

# **Security Specialist Project**

## **Secure Jetson Nano**

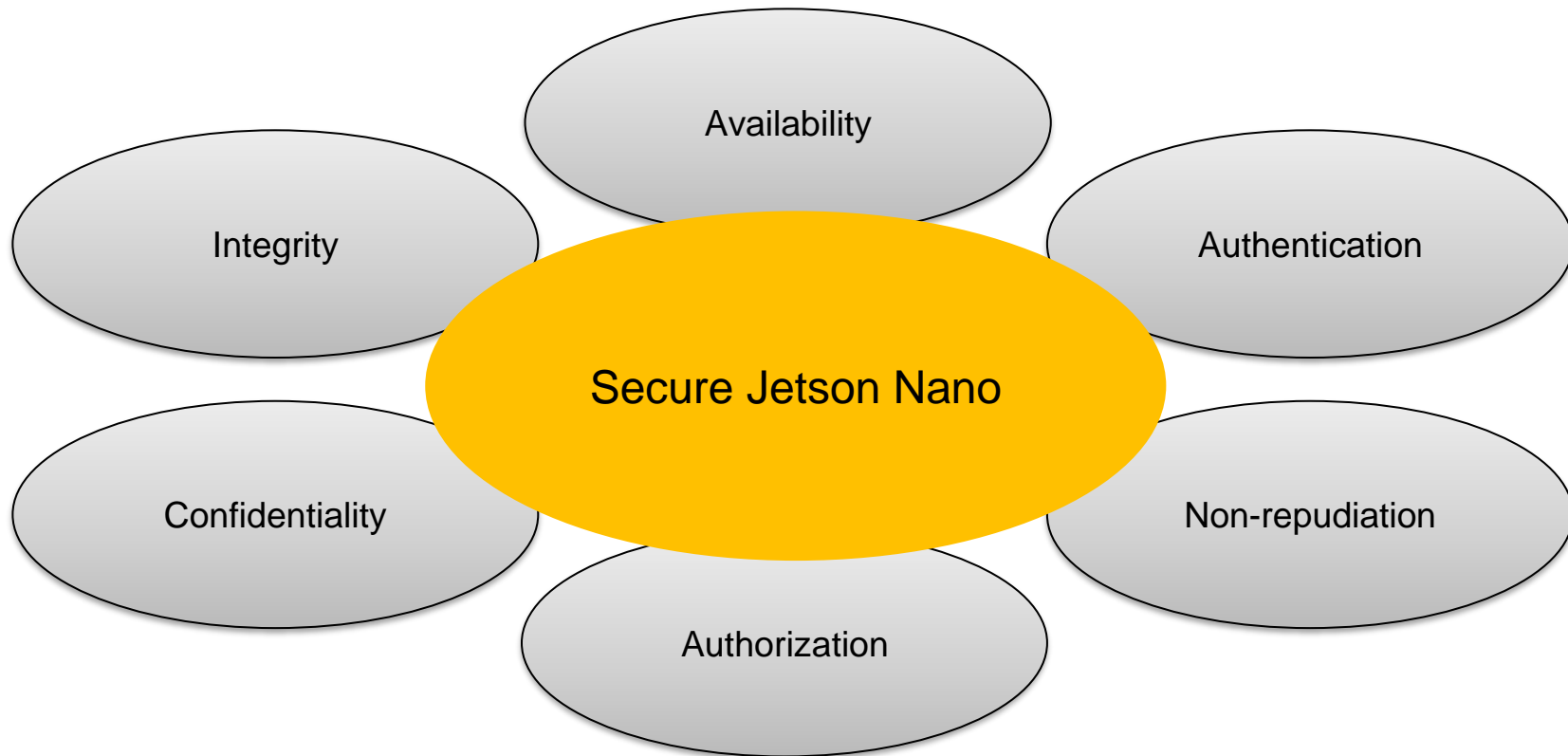
**ShinPark Team**

**LGE security specialist Team 1 developed a Secure Jetson Nano for the project of '2021 LGE Security Specialist course' in Carnegie Mellon University.**

**This document contains a security concept that aims to fulfill the security development process. The secure Jetson Nano is developed to cover the following processes:**

- 1. Asset Identification**
- 2. Security Risk Assessment**
- 3. Threat Analysis**
- 4. Mitigation Threats**
- 5. Security Requirements**
- 6. Secure Coding**
- 7. Static Analysis**

Goal of secure Jetson Nano is based on 6 security characteristics.

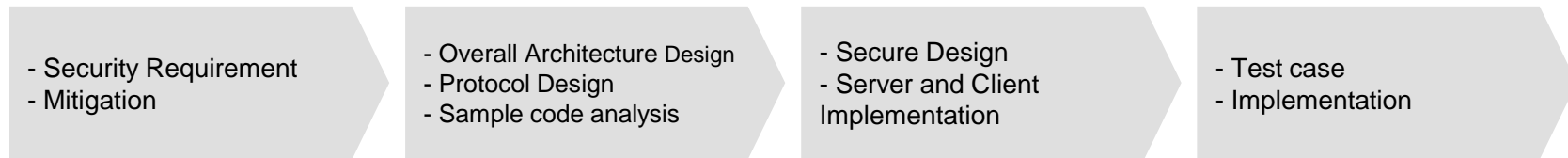


Role	Description	Name	Responsibility
<b>Project Manager</b>	<ul style="list-style-type: none"><li>• Project Coordinator</li><li>• Schedule management</li></ul>	<ul style="list-style-type: none"><li>• Jonghyun Park</li></ul>	Organize the team and manages project resources by planning. Manages the relationship with project stakeholder and mentor
<b>Architect</b>	<ul style="list-style-type: none"><li>• System Design</li><li>• Implementation review</li></ul>	<ul style="list-style-type: none"><li>• Sungjin Lee</li></ul>	Create strategy of system architecture development Detailed design of server and communication protocols
<b>Developer</b>	<ul style="list-style-type: none"><li>• Definition protocol</li><li>• Implementation secure channel</li></ul>	<ul style="list-style-type: none"><li>• Seokwang Kim</li><li>• Jaewon Lee</li></ul>	Have ownership of development server application
	<ul style="list-style-type: none"><li>• UX Design</li><li>• Client Application</li><li>• Protocol Design</li></ul>	<ul style="list-style-type: none"><li>• Yeonbi Shin</li><li>• Sungsoo Kim</li></ul>	Detail design of client application
<b>Tester</b>	<ul style="list-style-type: none"><li>• Create Test case</li><li>• Fuzz testing &amp; Static Analysis</li></ul>	<ul style="list-style-type: none"><li>• Jonghyun Park</li><li>• Sungjin Lee</li><li>• Jaewon Lee</li></ul>	Create test strategy and test cases Ensure the products meet standards of quality

### 1 Week (Planning & Analysis)



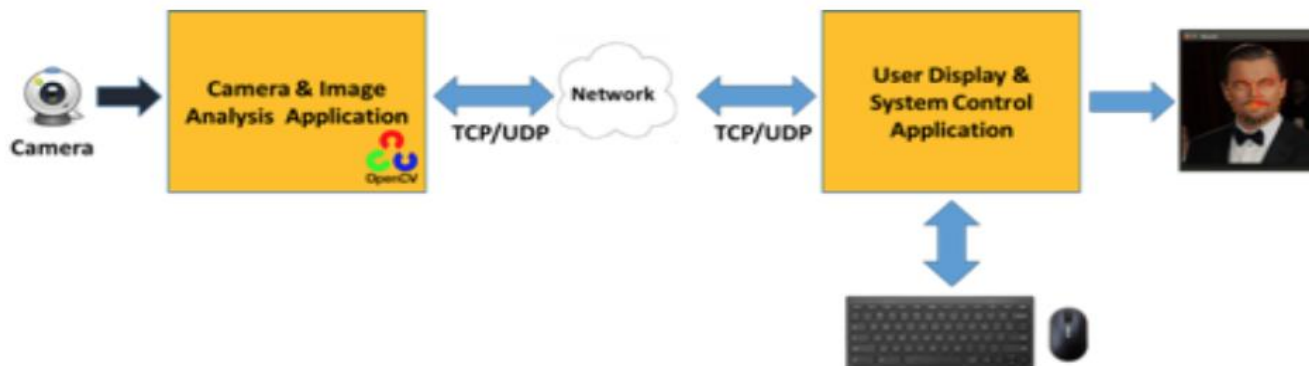
### 2 Week (Analysis & Design)



### 3 Week (Implementation & Test)

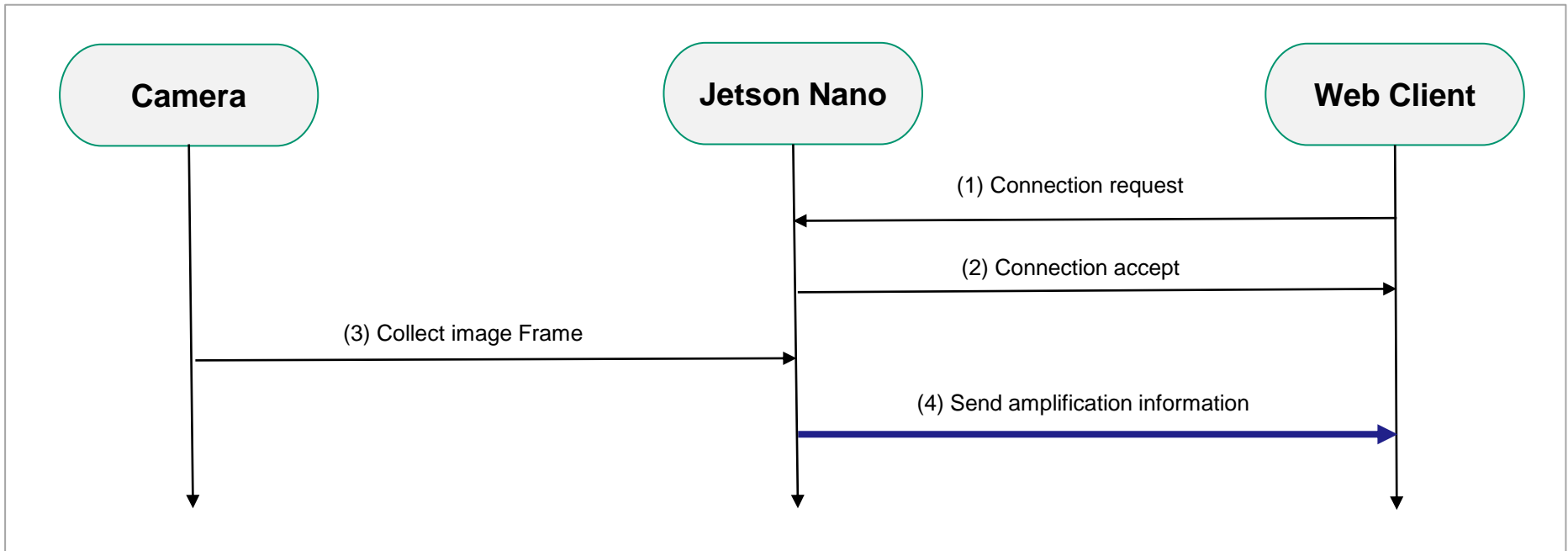


	Jetson Nano	Client
<b>HW</b>	<ul style="list-style-type: none"><li>• Jetson Nano Board</li><li>• Camera module</li></ul>	<ul style="list-style-type: none"><li>• PC</li></ul>
<b>Interface</b>	<ul style="list-style-type: none"><li>• Wi-Fi</li><li>• USB</li></ul>	<ul style="list-style-type: none"><li>• Wi-Fi</li></ul>
<b>OS</b>	<ul style="list-style-type: none"><li>• Ubuntu 18.04</li></ul>	<ul style="list-style-type: none"><li>• Windows 10</li></ul>
<b>SW Module</b>	<ul style="list-style-type: none"><li>• FaceRecDemoTCP</li></ul>	<ul style="list-style-type: none"><li>• RecvImageTCP</li></ul>
<b>Data</b>	<ul style="list-style-type: none"><li>• Video Stream</li><li>• Captured Image</li><li>• User ID/PW</li></ul>	<ul style="list-style-type: none"><li>• Video Stream</li><li>• Captured Image</li><li>• User ID/PW</li></ul>



## 2.1 Sequence Diagram

1. User connect the Jetson Nano through SSH using specified ID/PW.
2. Jetson Nano uses a camera to collect image frames and analyzes them with artificial intelligence (AI) to implement face detection and recognition.
3. After the video frame is analyzed, the additional amplification information obtained from the analysis is sent to the user display and system control application.
4. The user display and system control application get the information from Jetson Nano and display it.



