1. Introduction

1.1 Purpose

The purpose of this document is to describe system design and design decisions to achieve quality of the Tartan monitoring system.

1.2 Scope

This document includes the following:

- Software quality goals implemented in the project
- Strategies and tactics to achieve quality goals
- System Architecture Overview
- Requirements and user cases, quality attributes
- Design decisions to achieve detailed goals

1.3 Definitions, acronyms, and abbreviations

- Authorized Person: Someone who can enter the server room. (Registered Persons with Jetson nano.)
- CCTV: Jetson Nano equipped with a camera (target)
- Monitoring System: A system that receives and displays a video screen sent by a Jetson Nano equipped with a camera
- User Register: A process for adding an Authorized Person.
- Security agent: A person observing the video transmitted by a Jetson Nano equipped with a camera. The role of supervising whether unauthorized persons enter the server room while observing the video through the monitoring system.
- Monitoring System manager: A person who has authority to add a new permitted person to enter server room

1.4 References

- Software Requirements
- LGE secure coding guide (LGE internal link) http://collab.lge.com/main/pages/viewpage.action?pageId=769000639#SecureCodingRule-C++

2. Project Overview

The main objective of this project is to design and implement a Tartan monitoring system to be secure and secure against various threats.

2.1 Quality Objectives

The main quality objectives of the project are as follows:.

- Confidentiality - Video stream data and stored personal data in the system should be protected from unintentional information leakage.
- Integrity - Video stream data and logs must not be attacked or modified arbitrarily.
- Availability - It should be always operated except during fixed daily maintenance hours.
- Non-repudiation - Tartan service should be able to trace the usage history of the service and records of access to the server room.

2.2 Strategies

Strategies to achieve the quality goal of project are as follows:

- Identifying quality attributes and making a design decision to select the optimal alternative among the alternatives to satisfy the attribute.
- Identify threats by exploring possible threats as much as possible.
- Among the identified threats, a high-priority threat is selected to derive mitigation and implement it.
- Make secure code during implementation to prevent threats that may occur due to internal vulnerabilities.

2.3 Tactics

For each strategy, perform the following tactics.

2.3.1 Identifying threats

Perform threat modeling to identify threats that can be exposed during the lifecycle of the Tartan monitoring system.
The candidates for the treats modeling approach considered are as follows.

- STRIDE
- Security Cards
- PnG

Among them, it was decided to apply STRIDE and PnG together. This is because STRIDE had the most experience and proficiency among each method, had the most available tools, and was expected to identify the most possible threats. In addition, PnG was additionally applied because it was expected that it would be helpful in additionally identifying usable threats from the attacker's point of view.

2.3.2 Selecting threats to mitigate

It is impossible to deal with all identified threats due to project constraints, so it is necessary to analyze the threats that have a great impact on achieving the security goals of the Tartan monitoring system and deal with the high-priority threats.

Consideration: evaluation methodology

Prioritization requires an assessment of impact and likelihood. The evaluation of impact and likelihood is inevitably influenced by the subjectivity of the evaluator, and a method to supplement the maturity of evaluation within the project is needed.

