 3.1 Camera Unit. Consider using a standard authentication mechanism to identify the source process. | [Review] Server can control Camera Unit via Device driver, and authorized access is taken care of by the OS. |
| 25 | Spoofing | DF3.1 Camera Ctrl | 3.1 Camera Unit may be spoofed by an attacker and this may lead to information disclosure by 2.1 Server (Jetson). Consider using a standard authentication mechanism to identify the destination process. | [Review] Camera unit can get information only about Camera control signal, cable is dedicated for that. |
| 26 | Tampering | DF3.1 Camera Ctrl | Data flowing across DF3.1 Camera Ctrl may be tampered with by an attacker. This may lead to a denial of service attack against 3.1 Camera Unit or an elevation of privilege attack against 3.1 Camera Unit or an information disclosure by 3.1 Camera Unit. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach. | [Review] Since it is connected with a physical dedicated cable, it is difficult to interrupts and tamper data outside. |
| 27 | Repudiation | DF3.1 Camera Ctrl | 3.1 Camera Unit claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. | [Review] Camera Unit cannot claims the receive data from a source outside. |
| 28 | Information Disclosure | DF3.1 Camera Ctrl | Data flowing across DF3.1 Camera Ctrl may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow. | [Review] The camera unit can only do very simple things, and that threat is unlikely to arise. |
| 29 | Denial Of Service | DF3.1 Camera Ctrl | 3.1 Camera Unit crashes, halts, stops or runs slowly; in all cases violating an availability metric. | [Threat] It may be physically damaged and you may not be able to get Data from Camera [Review] Protect Camera from physical damage |
| 30 | Denial Of Service | DF3.1 Camera Ctrl | An external agent interrupts data flowing across a trust boundary in either direction. | [Review] Since they are connected by physical cables, it is difficult to interrupt with data. |
| 31 | Elevation Of Privilege | DF3.1 Camera Ctrl | 3.1 Camera Unit may be able to impersonate the context of 2.1 Server (Jetson) in order to gain additional privilege. | [Review] Even if the camera unit acquires additional privileges, It just send Sensor Data, so no threat is expected to arise. |
| 32 | Elevation Of Privilege | DF3.1 Camera Ctrl | 2.1 Server (Jetson) may be able to remotely execute code for 3.1 Camera Unit. | [Review] Camera is just simple unit, so no threat is expected to arise. |
| 33 | Elevation Of Privilege | DF3.1 Camera Ctrl | An attacker may pass data into 3.1 Camera Unit in order to change the flow of program execution within 3.1 Camera Unit to the attacker's choosing. | [Review] Camera is just simple unit, so no threat is expected to arise. |
| 34 | Denial Of Service | DF4.1 Store Login Credential / Learning Data ... | Does 2.1 Server (Jetson) or S1. User Credential Data File System take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout. | [Threat] It is possible to add a lot of Images in the storage. [Review] The limitation of number of image is need. |
| 35 | Information Disclosure | DF4.1 Store Login Credential / Learning Data ... | Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a salted hash of the credentials instead of storing the credentials themselves. If this is not possible due to business requirements, be sure to encrypt the credentials before storage, using an SDL-approved mechanism. For client side, if storing credentials is required, encrypt them and protect the data store in which they're stored | [Threat] User credential may be disclosed. [Review] User credential should be encrypted before being stored. |
| 36 | Repudiation | DF4.1 Store Login Credential / Learning Data ... | Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs, or attack log analysis programs. Ensure access to the log is through a reference monitor, which controls read and write separately. Document what filters, if any, readers can rely on, or writers should expect | [Review] This case will not happen in the system. |
| 37 | Repudiation | DF4.1 Store Login Credential / Learning Data ... | Does the log capture enough data to understand what happened in the past? Do your logs capture enough data to understand an incident after the fact? Is such capture lightweight enough to be left on all the time? Do you have enough data to deal with repudiation claims? Make sure you log sufficient and appropriate data to handle a repudiation claims. You might want to talk to an audit expert as well as a privacy expert about your choice of data. | [Review] This case will not happen in the system. |
| 38 | Repudiation | DF4.1 Store Login Credential / Learning Data ... | Do you accept logs from unknown or weakly authenticated users or systems? Identify and authenticate the source of the logs before accepting them. | [Review] This case will not happen in the system. |
| 39 | Repudiation | DF4.1 Store Login Credential / Learning Data ... | If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. Only allow trusted code to log. | [Review] This case will not happen in the system. |