### Basic system requirements without considering security aspects.

Part	No.	Requirement
General	RQ-GEN-01	Server and client should communicate normally.
	RQ-GEN-02	Secure or non-secure mode should be implemented between the server and the client.
	RQ-GEN-03	The status of connection should be reported (eg. fault/error detection, recovery, etc)
Jetson Nano (Server)	RQ-SVR-01	Server should be run as Learning, Run, Test Run Mode.
	RQ-SVR-02	In learning mode, the name of the person in front of the camera should be input, registered in the DB, and the result should be transmitted to the client.
	RQ-SVR-03	In Run Mode, the server should perform face recognition using the camera and transmit the result to the client.
	RQ-SVR-04	In Test Run Mode, face recognition should be performed using the given video file and the result should be transmitted to the client.
	RQ-SVR-05	The server should be able to map multiple photos of a user to a single ID.
	RQ-SVR-06	The server must listen to the Secure/Non Secure port for secure communication.
PC (Client)	RQ-CLI-01	In the client authentication screen, the SW should provide a UI that determines the Secure/Non Secure mode among the communication methods with the server.
	RQ-CLI-02	The client SW should provide a UI that determines the operation mode of the server - Learning, Run, Test Run Mode.
	RQ-CLI-03	In learning mode, the client must pass the username as input to the server .



### 3. Asset Identification

Asset of Jetson Nano?

- Things attackers want
- Things you want to protect
- Stepping stones to either of these

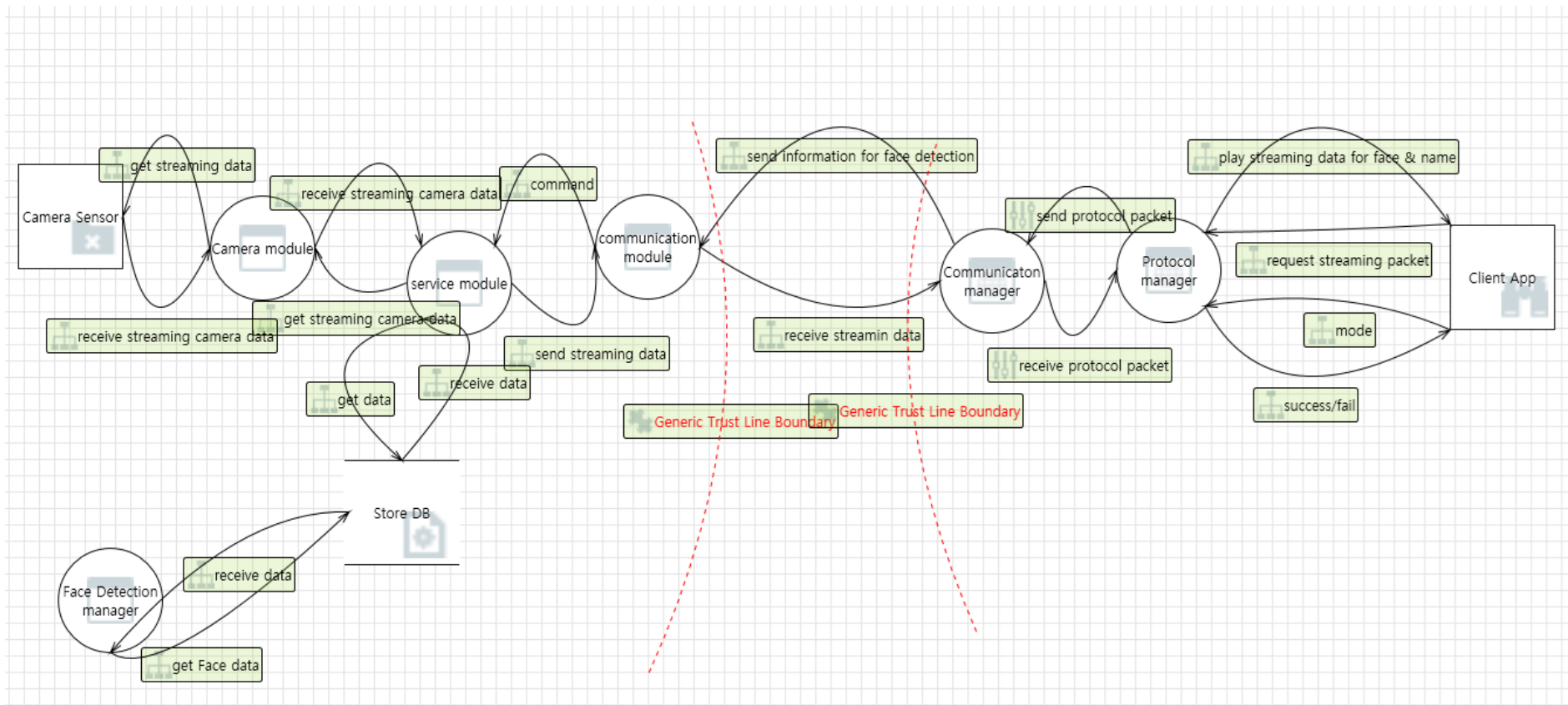
Part	No.	Asset
HW	Asset-HW-01	Camera
	Asset-HW-02	Jetson Nano
	Asset-HW-03	PC
SW	Asset-SW-01	User Information
	Asset-SW-02	Face Data Base
	Asset-SW-03	Image Information data (name, count, etc)
	Asset-SW-04	Control system data (mode, error, etc)

## 4. Risk Assessment

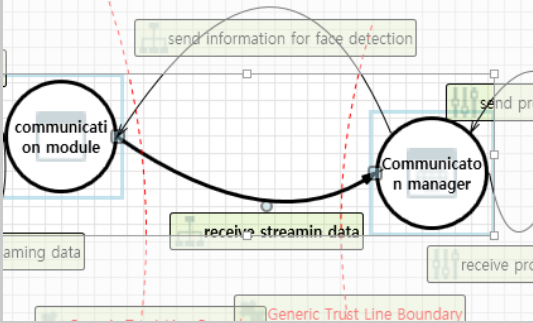
Identify project risks

RISK ID	Condition	Consequence	Probability	Impact	Rating
RSK-01	Noise data from the network	The control system cannot quickly set the normal data.	9	2	18
RSK-02	Replay attack for Network communication	Attacker can use old packet for replay attack	5	10	50
RSK-03	Data flow sniffing	Attacker can see the data from camera to control system	7	8	56
RSK-04	Someone stole Jetson Nano board	The project will be stopped, and it takes a long time to buy a new one.	2	5	10
RSK-05	Face image and names stored in DB leaked	Personal information leakage	3	7	21
RSK-06	The network packet between the Jetson Nano board and the client pc is sniped	Information from DB data is leaked and hacker can be tricked into a registered member and access is successful.	9	9	81
RSK-07	One of your team members is ill or infected with Covid-19. Vacation due to emergency.	The patient could not participate in the project until fully recovered, increasing the stress on the remaining members. In the worst case, schedule delays or reduced project completion	6	7	42
RSK-08	Jetson Nano board or camera module is physically broken	Project cannot be completed because there is no replacement HW	5	10	50
RSK-09	Lost or broken development PC	Work is delayed	2	6	12
RSK-10	Design or threat modeling that differs from project goals	Failed to submit project results and must be completely redesigned and redeveloped	3	8	24
RSK-11	Saved DBs can be tampered with by hackers.	Security cameras recognize faces differently. For example, consider A as B.	2	10	20
RSK-12	Normal user get administrator right (root privilege) and change the system.	A normal user can put a malicious backdoor on behalf of the normal system.	3	10	30
RSK-13	Jetson Nano responds that it did not receive the data sent by the client.	The mode setting data sent by the client cannot be transmitted and may be set to another mode.	3	8	24

## DFD for Threat Analysis



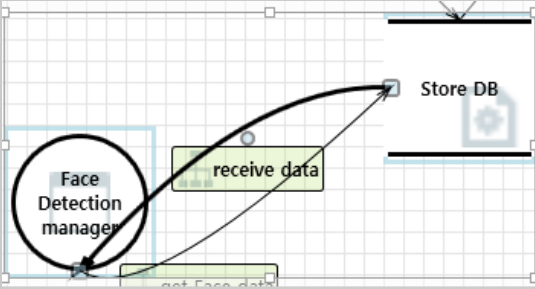
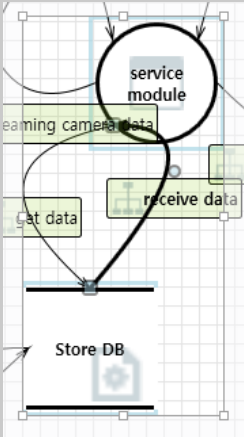
# 5.1 Threat modeling - STRIDE

Interaction Part	Category	Description	Asset No.
	Tampering	If communication module is given access to memory, such as shared memory or pointers, or is given the ability to control what Communication manager executes (for example, passing back a function pointer.), then communication module can tamper with Communication manager. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.	Asset-SW-01 Asset-SW-02 Asset-SW-03 Asset-SW-04
		Data flowing across send information for face detection may be tampered with by an attacker. This may lead to a denial of service attack against communication module or an elevation of privilege attack against communication module or an information disclosure by communication module. 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.	
		Data flowing across receive streaming data may be tampered with by an attacker. This may lead to a denial of service attack against Communication manager or an elevation of privilege attack against Communication manager or an information disclosure by Communication manager. 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.	
	Spoofing	Communication manager may be spoofed by an attacker and this may lead to unauthorized access to communication module. Consider using a standard authentication mechanism to identify the source process.	
		communication module may be spoofed by an attacker and this may lead to information disclosure by Communication manager. Consider using a standard authentication mechanism to identify the destination process.	
		communication module may be spoofed by an attacker and this may lead to unauthorized access to Communication manager. Consider using a standard authentication mechanism to identify the source process.	
		Communication manager may be spoofed by an attacker and this may lead to information disclosure by communication module. Consider using a standard authentication mechanism to identify the destination process.	
	Repudiation	Communication manager 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.	
		communication module 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.	

## 5.1 Threat modeling - STRIDE

Interaction Part	Category	Description	Asset No.
	Information Disclosure	Data flowing across receive streaming 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.	
		Data flowing across send information for face detection 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.	
	Elevation Of Privilege	An attacker may pass data into Communication manager in order to change the flow of program execution within Communication manager to the attacker's choosing.	
		communication module may be able to remotely execute code for Communication manager.	
		An attacker may pass data into communication module in order to change the flow of program execution within communication module to the attacker's choosing.	
		Communication manager may be able to remotely execute code for communication module.	
		Communication manager may be able to impersonate the context of communication module in order to gain additional privilege.	
		communication module may be able to impersonate the context of Communication manager in order to gain additional privilege.	
	Denial Of Service	An external agent interrupts data flowing across a trust boundary in either direction.	
		Communication manager crashes, halts, stops or runs slowly; in all cases violating an availability metric.	
		An external agent interrupts data flowing across a trust boundary in either direction.	
		communication module crashes, halts, stops or runs slowly; in all cases violating an availability metric.	

# 5.1 Threat modeling - STRIDE

Interaction Part	Category	Description	Asset No.
	Spoofing	Store DB may be spoofed by an attacker and this may lead to incorrect data delivered to Face Detection manager. Consider using a standard authentication mechanism to identify the source data store.	Asset-SW-02 Asset-SW-03
		Store DB may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Store DB. Consider using a standard authentication mechanism to identify the destination data store.	
	Information Disclosure	Improper data protection of Store DB can allow an attacker to read information not intended for disclosure. Review authorization settings.	
	Denial Of Service	Does service module or Store DB 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.	
	Spoofing	Store DB may be spoofed by an attacker and this may lead to incorrect data delivered to service module. Consider using a standard authentication mechanism to identify the source data store.	Asset-SW-01 Asset-SW-04
	Information Disclosure	Improper data protection of Store DB can allow an attacker to read information not intended for disclosure. Review authorization settings.	
	Denial Of Service	Does Face Detection manager or Store DB 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.	

Categorizing each risks according to the STRIDE and perform mitigation measure on them.