Decision: OWASP Risk Rating Methodology

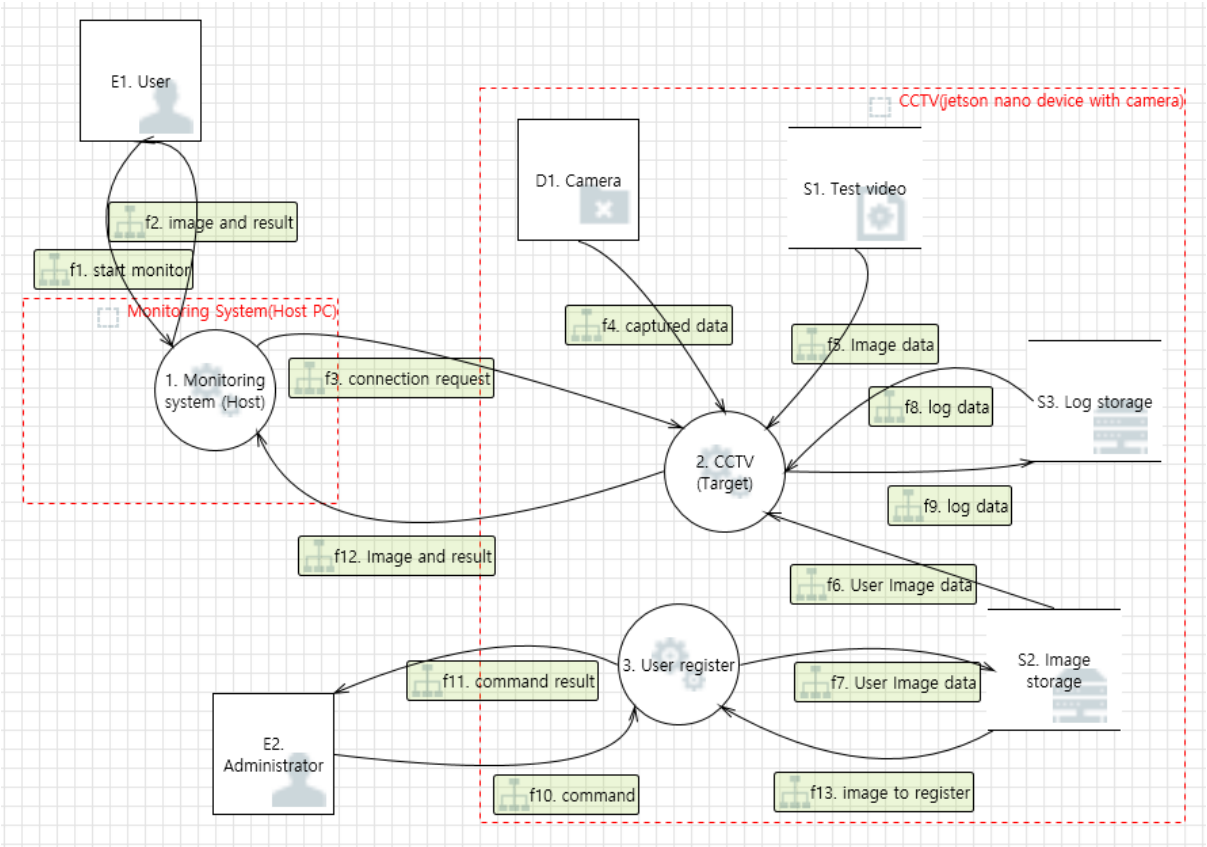
OWASP Risk Rating Methodology includes a scale that can be used for evaluation, and a framework for severity evaluation is formed, so it was decided to use it for evaluation.

2.3.3 secure coding

To keep the code secure, perform the following activities.

- For each pull-request, perform the code review by referring to the C++ secure coding guide of the LG Electronics Security Implementation Guide.
- In the integration stage, review analysis results of the tools below.
    - code X-ray: Review for severity greater than Major
    - sonar cloud: Review for severity greater than Major
    - FlawFinder: Review for severity greater than level 2

3. System Context



4. Architecture Drivers

4.1 Functional Requirements

4.1.1 operation mode

4.1.1.1 FR-1-01 Video stream

Security agents can view real-time video (video + personnel name) with the monitoring system.

Use case 1-01-1

User: security agents

Preconditions:

- The Monitoring System is installed on the PC(also cert. key is installed)
- Security agent was log on the PC
- CCTV is operating

Primary Flow

1. A Security Agent runs the Monitoring System.
2. After the Monitoring System is running, the video feed currently being sent by the CCTV is displayed on the monitor.
3. When an Authorized person enters the server room where CCTV is installed, their name is displayed in the video feed.
4. A Security Agent observes the Monitoring System during working hours.

Alternative Flow 1

1. A Security Agent runs the Monitoring System.
2. After the Monitoring System is running, the video feed currently being sent by the CCTV is displayed on the monitor.
3. When an unauthorized person enters the server room where CCTV is installed, "Unauthorized" is displayed in the video feed.
4. The Security Agent calls the Security guards immediately.

Use case 1-01-2

User: security agents

Preconditions:

- The Monitoring System is installed on the PC(also cert. key is installed)
- Security agent was logged on the PC and the Monitoring System is running.
- CCTV is operating.