| 40 | Tampering | DF4.1 Store Login Credential / Learning Data ... | Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources. | [Review] This case will not happen in the system. |
| 41 | Spoofing | DF4.1 Store Login Credential / Learning Data ... | S1. User Credential Data File System may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of S1. User Credential Data File System. Consider using a standard authentication mechanism to identify the destination data store. | [Threat] User Credential Data can be exposed to attackers. [Review] User Credential Data should be kept securely. |
| 42 | Spoofing | DF1.1 User Input (Login Credential & Mode Control Input) | E1. Human User may be spoofed by an attacker and this may lead to unauthorized access to 1.1 Client (PC). Consider using a standard authentication mechanism to identify the external entity. | [Review] Client cannot distinguish Human Users. |
| 43 | Elevation Of Privilege | DF1.1 User Input (Login Credential & Mode Control Input) | 1.1 Client (PC) may be able to impersonate the context of E1. Human User in order to gain additional privilege. | [Review] Client cannot distinguish Human Users. |
| 44 | Spoofing | DF2.5 Result (Video Stream...) | 2.1 Server (Jetson) may be spoofed by an attacker and this may lead to unauthorized access to 1.1 Client (PC). Consider using a standard authentication mechanism to identify the source process. | [Threat] Server (Jetson) may be spoofed by an attacker  [Review] use mutual authentication |
| 45 | Spoofing | DF2.5 Result (Video Stream...) | 1.1 Client (PC) may be spoofed by an attacker and this may lead to information disclosure by 2.1 Server (Jetson). Consider using a standard authentication mechanism to identify the destination process. | [Threat] Client (PC) may be spoofed by an attacker  [Review] use mutual authentication |
| 46 | Tampering | DF2.5 Result (Video Stream...) | Data flowing across DF2.5 Result (Video Stream...) may be tampered with by an attacker. This may lead to a denial of service attack against 1.1 Client (PC) or an elevation of privilege attack against 1.1 Client (PC) or an information disclosure by 1.1 Client (PC). Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach. | [Threat] Video Stream may be tampered with by an attacker. [Review] Video Stream over the connection should be protected. |
| 47 | Repudiation | DF2.5 Result (Video Stream...) | 1.1 Client (PC) claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. | [Review] even though This case will happen, this case does not affect. |
| 48 | Information Disclosure | DF2.5 Result (Video Stream...) | Data flowing across DF2.5 Result (Video Stream...) may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow. | [Threat] Video Stream may be sniffed with by an attacker. [Review] Video Stream over the connection should be protected. |
| 49 | Denial Of Service | DF2.5 Result (Video Stream...) | 1.1 Client (PC) crashes, halts, stops or runs slowly; in all cases violating an availability metric. | [Threat] Client (PC) crashes, halts, stops or runs slowly. [Review] Server is working properly. |
| 50 | Denial Of Service | DF2.5 Result (Video Stream...) | An external agent interrupts data flowing across a trust boundary in either direction. | [Review] This case won't be handled. |
| 51 | Elevation Of Privilege | DF2.5 Result (Video Stream...) | 1.1 Client (PC) may be able to impersonate the context of 2.1 Server (Jetson) in order to gain additional privilege. | [Review] support only single user |
| 52 | Elevation Of Privilege | DF2.5 Result (Video Stream...) | 2.1 Server (Jetson) may be able to remotely execute code for 1.1 Client (PC). | [Threat] Server (Jetson) may be able to remotely execute code [Review] need input sanitization |
| 53 | Elevation Of Privilege | DF2.5 Result (Video Stream...) | An attacker may pass data into 1.1 Client (PC) in order to change the flow of program execution within 1.1 Client (PC) to the attacker's choosing. | [Threat] An attacker may pass data into 1.1 Client (PC) [Review] need input sanitization |
| 54 | Information Disclosure | DF3.1 Camera Ctrl | Credentials on the wire are often subject to sniffing by an attacker. Are the credentials re-usable/re-playable? Are credentials included in a message? For example, sending a zip file with the password in the email. Use strong cryptography for the transmission of credentials. Use the OS libraries if at all possible, and consider cryptographic algorithm agility, rather than hardcoding a choice. | [Review] Since they are connected by physical cables, it is difficult to interrupt with data. |
| 55 | Information Disclosure | DF3.2 Sensor Data | Credentials on the wire are often subject to sniffing by an attacker. Are the credentials re-usable/re-playable? Are credentials included in a message? For example, sending a zip file with the password in the email. Use strong cryptography for the transmission of credentials. Use the OS libraries if at all possible, and consider cryptographic algorithm agility, rather than hardcoding a choice. | [Review] Since they are connected by physical cables, it is difficult to interrupt with data. |