Risk ID	Condition	Threat Category	Mitigation method
RSK-01	Noise data from the network	Denial Of Service	Network size limitation - Protocol manager to analyze and respond to large network packet size attacks quickly and efficiently.
RSK-02	Replay attack for Network communication	Spoofing	Time stamp for Network packet - New time stamp for communication data
RSK-03	Data flow sniffing	Information Disclosure	TLS applies - TLS 1.3 with wolfSSL - After TLS session, all transmitted data becomes encrypted.
RSK-05	Face image and names stored in DB leaked	Tampering	TLS applies - TLS 1.3 with wolfSSL - After TLS session, all transmitted data becomes encrypted.
RSK-06	The network packet between the Jetson Nano board and the client pc is sniped	Tampering	TLS applies - TLS 1.3 with wolfSSL - After TLS session, all transmitted data becomes encrypted.
RSK-11	Saved DBs can be tampered with by hackers.	Tampering	Data encryption - AES_128_CBC - SHA_256
RSK-12	Normal user get administrator right (root privilege) and change the system.	Elevation Of Privilege	Minimum privileges for user - applying the minimum necessary privileges of file access to each user Close unused ports - Network ports should be blocked by default and only allowed if they are really needed for legitimate connections
RSK-13	Jetson Nano responds that it did not receive the data sent by the client.	Repudiation	Request and Response - Check the request and the appropriate response message - Re-request if there is no expected response
RSK-14	Attackers create so many connections that Jetson Nano cannot handle	Denial Of Service	Apply Firewall to Jetson Nano - Drop all connection except serviced port - Add DoS attack defences

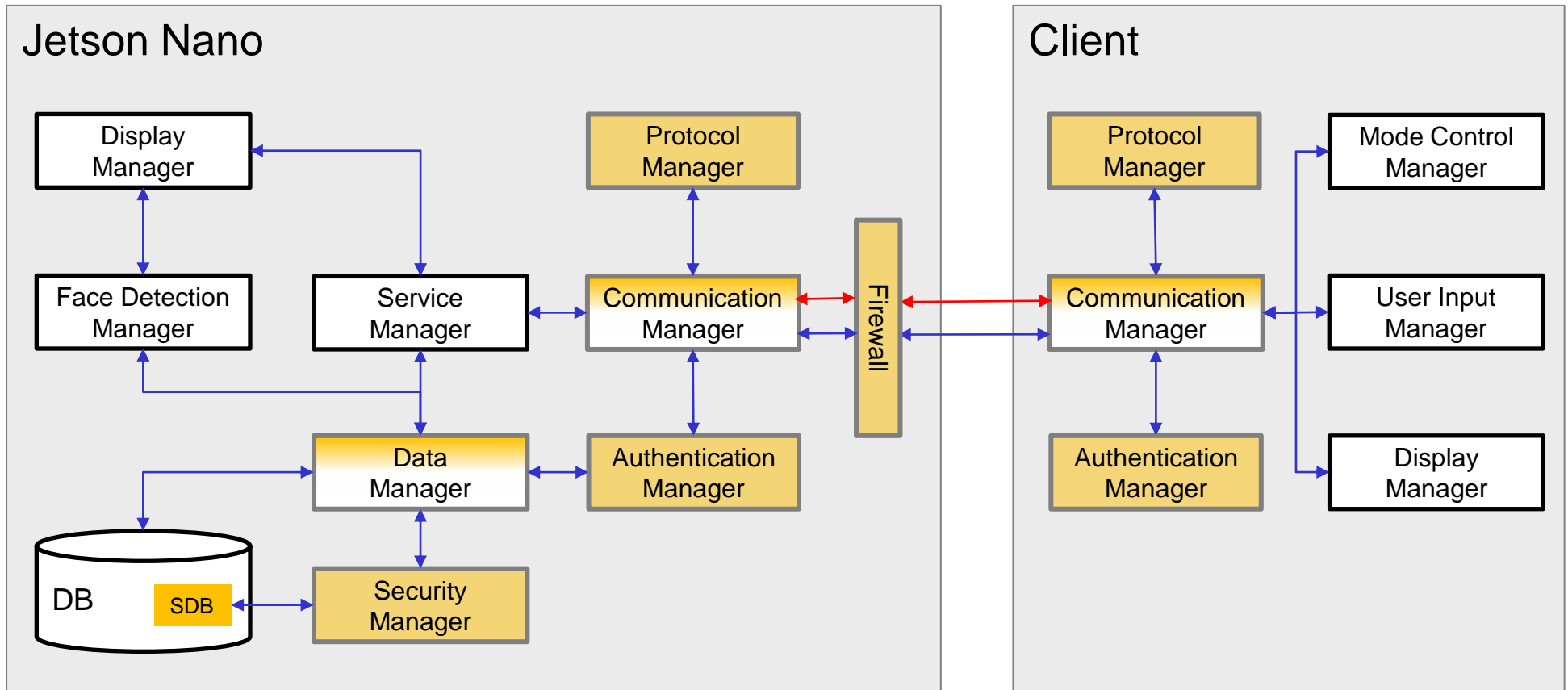
# 7. Security Requirements

Requirement ID	Descriptions	Related Risk ID
RQ-SEC-GEN-01	Authenticated communication should be implemented between server and client.	RSK-02 RSK-03 RSK-05 RSK-06 RSK-11
RQ-SEC-GEN-02	Secure mode should be implemented between server and client.	
RQ-SEC-GEN-03	In secure mode, all of data should be encrypted including time stamp.	
RQ-SEC-GEN-04	The server and the client must send and receive a request/response in the form of a message specified in the communication protocol.	
RQ-SEC-SVR-01	In learning mode, the name of the person in front of the camera and the number of images to be collected must be input and registered in the DB.	RSK-01 RSK-11
RQ-SEC-SVR-02	In learning mode, images must be saved according to the number of images given.	RSK-01 RSK-11
RQ-SEC-SVR-03	Test Run Mode should not allow files other than the given video files.	RSK-01 RSK-11
RQ-SEC-SVR-04	The server must only allow the authenticated user can access the system through the authentication process including user ID/PW.	RSK-03 RSK-06
RQ-SEC-SVR-05	The server should store the user's ID, password, and authority in the DB.	RSK-03 RSK-06 RSK-12
RQ-SEC-SVR-06	The server must close the socket when authentication fails.	RSK-02 RSK-03
RQ-SEC-SVR-07	When the server is connected to either the secure port or the non-secure port, the other port must be closed.	RSK-05 RSK-06 RSK-11
RQ-SEC-SVR-08	Only server administrator can change DB data of server.	RSK-12
RQ-SEC-SVR-09	The server must not be hang or crash due to an external DoS attack.	RSK-14
RQ-SEC-CLI-01	In learning mode, the client receives and transmits the number of images to be collected along with the user name.	RSK-01 RSK-11
RQ-SEC-CLI-02	The client should provide a UI to register the user ID/PW with the server.	RSK-03 RSK-06
RQ-SEC-CLI-03	The client must provide a UI to login to the server.	RSK-12



## Security-related quality attribute scenarios

QA ID	Category	QA Six parts	Description	Related Requirement
SEC-QA1	<b>Confidentiality</b>	Stimulus	Attempt to intercept packets between server and client	RQ-SEC-GEN-01 RQ-SEC-GEN-02 RQ-SEC-GEN-03
		Source	Attacker in the middle	
		Environment	Normal network communication between server & client	
		Artifact	All data include user ID/PW & image data	
		Response	Data encryption	
		Response measure	100% encrypted data When a tester capture the packet and check the contents, he should not be able to guess the contents of the packet at all.	
SEC-QA2	<b>Availability</b>	Stimulus	Disguise someone's identity with stolen credentials (ID/PW)	RQ-SEC-SVR-04
		Source	Attacker disguised as a normal user	
		Environment	Normal log in operation	
		Artifact	User data from server	
		Response	2-factor authentication	
		Response measure	Reject login attempts in case of 2-factor authentication failure Even if the password is stolen, the server must be able to verify that the accessor is a user with valid privileges. 2fa authorized users must be 100% loginable.	
SEC-QA3	<b>Integrity</b>	Stimulus	Attempt to change DB data of server	RQ-SEC-SVR-05 RQ-SEC-SVR-08
		Source	General user to gain administrator privileges	
		Environment	General user access	
		Artifact	All data in DB	
		Response	Prohibition of escalation of privileges from general user to administrator in the system	
		Response measure	Re-execution of administrator authentication procedure when accessing user DB	



— Secure channel



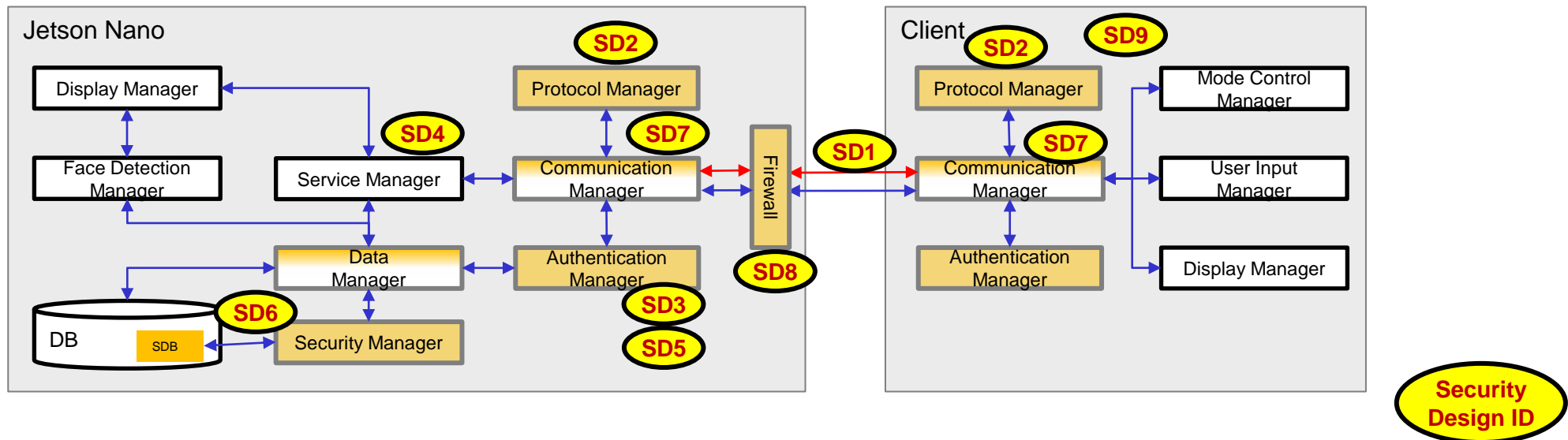
New Component



Modified Component

# 10. Security Design for Security Requirement

Security Design ID	Descriptions	Related Requirement ID
SD-01	Implementation of 'Secure mode' using TLS 1.3	RQ-SEC-GEN-02, RQ-SEC-GEN-03
SD-02	Implementation of 'Protocol Manager' module based on necessary data format	RQ-SEC-GEN-04
SD-03	Separation of administrator privilege to manage DB in learning mode	RQ-SEC-SVR-01, RQ-SEC-SVR-02 RQ-SEC-SVR-08
SD-04	Implemented a limited user operation	RQ-SEC-SVR-03, RQ-SEC-SVR-08
SD-05	Implementation of 'Authentication Manager' module based on authentication process	RQ-SEC-SVR-04
SD-06	Separation of 'Authentication Manager' domain to store credential data (user's ID/PW, authority)	RQ-SEC-SVR-05
SD-07	Modification of 'Communication Manager' to implement secure mode	RQ-SEC-SVR-06, RQ-SEC-SVR-07
SD-08	Apply Firewall	RQ-SEC-SVR-09
SD-09	UI design considering secure mode	RQ-SEC-CLI-01, RQ-SEC-CLI-02 RQ-SEC-CLI-03



## Apply TLS 1.3

- For the Secure Communication(All data encrypted between Server and Client)
- Provide mutual authentication through public key certificates
- Provide message integrity

## Design our own application protocol

- Server & Client only processing msg&data encapsulated by our own protocol
- Checking valid value & length each field for preventing tampering attack

## Add User Authentication

- ID/PW based
- User DB encrypted
- Prevent information disclosure

## Separate permissions based on user type

- Administrator only can run learning mode
- Face data encrypted & stored by SQL for preventing information disclosure

## Apply Firewall

- Block unauthorized connections
- Defense Dos Attack

# 11. Secure Coding Rule - CWE

Secure Jetson Nano project follows 'CWE' C code standards using 'flawfinder' tool

<https://cwe.mitre.org/data/definitions/699.html>



violation

son\_NanoV2/MTCNN\_FaceDetection\_TensorRT/src/mtcnn.cpp:113: [2] (buffer) memcpy:  
buffer overflows when copying to destination (CWE-120).  
Destination can always hold the source data.

```
resize(image(temp), secImage, Size(24, 24), 0, 0, cv::INTER_LINEAR);  
transpose(secImage, secImage);  
refineNet->run(secImage, *rnet_engine);  
if(*(refineNet->score_>pdata+1) > refineNet->Rthreshold){  
    if(sizeof(mydataFmt) < 0) return;  
    memcpy(it->regCoord, refineNet->regCoord, sizeof(mydataFmt));  
    it->area = (it->x2 - it->x1) * (it->y2 - it->y1);  
    it->score = *(refineNet->score_>pdata);  
}
```



modification

## Verification of Secure Coding using 'flawfinder' tool

### Server

```
Jetson_NanoV2/MTCNN_FaceDetection_TensorRT/src/mtcnn.cpp:113: [2] (buffer) memcpy:
Does not check for buffer overflows when copying to destination (CWE-120).
Make sure destination can always hold the source data.
Jetson_NanoV2/MTCNN_FaceDetection_TensorRT/src/mtcnn.cpp:145: [2] (buffer) memcpy:
Does not check for buffer overflows when copying to destination (CWE-120).
Make sure destination can always hold the source data.
./LgFaceRecDemoTCP_Jetson_NanoV2/MTCNN_FaceDetection_TensorRT/src/pnet_rt.cpp:24: [2] (misc) open:
Check when opening files - can an attacker redirect it (via symlinks),
force the opening of special file type (e.g., device files), move things
around to create a race condition, control its ancestors, or change its
contents? (CWE-362).
./LgFaceRecDemoTCP_Jetson_NanoV2/MTCNN_FaceDetection_TensorRT/src/pnet_rt.cpp:40: [2] (misc) open:
Check when opening files - can an attacker redirect it (via symlinks),
force the opening of special file type (e.g., device files), move things
around to create a race condition, control its ancestors, or change its
contents? (CWE-362).
./LgFaceRecDemoTCP_Jetson_NanoV2/src/NetworkTCP.cpp:560: [2] (buffer) memcpy:
Does not check for buffer overflows when copying to destination (CWE-120).
Make sure destination can always hold the source data.
./LgFaceRecDemoTCP_Jetson_NanoV2/src/NetworkTCP.cpp:600: [2] (buffer) memcpy:
Does not check for buffer overflows when copying to destination (CWE-120).
Make sure destination can always hold the source data.
./LgFaceRecDemoTCP_Jetson_NanoV2/src/UdpSendRecvJpeg.cpp:37: [2] (buffer) char:
Statically-sized arrays can be improperly restricted, leading to potential
overflows or other issues (CWE-119/CWE-120). Perform bounds checking, use
functions that limit length, or ensure that the size is larger than the
maximum possible length.
./LgFaceRecDemoTCP_Jetson_NanoV2/src/baseEngine.cpp:92: [2] (misc) open:
Check when opening files - can an attacker redirect it (via symlinks),
force the opening of special file type (e.g., device files), move things
around to create a race condition, control its ancestors, or change its
contents? (CWE-362).
./LgFaceRecDemoTCP_Jetson_NanoV2/src/cyber.cpp:10: [2] (buffer) char:
Statically-sized arrays can be improperly restricted, leading to potential
overflows or other issues (CWE-119/CWE-120). Perform bounds checking, use
functions that limit length, or ensure that the size is larger than the
maximum possible length.
./LgFaceRecDemoTCP_Jetson_NanoV2/src/cyber.cpp:11: [2] (buffer) char:
Statically-sized arrays can be improperly restricted, leading to potential
overflows or other issues (CWE-119/CWE-120). Perform bounds checking, use
functions that limit length, or ensure that the size is larger than the
maximum possible length.
./LgFaceRecDemoTCP_Jetson_NanoV2/src/cyber.cpp:49: [2] (buffer) char:
Statically-sized arrays can be improperly restricted, leading to potential
overflows or other issues (CWE-119/CWE-120). Perform bounds checking, use
functions that limit length, or ensure that the size is larger than the
maximum possible length.
./LgFaceRecDemoTCP_Jetson_NanoV2/src/cyber.cpp:56: [2] (buffer) char:
Statically-sized arrays can be improperly restricted, leading to potential
overflows or other issues (CWE-119/CWE-120). Perform bounds checking, use
functions that limit length, or ensure that the size is larger than the
```

### Client

```
Common/SG_InputBox.cpp:52: [4] (buffer) strcpy:
Does not check for buffer overflows when copying to destination [MS-banned]
(CWE-120). Consider using a function version that stops copying at the end
of the buffer.
./MFCApplication1/Common/NetworkTCP.cpp:602: [2] (buffer) memcpy:
Does not check for buffer overflows when copying to destination (CWE-120).
Make sure destination can always hold the source data.
./MFCApplication1/Common/NetworkTCP.cpp:651: [2] (buffer) memcpy:
Does not check for buffer overflows when copying to destination (CWE-120).
Make sure destination can always hold the source data.
./MFCApplication1/Common/Protocol/Msg/protocolLogin.pb.cc:2059: [2] (buffer) memcpy:
Does not check for buffer overflows when copying to destination (CWE-120).
Make sure destination can always hold the source data.
./MFCApplication1/Common/Protocol/ProtocolManager.cpp:53: [2] (buffer) memcpy:
Does not check for buffer overflows when copying to destination (CWE-120).
Make sure destination can always hold the source data.
./MFCApplication1/Common/SG_InputBox.h:36: [2] (buffer) wchar_t:
Statically-sized arrays can be improperly restricted, leading to potential
overflows or other issues (CWE-119/CWE-120). Perform bounds checking, use
functions that limit length, or ensure that the size is larger than the
maximum possible length.
./MFCApplication1/Common/SG_InputBox.h:50: [2] (buffer) wchar_t:
Statically-sized arrays can be improperly restricted, leading to potential
overflows or other issues (CWE-119/CWE-120). Perform bounds checking, use
functions that limit length, or ensure that the size is larger than the
maximum possible length.
./MFCApplication1/Common/UdpSendRecvJpeg.cpp:38: [2] (buffer) char:
Statically-sized arrays can be improperly restricted, leading to potential
overflows or other issues (CWE-119/CWE-120). Perform bounds checking, use
functions that limit length, or ensure that the size is larger than the
maximum possible length.
./MFCApplication1/ProtocolDef.h:59: [2] (buffer) char:
Statically-sized arrays can be improperly restricted, leading to potential
overflows or other issues (CWE-119/CWE-120). Perform bounds checking, use
functions that limit length, or ensure that the size is larger than the
maximum possible length.
./MFCApplication1/ProtocolDef.h:67: [2] (buffer) char:
Statically-sized arrays can be improperly restricted, leading to potential
overflows or other issues (CWE-119/CWE-120). Perform bounds checking, use
functions that limit length, or ensure that the size is larger than the
maximum possible length.
```



## Static Analysis using 'cppcheck' tool

### Server

```
(portability) %zu in format string (no. 2) requires 'size_t' but the argument type is 'ssize_t (aka signed long)'.
(portability) %zu in format string (no. 1) requires 'size_t' but the argument type is 'ssize_t (aka signed long)'.
[Common/NetworkTCP.cpp:601]: (portability) %zu in format string (no. 2) requires 'size_t' but the argument type is 'ssize_t (aka signed long)'.
[Common/NetworkTCP.cpp:616]: (style) The scope of the variable 'bytes_written' can be reduced.
[Common/NetworkTCP.cpp:633]: (style) The scope of the variable 'bytes_written' can be reduced.
Checking Common/NetworkTCP.cpp: _WIN32;_WIN64...
3/49 files checked 6% done
Checking Common/NetworkUDP.cpp ...
Checking Common/NetworkUDP.cpp: _WIN32;_WIN64...
4/49 files checked 8% done
Checking Common/Protocol/BaseProtocol.cpp ...
5/49 files checked 10% done
Checking Common/Protocol/MyProtocol.cpp ...
[Common/Protocol/MyProtocol.h:46]: (style) Class 'CControlModeProtocol' has a constructor with 1 argument that is not explicit.
[Common/Protocol/MyProtocol.h:56]: (style) Class 'CServerSettingProtocol' has a constructor with 1 argument that is not explicit.
[Common/Protocol/MyProtocol.h:70]: (style) Class 'CVideoFileListProtocol' has a constructor with 1 argument that is not explicit.
[Common/Protocol/MyProtocol.h:82]: (style) Class 'CTestMode_PlayVideoProtocol' has a constructor with 1 argument that is not explicit.
[Common/Protocol/MyProtocol.cpp:12]: (performance) Function parameter 'id' should be passed by reference.
[Common/Protocol/MyProtocol.cpp:12]: (performance) Function parameter 'pw' should be passed by reference.
[Common/Protocol/MyProtocol.cpp:18]: (performance) Function parameter 'id' should be passed by reference.
[Common/Protocol/MyProtocol.cpp:22]: (performance) Function parameter 'password' should be passed by reference.
6/49 files checked 12% done
Checking Common/Protocol/ProtocolManager.cpp ...
[Common/Protocol/ProtocolManager.cpp:60]: (warning) %d in format string (no. 1) requires 'int' but the argument type is 'unsigned int'.
[Common/Protocol/ProtocolManager.cpp:61]: (portability) %zd in format string (no. 1) requires 'ssize_t' but the argument type is 'size_t (aka unsigned int)'.
[Common/Protocol/ProtocolManager.cpp:70]: (warning) %d in format string (no. 1) requires 'int' but the argument type is 'unsigned int'.
[Common/Protocol/ProtocolManager.cpp:73]: (warning) %d in format string (no. 1) requires 'int' but the argument type is 'unsigned int'.
[Common/Protocol/ProtocolManager.cpp:74]: (warning) %d in format string (no. 1) requires 'int' but the argument type is 'unsigned int'.
[Common/Protocol/MyProtocol.h:18]: (performance) Function parameter 'id' should be passed by reference.
[Common/Protocol/MyProtocol.h:18]: (performance) Function parameter 'pw' should be passed by reference.
[Common/Protocol/MyProtocol.h:19]: (performance) Function parameter 'id' should be passed by reference.
[Common/Protocol/MyProtocol.h:20]: (performance) Function parameter 'password' should be passed by reference.
7/49 files checked 14% done
Checking Common/SG_InputBox.cpp ...
8/49 files checked 16% done
Checking Common/TcpSendRecvJpeg.cpp ...
[Common/TcpSendRecvJpeg.cpp:83]: (style) Checking if unsigned variable 'imagesize' is less than zero.
[Common/TcpSendRecvJpeg.cpp:107]: (style) Checking if unsigned variable 'imagesize' is less than zero.
Checking Common/TcpSendRecvJpeg.cpp: _WIN32;_WIN64...
9/49 files checked 18% done
Checking Common/UdpSendRecvJpeg.cpp ...
Checking Common/UdpSendRecvJpeg.cpp: _WIN32;_WIN64...
10/49 files checked 20% done
Checking Common/Utils.cpp ...
11/49 files checked 22% done
Checking LgFaceRecDemoTCP_Jetson_NanoV2/MTCNN_FaceDetection_TensorRT/src/baseEngine.cpp ...
[LgFaceRecDemoTCP_Jetson_NanoV2/MTCNN_FaceDetection_TensorRT/src/baseEngine.cpp:6]: (warning) Member variable 'baseEngine::context' is
12/49 files checked 24% done
Checking LgFaceRecDemoTCP_Jetson_NanoV2/MTCNN_FaceDetection_TensorRT/src/common.cpp ...
13/49 files checked 26% done
```

### Client

```
<?xml v
<results
<cp
- <errors>
- <error sinceDate="2021-06-17" cwe="758" verbose="Returning an integer (int/long/etc) in a function with pointer return type is not portable
across different platforms and compilers. For example in 32-bit Windows and Linux they are same width, but in 64-bit Windows and Linux
they are of different width. In worst case you end up casting 64-bit integer down to 32-bit pointer. The safe way is to always return a
pointer." msg="Returning an integer in a function with pointer return type is not portable." severity="portability"
id="CastIntegerToAddressAtReturn">
<location line="124" file="..\..\..\opencv\build\include\opencv2\core\cvstd_wrapper.hpp"
file0="Git/LGSecurity/MFCAApplication1/Common/NetworkManager.cpp"/>
</error>
- <error sinceDate="2021-06-17" cwe="398" verbose="Struct &#039;Ptr &lt; Impl &gt;&#039; has a constructor with 1 argument that is not
explicit. Such constructors should in general be explicit for type safety reasons. Using the explicit keyword in the constructor means some
mistakes when using the class can be avoided." msg="Struct &#039;Ptr &lt; Impl &gt;&#039; has a constructor with 1 argument that is not
explicit." severity="style" id="noExplicitConstructor">
<location line="79" file="..\..\..\opencv\build\include\opencv2\core\cvstd_wrapper.hpp"
file0="Git/LGSecurity/MFCAApplication1/Common/NetworkManager.cpp"/>
</error>
- <error sinceDate="2021-06-17" cwe="398" verbose="Struct &#039;Ptr &lt; Impl &gt;&#039; has a constructor with 1 argument that is not
explicit. Such constructors should in general be explicit for type safety reasons. Using the explicit keyword in the constructor means some
mistakes when using the class can be avoided." msg="Struct &#039;Ptr &lt; Impl &gt;&#039; has a constructor with 1 argument that is not
explicit." severity="style" id="noExplicitConstructor">
<location line="88" file="..\..\..\opencv\build\include\opencv2\core\cvstd_wrapper.hpp"
file0="Git/LGSecurity/MFCAApplication1/Common/NetworkManager.cpp"/>
</error>
- <error sinceDate="2021-06-17" cwe="398" verbose="Struct &#039;Ptr &lt; Impl &gt;&#039; has a constructor with 1 argument that is not
explicit. Such constructors should in general be explicit for type safety reasons. Using the explicit keyword in the constructor means some
mistakes when using the class can be avoided." msg="Struct &#039;Ptr &lt; Impl &gt;&#039; has a constructor with 1 argument that is not
explicit." severity="style" id="noExplicitConstructor">
<location line="89" file="..\..\..\opencv\build\include\opencv2\core\cvstd_wrapper.hpp"
file0="Git/LGSecurity/MFCAApplication1/Common/NetworkManager.cpp"/>
</error>
- <error sinceDate="2021-06-17" cwe="398" verbose="Struct &#039;Ptr &lt; Impl &gt;&#039; has a constructor with 1 argument that is not
explicit. Such constructors should in general be explicit for type safety reasons. Using the explicit keyword in the constructor means some
mistakes when using the class can be avoided." msg="Struct &#039;Ptr &lt; Impl &gt;&#039; has a constructor with 1 argument that is not
explicit." severity="style" id="noExplicitConstructor">
<location line="91" file="..\..\..\opencv\build\include\opencv2\core\cvstd_wrapper.hpp"
file0="Git/LGSecurity/MFCAApplication1/Common/NetworkManager.cpp"/>
</error>
- <error sinceDate="2021-06-17" cwe="398" verbose="Struct &#039;Ptr &lt; Impl &gt;&#039; has a constructor with 1 argument that is not
explicit. Such constructors should in general be explicit for type safety reasons. Using the explicit keyword in the constructor means some
mistakes when using the class can be avoided." msg="Struct &#039;Ptr &lt; Impl &gt;&#039; has a constructor with 1 argument that is not
explicit." severity="style" id="noExplicitConstructor">
<location line="92" file="..\..\..\opencv\build\include\opencv2\core\cvstd_wrapper.hpp"
file0="Git/LGSecurity/MFCAApplication1/Common/NetworkManager.cpp"/>
</error>
- <error sinceDate="2021-06-17" cwe="398" verbose="Struct &#039;Ptr &lt; Impl &gt;&#039; has a constructor with 1 argument that is not
explicit. Such constructors should in general be explicit for type safety reasons. Using the explicit keyword in the constructor means some
mistakes when using the class can be avoided." msg="Struct &#039;Ptr &lt; Impl &gt;&#039; has a constructor with 1 argument that is not
explicit." severity="style" id="noExplicitConstructor">
<location line="103" file="..\..\..\opencv\build\include\opencv2\core\cvstd_wrapper.hpp"
file0="Git/LGSecurity/MFCAApplication1/Common/NetworkManager.cpp"/>
</error>
```