## 5.3. PnG

|  |  |  |
| --- | --- | --- |
| PnG 1 | Type | Internal Engineer |
| Goal | Ruin the administrator's reputation |
| Motivation | Revenge to the administrator |
| Skill | manipulate the user credential data, find out the administrator’s password from the previous one that is used to other system |
| Misuse case | 1. Change the image data not to recognize registered users.  2. Disclose administrator’s ID/Password to the employees in the company. |

|  |  |  |
| --- | --- | --- |
| PnG 2 | Type | Spy |
| Goal | Steal all components of the system |
| Motivation | Competitors request |
| Skill | Physical power and ability to use various equipment |
| Misuse case | 1. Steal the client and server |

|  |  |  |
| --- | --- | --- |
| PnG 3 | Type | Hacker |
| Goal | Post the achievements of hacking on the internet |
| Motivation | Strives for recognition |
| Skill | Extensive knowledge of network protocols and hacking program. |
| Misuse case | 1. Sniff the communication channel between server and client to get user credential data. |

## 5.4. Result of Threat Modeling

We found 25 threats by using STRIDE, PnG, Brainstorming.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Tool | Category | Interaction | Threat | Review |
| 1 | STRIDE | Information Disclosure | DF4.2 Load Login Credential / Learning Data ... | If the user credential data is stored as plain text, it can be disclosed. | User credential should be kept securely |
| 2 | STRIDE | Tampering | DF4.2 Load Login Credential / Learning Data ... | An attacker modify user credential data. | User credential should be kept securely |
| 3 | STRIDE | Spoofing | DF4.2 Load Login Credential / Learning Data ... | An attacker modify user credential data and then server can use it without checking. | User credential should be kept securely |
| 4 | STRIDE | Spoofing | DF2.1 Request (Login / Mode Ctrl..) | An attacker spoof the user (Client) | Need to more stronger authentication process |
| 5 | STRIDE | Tampering | DF2.1 Request (Login / Mode Ctrl..) | An attacker tampers Login or Mode control data to server in order to get information. | Need to encrypt communication channel |
| 6 | STRIDE | Repudiation | DF2.1 Request (Login / Mode Ctrl..) | Clients can repudiate the actions they have performed. | Need to apply mutual authentication |
| 7 | STRIDE | Information Disclosure | DF2.1 Request (Login / Mode Ctrl..) | An attack can sniff the data on the connection. | Need to consider encrypting the data flow. |
| 8 | STRIDE | Information Disclosure | DF2.1 Request (Login / Mode Ctrl..) | Weak authentication may lead to disclose information | Need to more stronger authentication process |
| 10 | STRIDE | Denial Of Service | DF2.1 Request (Login / Mode Ctrl..) | the information of the communication between client and server is interrupted by attackers. | Need to use TLS |
| 13 | STRIDE | Elevation Of Privilege | DF2.1 Request (Login / Mode Ctrl..) | An attacker sends a malicious data to server in order to change the flow of program execution. | Need to apply input sanitization |
| 29 | STRIDE | Denial Of Service | DF3.1 Camera Ctrl | It may be physically damaged and you may not be able to get Data from Camera | Need to protect camera unit from physical damage |
| 34 | STRIDE | Denial Of Service | DF4.1 Store Login Credential / Learning Data ... | It is possible to add a lot of Images in the storage. | Need to limit the number of images |
| 35 | STRIDE | Information Disclosure | DF4.1 Store Login Credential / Learning Data ... | User credential may be disclosed. | Need to encrypt user credential data |
| 41 | STRIDE | Spoofing | DF4.1 Store Login Credential / Learning Data ... | User Credential Data can be exposed to attackers. | Need to encrypt user credential data |
| 44 | STRIDE | Spoofing | DF2.5 Result (Video Stream...) | Server (Jetson) may be spoofed by an attacker | Need to apply mutual authentication |
| 45 | STRIDE | Spoofing | DF2.5 Result (Video Stream...) | Client (PC) may be spoofed by an attacker | Need to apply mutual authentication |
| 46 | STRIDE | Tampering | DF2.5 Result (Video Stream...) | Video Stream may be tampered with by an attacker. | Need to protect the video stream over the connection |
| 48 | STRIDE | Information Disclosure | DF2.5 Result (Video Stream...) | Video Stream may be sniffed with by an attacker. | Need to protect the video stream over the connection |
| 49 | STRIDE | Denial Of Service | DF2.5 Result (Video Stream...) | Client (PC) crashes, halts, stops or runs slowly. | Need to remain stable in abnormal cases |
| 52 | STRIDE | Elevation Of Privilege | DF2.5 Result (Video Stream...) | Server (Jetson) may be able to remotely execute code | Need input sanitization |
| 53 | STRIDE | Elevation Of Privilege | DF2.5 Result (Video Stream...) | An attacker may pass data into 1.1 Client (PC) | Need input sanitization |
| 56 | PnG | Tampering | User credential data | Change the image data not to recognize registered users. | Need to protect user credential data |
| 57 | PnG | Information Disclosure | Client => Server | Disclose administrator’s ID/Password to the employees in the company. | Need to more stronger process for authentication |
| 59 | PnG | Information Disclosure | Server <=> Client | Sniff the communication channel between server and client to get user credential data. | Need to protect the data over the connection |
| 60 | Brainstorming | N/A | Network | Compromise the connection of network physically by an attacker | Server need to be robust in abnormal case. |