## Design 24 testcases & Run test

➤ Result : 24 Pass, 0 Fail (<https://drive.google.com/file/d/1avvoxG8JM5V3aDeXzDjdWqXfNR5TAA3E/view?usp=sharing>)

No	Module	Function	Category	Precondition	Procedure	Expected Result	Result	Comments
1	Client	Input validation	id	1. run program	1. input long length string 2. enter special characters	1. cannot enter more than 10 characters. (alphabet, numbers only)	pass	
2	Client	Input validation	password	1. run program	1. input long length string 2. enter special characters	1. cannot enter more than 10 characters. (alphabet, numbers only)	pass	
3	Client	Operate either secure or non-secure mode	mode	1. run program	1. select either secure or non-secure mode	1. only one mode can be selected	pass	
4	Client	Try log in with registered ID	log in	1. run program	1. input registered id	1. success to log in	pass	
5	Client	Try log in with unregistered ID	log in	1. run program	1. input unregistered id	1. fail to log in	pass	
6	Client	Select operation mode with administrator privilege	operation mode	1. run program2. log in	1. log in with administrator privileges	1. can select one of three mode	pass	
7	Client	Select operation mode with user privileges	operation mode	1. run program2. log in	1. log in with user privileges	1. can select either Run or Test Run	pass	
8	Client	Select operation mode	operation mode	1. run program2. log in	1. log in2. can push Apply button	1. enable Apply button 2. when selected, the label is changed to stop	pass	
9	Client	Stop operation mode	operation mode	1. run program2. log in3. Op	1. log in2. Operation mode has been select	1. enable Stop button 2. when selected, the label is changed to Apply	pass	
10	Client	Operation mode stop	operation mode	1. run program2. log in	1. log in with user privileges	1. can select either Run or Test Run	pass	

## Testing example

20 0.000412	192.168.0.223	192.168.0.228	TCP	1514 50000 → 4501 [ACK] Seq=21901 Ack=1 Win=229 Len=1460 [TCP segment of a reassembled PDU]
21 0.000412	192.168.0.223	192.168.0.228	TCP	1514 50000 → 4501 [ACK] Seq=23361 Ack=1 Win=229 Len=1460 [TCP segment of a reassembled PDU]
22 0.000412	192.168.0.223	192.168.0.228	TCP	1514 50000 → 4501 [ACK] Seq=24821 Ack=1 Win=229 Len=1460 [TCP segment of a reassembled PDU]
23 0.000412	192.168.0.223	192.168.0.228	TCP	1514 50000 → 4501 [ACK] Seq=26281 Ack=1 Win=229 Len=1460 [TCP segment of a reassembled PDU]

```

00022910 60 2A 18 C1 18 61 8A 63 44 47 D2 AE 99 D4 9E 82  *.Ã.ašcDGOöZ,
00022920 94 48 08 FB A2 85 27 B8 59 1F FF D9 53 42 31 54  "H.öc...'.Y.yÜSBlT
00022930 24 8A 00 01 29 A2 66 19 EA 03 00 00 08 8C 94 02  Š.)öf.e...ö".
00022940 12 8C 94 01 FF D8 FF E0 00 10 4A 46 49 46 00 01  .ö".yöyö..JFIF..
00022950 01 00 00 00 00 01 00 00 FF DB 00 43 00 06 04 05  .....yÜ.C.....
00022960 06 05 04 06 06 05 06 07 07 06 08 0A 10 0A 0A 09  .....yÜ.C.....

```

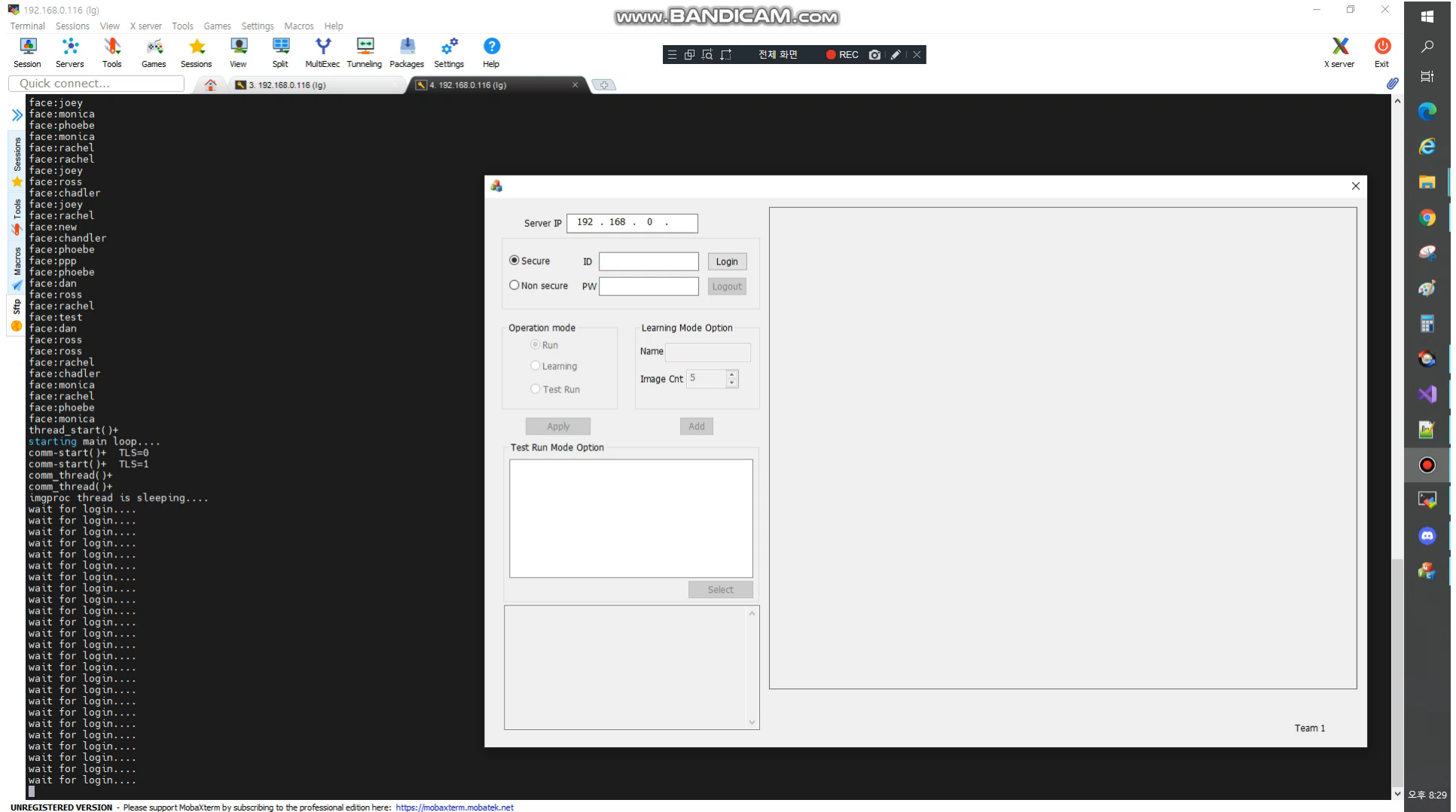


25727 44.761632	192.168.0.223	192.168.0.228	TCP	60 55555 → 10004 [ACK] Seq=1200 Ack=345 Win=30336 Len=0
25728 44.761632	192.168.0.223	192.168.0.228	TLSv1.3	236 Application Data
25730 44.775070	192.168.0.228	192.168.0.223	TLSv1.3	104 Application Data
25733 44.818018	192.168.0.223	192.168.0.228	TCP	60 55555 → 10004 [ACK] Seq=1390 Ack=395 Win=30336 Len=0
25756 46.599628	192.168.0.223	192.168.0.228	TLSv1.3	94 Application Data
25762 46.641462	192.168.0.228	192.168.0.223	TCP	54 10004 → 55555 [ACK] Seq=395 Ack=1430 Win=20336 Len=0
25796 50.595352	192.168.0.228	192.168.0.223	TLSv1.3	92 Application Data
25797 50.597173	192.168.0.223	192.168.0.228	TCP	60 55555 → 10004 [ACK] Seq=1430 Ack=433 Win=30336 Len=0
25801 51.597784	192.168.0.223	192.168.0.228	TLSv1.3	92 Application Data
25806 51.645465	192.168.0.228	192.168.0.223	TCP	54 10004 → 55555 [ACK] Seq=433 Ack=1468 Win=204800 Len=0
25812 51.719659	192.168.0.223	192.168.0.228	TCP	1514 55555 → 10004 [ACK] Seq=1468 Ack=433 Win=30336 Len=1460 [TCP segment of a reassembled PDU]

Connection is not secure in **Non-Secure mode**  
Attacker is able to get JPG in the middle

Connection is protect by TLS 1.3 in **Secure mode**  
Attacker can't get JPG in the middle





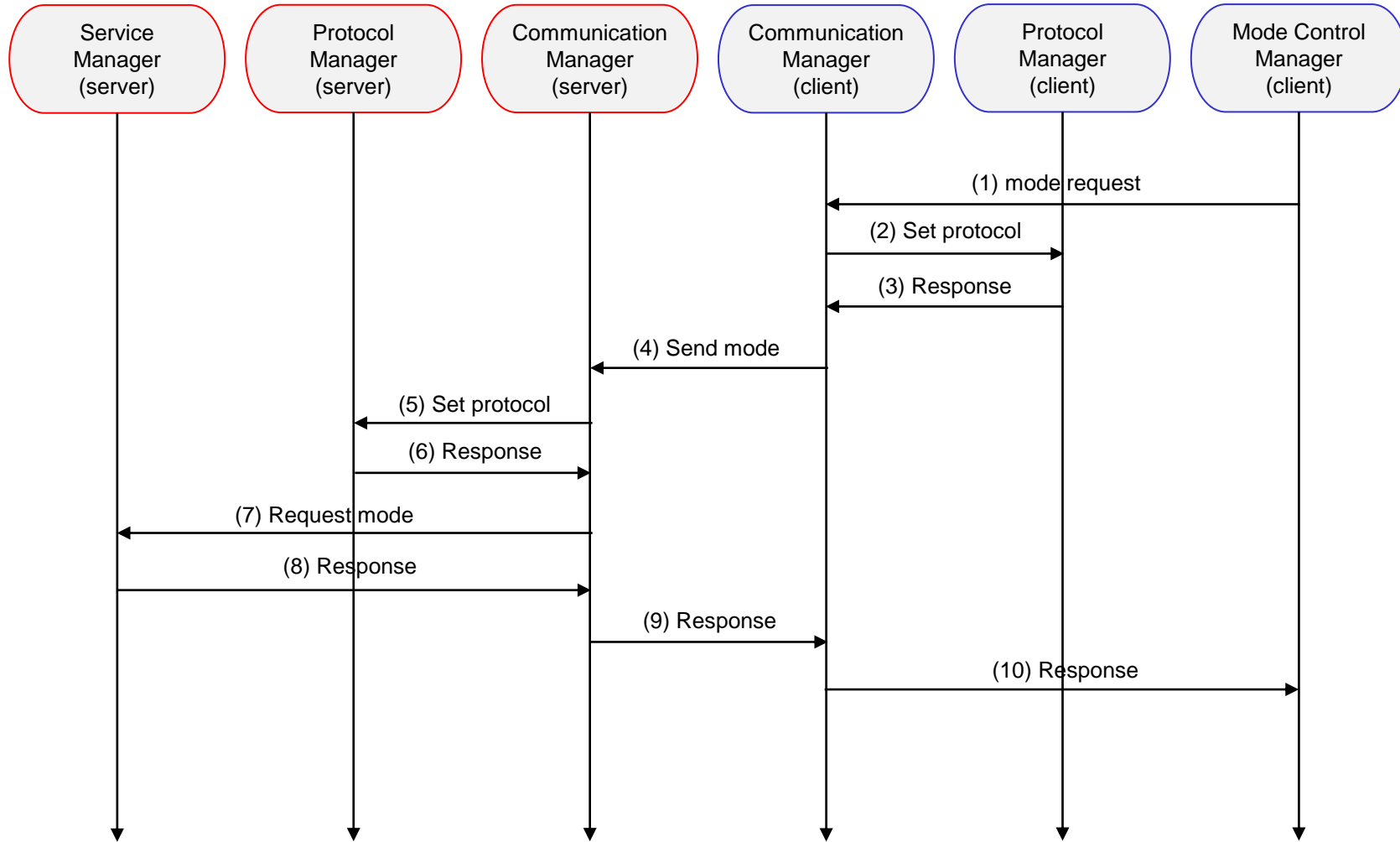
Lesson	Activities	Learned
Asset Identification	Identifying assets <ul style="list-style-type: none"> <li>➤ Things attackers want</li> <li>➤ Things you want to protect</li> <li>➤ Stepping stones to either of these</li> </ul>	Good: Knowing the assets that actually need to be protected can make an effort to constantly improve the quality of developments.
Security Risk Assessment	Brainstorming Security Risk and Rating 3 points of view <ul style="list-style-type: none"> <li>➤ Sniffing data flow</li> <li>➤ Attack network communication</li> <li>➤ Tampering DB data</li> </ul>	Good: Listing the different scenarios of risk can have makes it clear what tasks need to be done Bad: Difficult to define exact criteria for scoring
Threat Analysis	Analysis threat using MS Threat modeling tool <ul style="list-style-type: none"> <li>➤ Drawing DFD</li> <li>➤ Define Trust boundaries</li> <li>➤ Categorizing threats with STRIDE</li> </ul>	Good: The vague risk becomes clear through the tool Bad: Difficult to define exact criteria for scoring
Mitigation Threats	Establishing Threat Mitigation Plans <ul style="list-style-type: none"> <li>➤ Relay attack – add New time stamp</li> <li>➤ Sniffing Data flow → TLS 1.3 with wolfSSL</li> <li>➤ Tampered DBs → AES_128_CBC data encryption</li> <li>➤ Elevation of Root privilege → minimum privileges for user</li> <li>➤ Attacking many connections → Drop all except serviced port</li> </ul>	Good: Possible to investigate various threat mitigation measures. Bad: Many of the mitigation measures initially determined were not implemented due to time reasons.
Security Requirements & Quality Attributes	Describe new security requirements and considering QA <ul style="list-style-type: none"> <li>➤ Confidentiality</li> <li>➤ Integrity</li> <li>➤ Availability</li> </ul>	Good: Can guarantee security requirement with confidentiality, integrity, availability through Quality attribute process Bad: The boundary between requirements and QA was ambiguous, so it was not possible to accurately distinguish them.
Secure Coding & Static Analysis	Reviewing c++ code standard and selecting tool <ul style="list-style-type: none"> <li>➤ OWASP</li> <li>➤ CERT</li> <li>➤ CWE</li> <li>➤ Misra-c</li> </ul> selecting tool <ul style="list-style-type: none"> <li>➤ flawfinder</li> <li>➤ cppcheck</li> </ul>	Good: Being able to look at and review the standards of secure coding Bad: Difficult to apply the tool to the ARM-based device system. Not spending more time on static analysis