# 6. Security Risk Assessment

# 7. Security Requirements

// TODO: update Security Requirements

-- iter 1

[ ] Any information related (personal) privacy SHALL be protected securely. (Friend video/Learned PHOTO)

[ ] Any information related (personal) privacy SHALL be accessible to only authorized entities. (Learned PHOTO)

[\*] The system SHALL use only approved algorithms for cryptographic operation.

[\*] Server and client SHALL communicate over encrypted and authenticated channel.

-- iter 2

[\*] Any information related (personal) privacy SHALL be protected securely. (ID/PASS/Friend video/Learned PHOTO)

[\*] Any information related (personal) privacy SHALL be accessible to only authorized entities. (ID/PASS/Learned PHOTO)

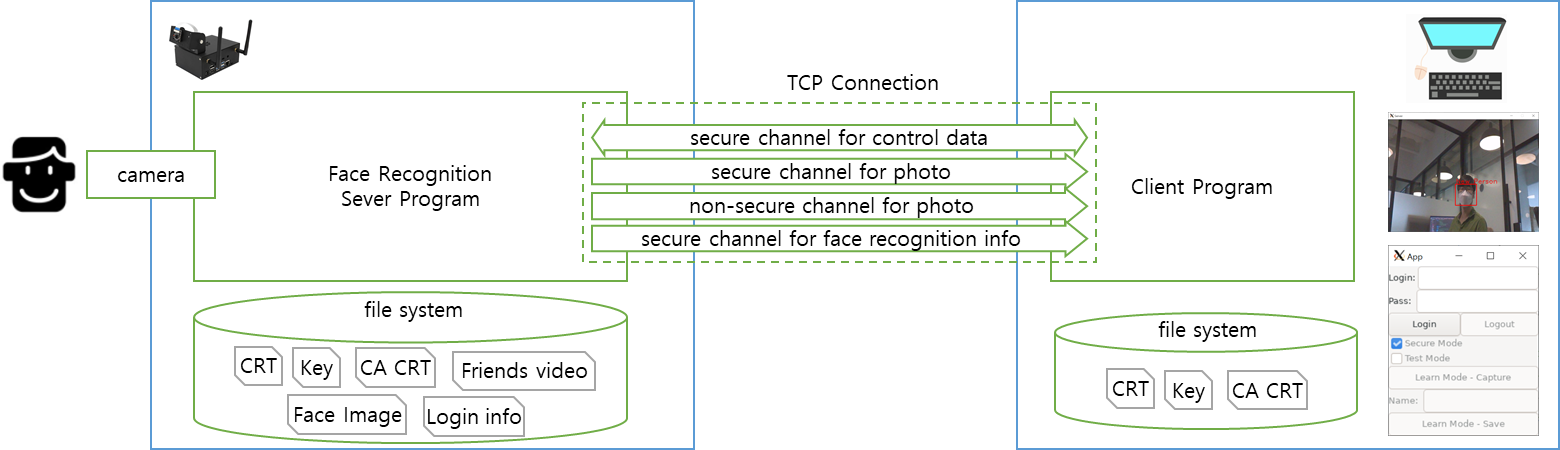
[\*] The system SHALL have a resiliency against key compromise. (TLS Key, Cert)

# 8. Mitigation

// TODO:

# 9. Architecture

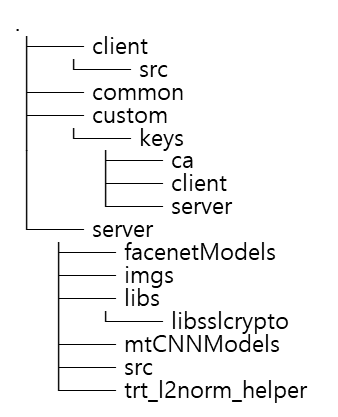
## 9.1. Overall Architecture



## 9.2. Terminology and Definitions

|  |  |
| --- | --- |
| **Terminology** | **Definitions** |
| CA CRT | Self-signed Root Certificate |
| CRT | CA signed Certificate |
| Key | Private Key |
| Login info |  |
| Face Image |  |
| Photo |  |
| Secure Mode |  |
| Non Secure Mode |  |
| Run Mode |  |
| Test Run Mode |  |
| Learn Mode |  |
| Secure channel for control data | TLS TCP connection.  The request and response message is transmitted. |
| Secure channel for photo | TLS TCP connection.  The photo data is transmitted from the server to the client |
| Non-secure channel for photo | TCP connection.  The photo data is transmitted from the server to the client |
| Secure channel for face recognition info | TLS TCP connection.  The coordination of the recognized face on the photo and the recognized name is transmitted from the server to the client |

## 9.3. Source Directory



## 9.4. Setup Guide

### 9.4.1. Server

|  |
| --- |
| # cd source/server/  # python3 step01\_pb\_to\_uff.py  # rm -rf MTCNN\_FaceDetection\_TensorRT/  # git clone https://github.com/PKUZHOU/MTCNN\_FaceDetection\_TensorRT  # mv MTCNN\_FaceDetection\_TensorRT/det\* ./mtCNNModels  # mkdir build; cd build  # cmake -DCMAKE\_BUILD\_TYPE=Release ..  # make -j  # ./LgFaceRecDemoTCP\_Jetson\_NanoV2 5000 9.2.2. Client |

### 9.4.2. Client

|  |
| --- |
| # apt install cmake libssl-dev libgtkmm-3.0-dev libopencv-dev  # cd source/client/ && mkdir build; cd build  # cmake ..  # make  # ./client |

## 9.5. Crypto Algorithms

### 9.5.1. Primitives and Algorithms

1. Crypto Library : OpenSSL
2. Version : 1.1.1
3. OpenSSL has known vulnerabilities, but Jetson Nano Development Environment has dependencies to OpenSSL 1.1.1 (ex: curl, cmake ...), so we use this version as is.
4. Followings are known vulnerabilities on OpenSSL 1.1.1
   1. CVE-2021-3449
   2. CVE-2021-23841
   3. CVE-2021-23840
   4. CVE-2020-1971
   5. CVE-2019-1563
   6. CVE-2019-1552
   7. CVE-2019-1551
   8. CVE-2019-1549
   9. CVE-2019-1547
   10. CVE-2019-1543
   11. CVE-2019-0190
   12. CVE-2018-0735
   13. CVE-2018-0734
   14. CVE-2007-5502

### 9.5.2. Symmetric cipher algorithm

1. Algorithm : AES
2. Key Size : 256 bits
3. Mode of Operation : CBC
4. Key derivation function : PBKDF2

### 9.5.3. Methods of Secret Hiding

1. Code obfuscation: Hardware security module will provide the strong security strength. However, the system in this project has no support of hardware security anchor (e.g. TPM, HSM, PUF, TE etc.), So Code obfuscation is practical alternative choice (unless Whitebox crypto is not considered). Code obfuscation is less secure than Whitebox crypto, however, it provides the reliable security strength against real-world attacks.

### 9.5.4. User Data Encryption/ Decryption

1. Server encrypt user data. Examples of user data includes followings
   1. AI classified photo
   2. Video
   3. User credentials
   4. Key and CRT for TLS
2. Overall flows on user data encryptions are shown in the figure below



* 1. AES key for ROOT is obfuscated and distributed in code
  2. Use PBKDF2 function for derive ROOT key
  3. Create hash and attach for Integrity verification
  4. Generate Random Number and use it for AES encrypt key in every time at encrypt User Data

1. Overall flows on user data decryptions are shown in the figure below



## 9.5. Scenario

# 10. Static Analysis

# 11. Fuzz & Penetration Test

# 12. Conclusion