# Appendix

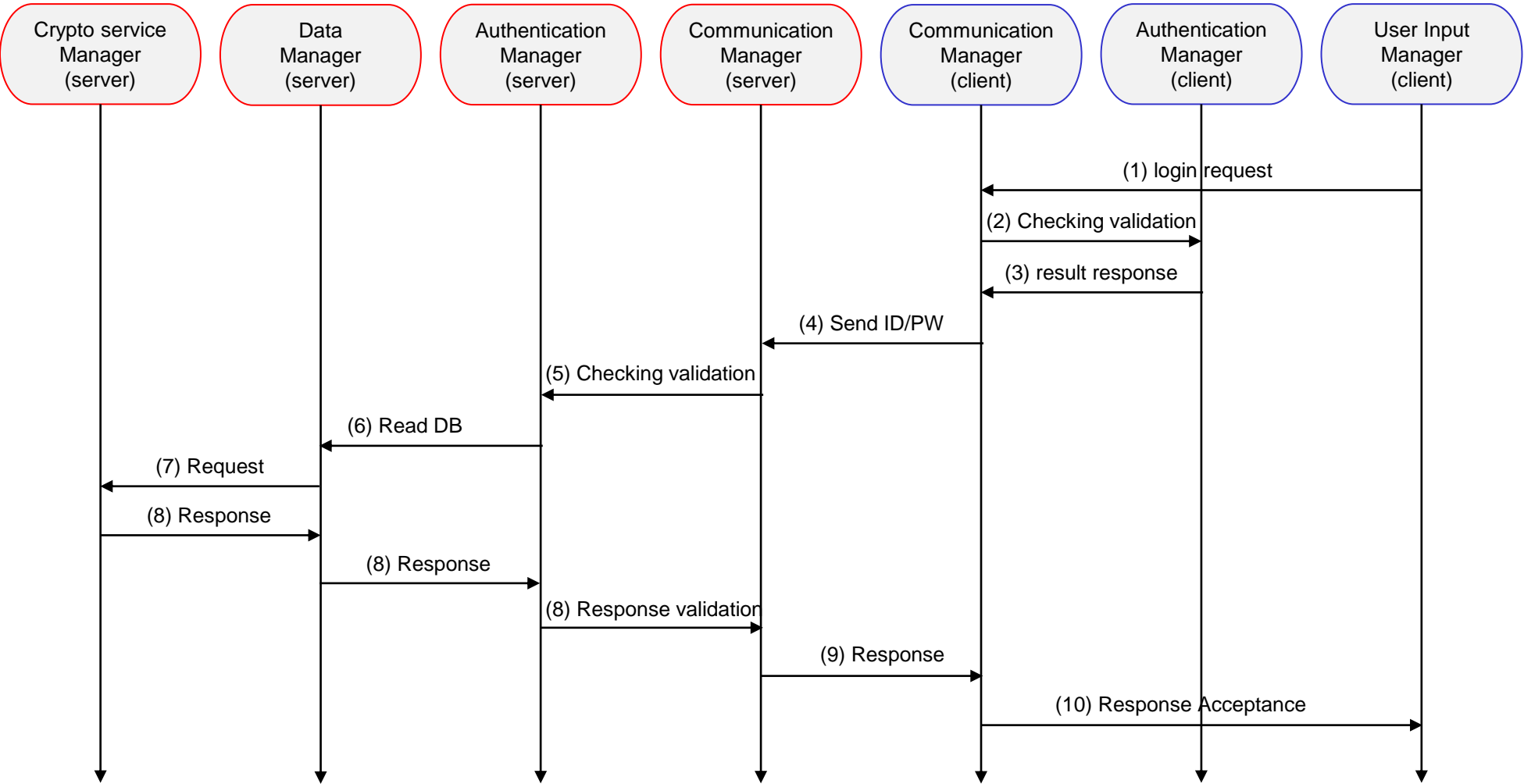
# Secure system Sequence Diagram #1



## Case #1 set secure mode



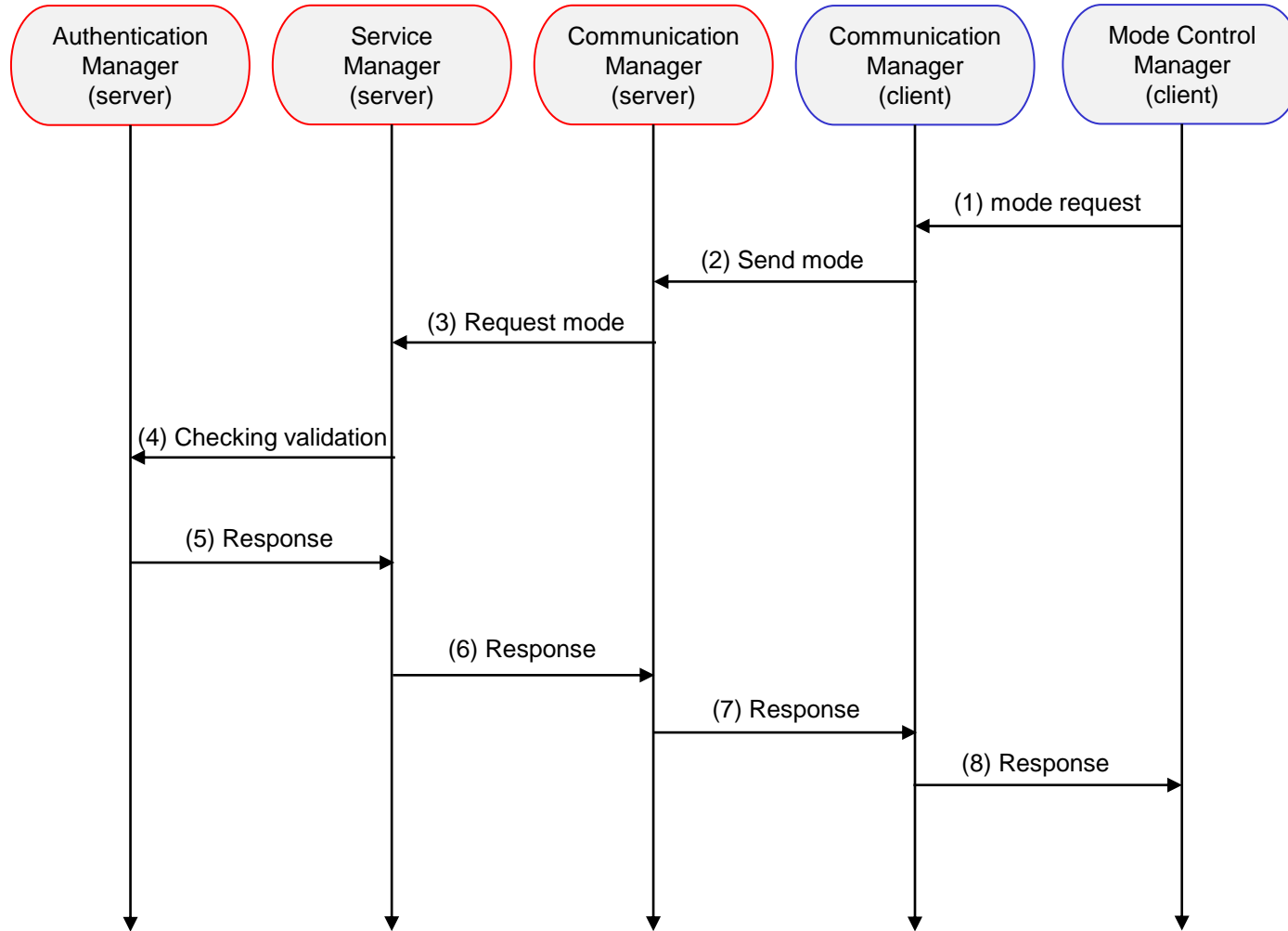
Case #2 login process in secure mode



# Secure system Sequence Diagram #3



Case #3 mode selection in secure mode



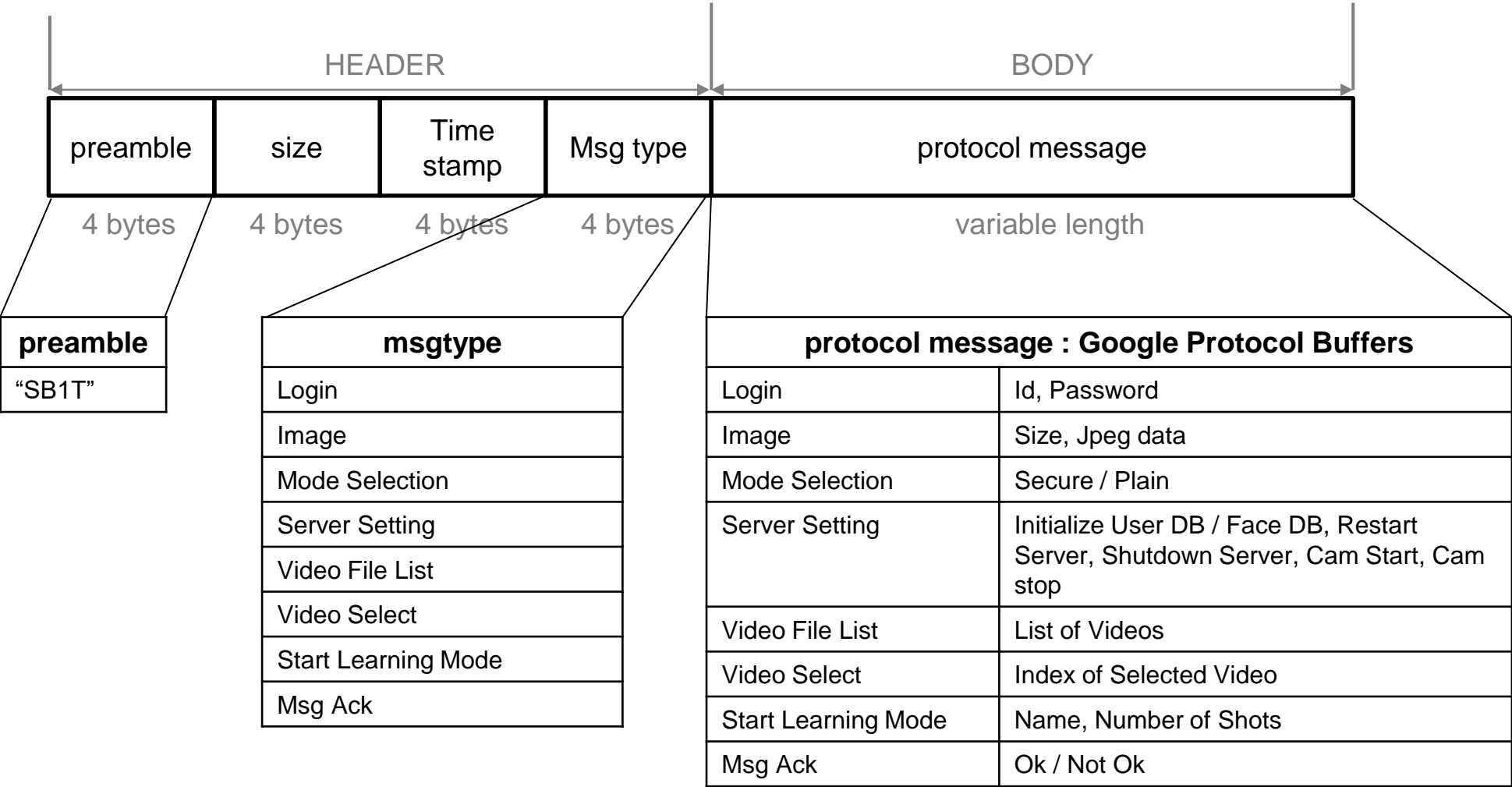
No.	Requirement	Requirement No.
SD-01	Implementation of 'Secure mode' using TLS 1.3	RQ-SEC-GEN-02 RQ-SEC-GEN-03

	Design	Remark
Library	Use wolfSSL 4.7.1	* More useful in embedded ssl implementations (small, fast) * vulnerability free version ( <a href="https://www.wolfssl.com/docs/security-vulnerabilities/">https://www.wolfssl.com/docs/security-vulnerabilities/</a> )
TLS version	Only support 1.3	* Weak cipher suites have been removed * All handshake messages after the ServerHello are now encrypted -> More Secure than prior version
Certificate	Generate Root-CA Certification, Server Certification	ECDSA prime256v1
Cipher suite	Only use TLS 1.3 Cipher suite	TLS_AES_256_GCM_SHA384. TLS_CHACHA20_POLY1305_SHA256. TLS_AES_128_GCM_SHA256. TLS_AES_128_CCM_8_SHA256. TLS_AES_128_CCM_SHA256.

Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number:  
39:51:16:c1:3c:d5:3b:5c:04:77:64:1e:7b:a7:24:c7:90:dc:8e  
Signature Algorithm: ecdsa-with-SHA256  
Issuer: C=KR, ST=Seoul, O=LG Electronics, OU=CMU, CN=root-ca.sinbak  
Validity  
Not Before: Jun 10 06:16:33 2021 GMT  
Not After : Jun 10 06:16:33 2022 GMT  
Subject: C=KR, ST=Seoul, O=LG Electronics, OU=CMU, CN=team1  
Subject Public Key Info:  
Public Key Algorithm: id-ecPublicKey  
Public-Key: (256 bit)  
pub:  
04:68:c7:38:f6:e6:be:31:2b:ec:60:a7:f8:4d:d9:  
3f:6e:c3:30:35:97:a0:82:13:6d:92:d0:64:09:a3:  
45:6b:d8:1e:12:79:0d:d6:aa:f8:a5:c9:cc:b9:ee:  
c6:90:f4:33:70:ca:13:d5:50:2b:5e:c2:4e:2c:8a:  
3d:71:00:9c:3a  
ASN1 OID: prime256v1  
NIST CURVE: P-256  
X509v3 extensions:  
X509v3 Basic Constraints:  
CA:FALSE  
X509v3 Subject Key Identifier:  
A1:D4:70:04:A5:98:E5:E3:21:4F:2C:A9:E0:44:F0:CC:9C:21:2D:18  
X509v3 Authority Key Identifier:  
keyid:71:97:DF:C3:AF:40:16:2E:DA:4B:47:43:16:5C:7D:96:56:B3:10:AC  
DirName:/C=KR/ST=Seoul/O=LG Electronics/OU=CMU/CN=root-ca.sinbak  
serial:7D:0E:40:64:43:D7:28:C0:55:B9:90:6C:08:B7:32:6C:98:62:0F:29  
  
X509v3 Key Usage:  
Digital Signature, Non Repudiation, Key Encipherment  
X509v3 Extended Key Usage:  
TLS Web Server Authentication, TLS Web Client Authentication  
X509v3 Subject Alternative Name:  
DNS:team1  
Authority Information Access:  
CA Issuers - URI:<http://root-ca.sinbak/root-ca.crt>  
OCSP - URI:<http://ocsp.sinbak:8080>  
  
Netscape CA Revocation Url:  
<http://root-ca.sinbak/revoked.crl>  
Signature Algorithm: ecdsa-with-SHA256  
30:45:02:21:00:9b:7b:1c:a2:8e:f9:15:bd:f5:bd:4f:a6:df:  
7c:a9:ba:52:f9:2b:d7:7c:10:13:af:d2:16:7d:6c:dd:96:12:  
ba:02:20:16:da:15:9b:05:64:23:a6:aa:b5:2b:18:cf:6f:ac:  
6b:6a:59:04:10:98:03:b5:42:d7:cd:c1:da:cf:56:61:55



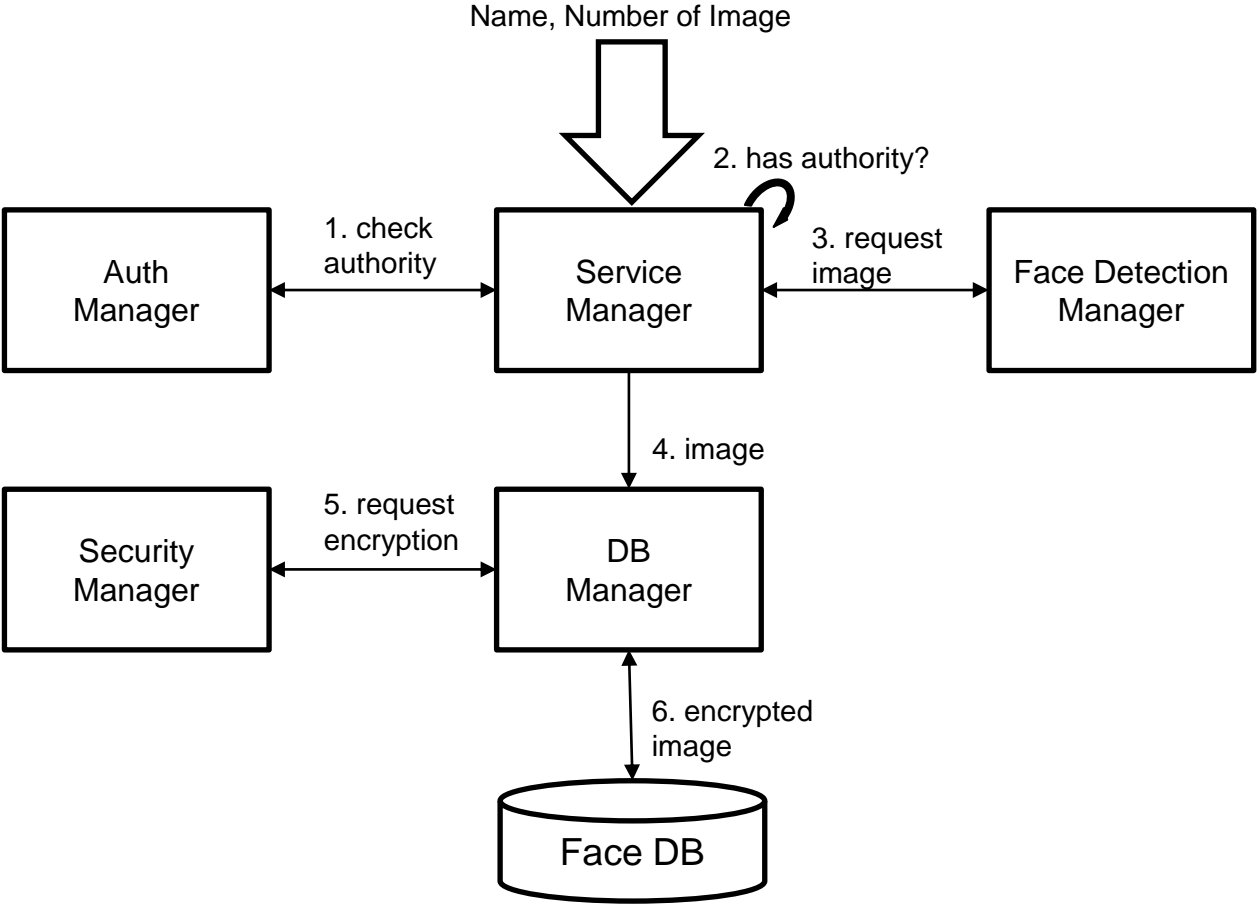
No.	Requirement	Requirement No.
SD-02	Implementation of 'Protocol Manager' module based on necessary data format	RQ-SEC-GEN-04





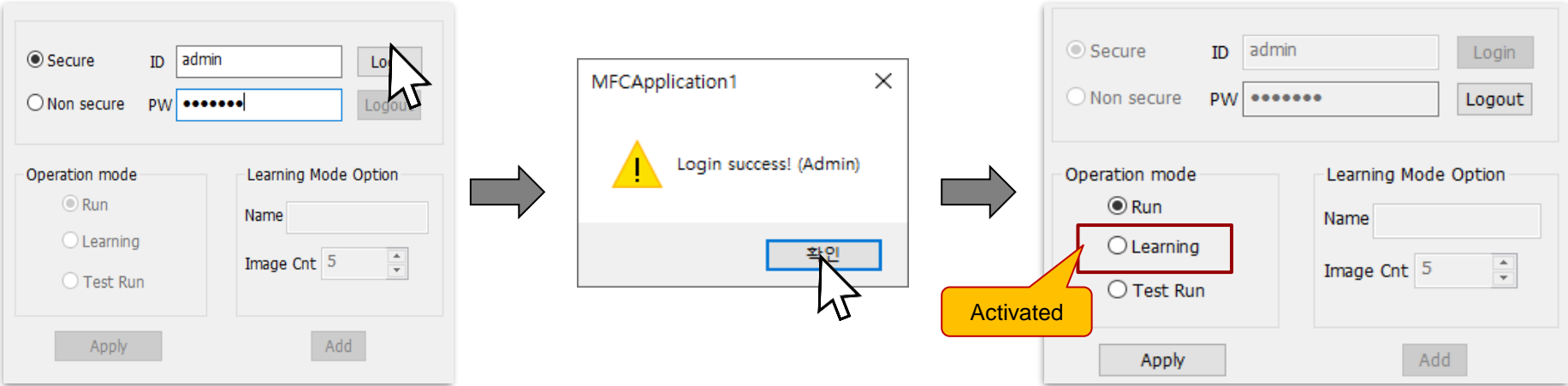


No.	Requirement	Requirement No.
SD-03	Separation of administrator privilege to manage DB in learning mode	RQ-SEC-SVR-01 RQ-SEC-SVR-02 RQ-SEC-SVR-08

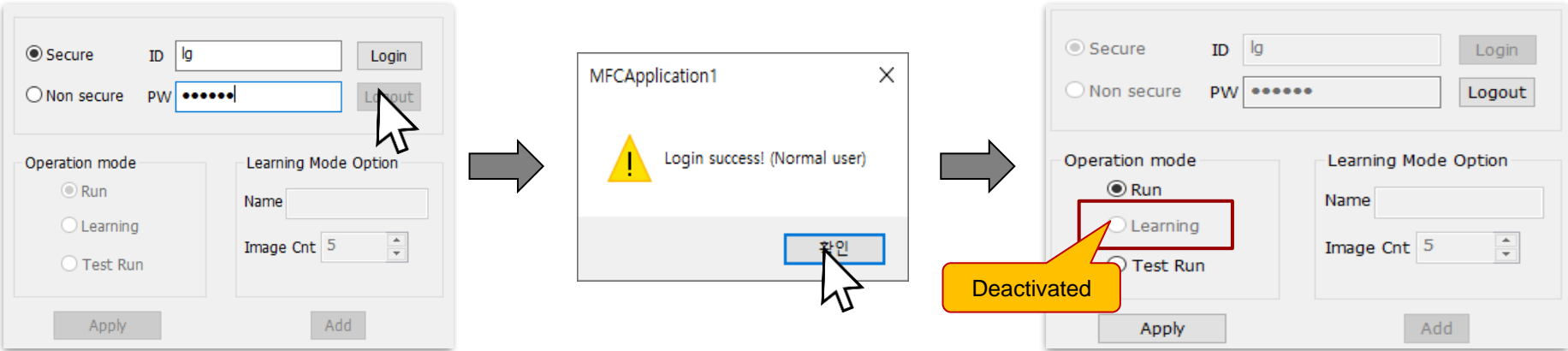


No.	Requirement	Requirement No.
SD-04	Implemented a limited user operation	RQ-SEC-SVR-03 RQ-SEC-SVR-08

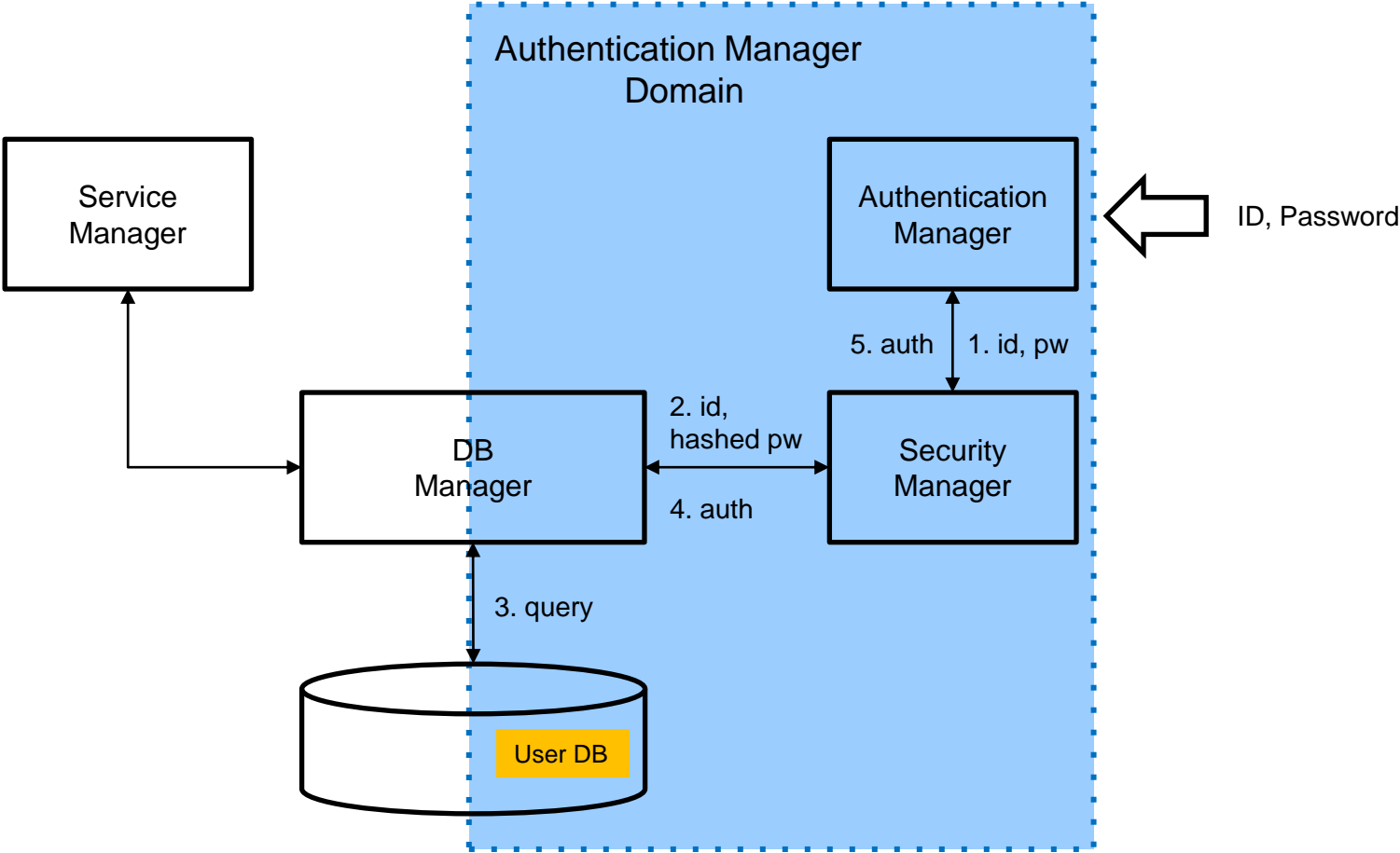
Administrator



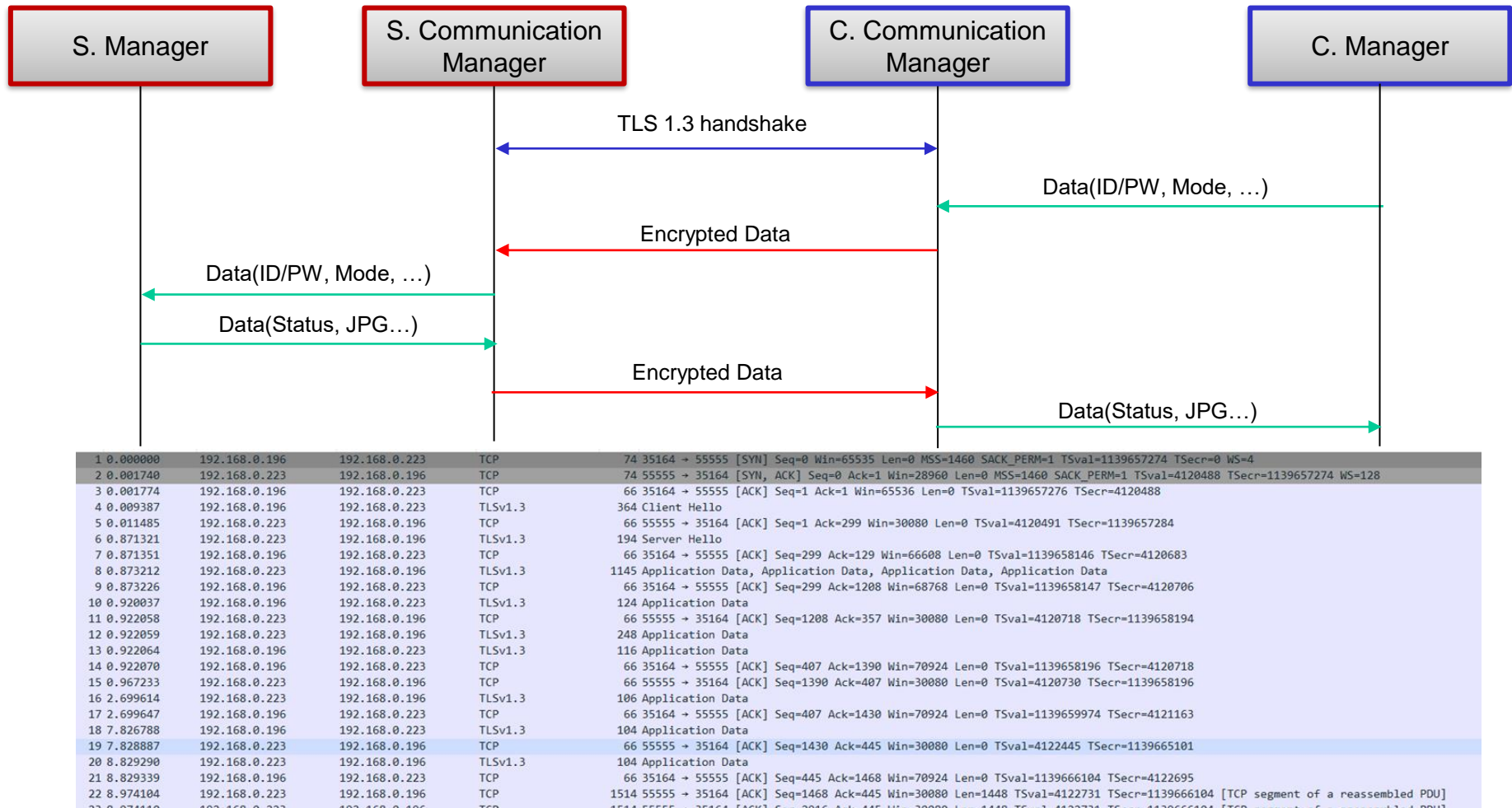
Normal user



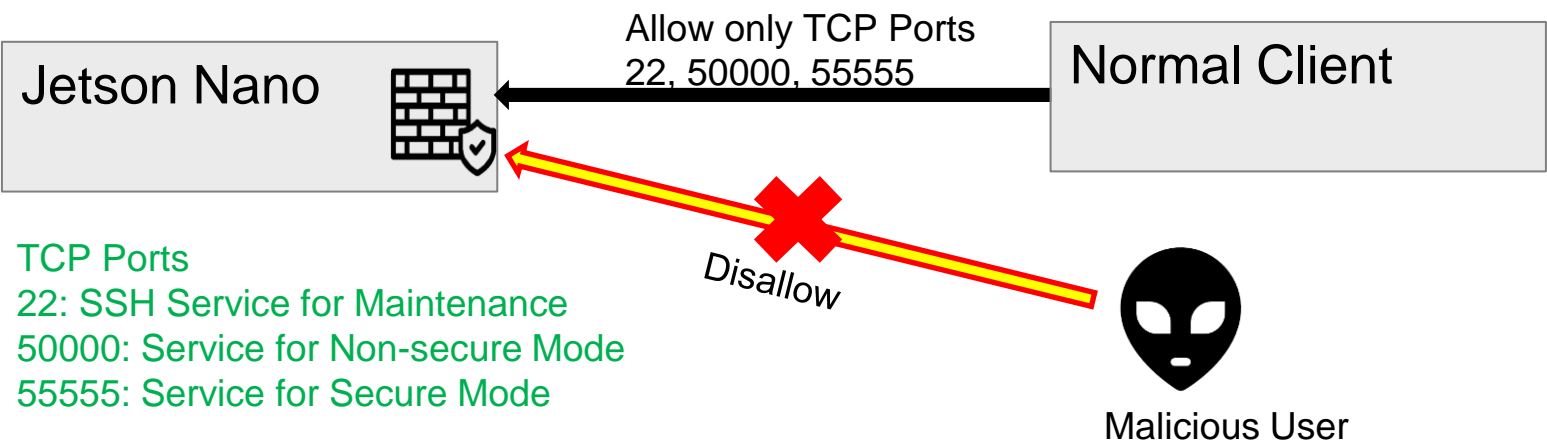
No.	Requirement	Requirement No.
SD-05	Implementation of 'Authentication Manager' module based on authentication process	RQ-SEC-SVR-04
SD-06	Separation of 'Authentication Manager' domain to store credential data (user's ID/PW, authority)	RQ-SEC-SVR-05



No.	Requirement	Requirement No.
SD-07	Modification of 'Communication Manager' to implement secure mode	RQ-SEC-SVR-06 RQ-SEC-SVR-07



No.	Requirement	Requirement No.
SD-08	Apply Firewall	RQ-SEC-SVR-09



No.	Requirement	Requirement No.
SD-09	UI design considering secure mode	RQ-SEC-CLI-01 RQ-SEC-CLI-02 RQ-SEC-CLI-03

TLS mode

☒ Secure

☐ Non secure

ID

admin

PW

••••••

Login

Logout

Plain text mode

Secure

Login

☐ Non secure

Logout

Operation mode

☒ Run

☐ Learning

☐ Test Run

Apply

Learning Mode Option

Name

Image Cnt

5

Add

Test Run Mode Option

Select

logging

Display

Team 1