Primary Flow

1. The connection between the monitoring system and CCTV that was observed is disconnected.
2. A message stating that the connection is trying is displayed on the screen.
3. It is connected to the CCTV again and the video feed currently being sent by the CCTV is displayed on the monitor.

Use case 1-01-3

User: an attacker
Preconditions:

- The Monitoring System is installed on attacker's PC
- CCTV is operating.

Primary Flow

1. The Attacker runs the Monitoring System.
2. The Monitoring System runs and attempts to connect to CCTV.
3. Connection to CCTV fails.

4.1.1.2 FR-1-02 Register Authorized

The Monitoring system manager can access CCTV and register a new Authorized Person.

Use case 1-02-1

User: a monitoring system manager

Preconditions:

- The name and photo of the Authorized Person to be added are saved in the PC
- Monitoring system manager logged into CCTV via ssh

Primary Flow

1. The monitoring system manager uploads a photo of the Authorized Person in the storage of the CCTV via scp.
2. The monitoring system manager executes User Register with the photo path uploaded and the name of the Authorized Person as arguments.
3. The User Register encrypts the photos, stores them in secured storage, and deletes the original photos.
4. The monitoring system manager logs out of ssh.

Alternative Flow

1. The monitoring system manager uploads a photo without the Authorized Person's face in the storage of the CCTV via scp.
2. The monitoring system manager executes User Register with the photo path uploaded from the shell and the name of the Authorized Person as arguments.
3. User Register displays a message saying that the face is not recognized as an invalid picture.
4. The monitoring system manager tries the contents of the Primary Flow again.

Alternative Flow

1. The monitoring system manager checks whether the photo is an inappropriate photo that is wearing a mask or is difficult to recognize normally.
2. The monitoring system manager rejects the inappropriate photo registration and requests a new photo from a new Authorized Person.

Use case 1-02-2

User: an attacker

Preconditions:
- The photo of the unauthorized person to infiltrate are stored in the PC
- Logged in to CCTV with the stolen user's account (not superuser)

Primary Flow
1. The attacker uploads a photo without the unauthorized Person's face in the storage of the CCTV via scp.
2. The attacker executes User Register with the photo path uploaded and any name as arguments.
3. Execution fails because the user which was stolen does not have permission to execute User Register.

4.1.1.3 FR-1-03 Unregister Authorized

The Monitoring system manager can access CCTV and unregister an Authorized Person.

Use case 1-03-1

User: a monitoring system manager

Preconditions:
- Having a list of people to exclude from Authorized Person
- The monitoring system manager logged into CCTV via ssh

Primary Flow
1. The monitoring system manager executes the User Register with the name of the person to be excluded from the Authorized Person as an argument.
2. The User Register deletes photos in secured storage.
3. The monitoring system manager logs out of ssh.

Alternative Flow
1. The system manager executes User Register with a name not included in Authorized Person as an argument.
2. User Register displays a message saying that the name does not exist.
3. The monitoring system manager tries the contents of the Primary Flow again.

4.1.1.4 FR-1-04 Entry / exit history log

The Monitoring system manager can check the past entry/exit history of the server room(time + person name)

Use cases 1-04-1

User: a monitoring system manager

Preconditions:

- A state in which someone entered after the CCTV was activated
- The monitoring system manager logged into CCTV via ssh

Primary Flow

1. The monitoring system manager moves to the [log directory] and checks the saved log file.
2. The monitoring system manager uses commands such as cat to read the contents of the log file.
3. The monitoring system manager logs out of ssh.

3.2.1.5 FR-1-05 Connection history log

The Monitoring system manager can check the past connection/disconnection records of the Monitoring System.

Use cases 1-05-1

User: a monitoring system manager

Preconditions:

- After the CCTV and the monitoring system are operated
- The monitoring system manager logged into CCTV via ssh

Primary Flow

1. The monitoring system manager moves to the [log directory] and checks the saved log file.
2. The monitoring system manager uses commands such as cat to read the contents of the log file.
3. The monitoring system manager logs out of ssh.

4.1.2 dev. mode

This function is not used when it is installed as a product.
This mod is for testing during development only and is not included when installed as a product.

4.1.2.1 FR-2-01 Video stream

Security agents can view real-time video (video + personnel name) with the monitoring system.

Use case 2-01-1

User: developer

Preconditions:

- The Tartan monitoring system is dev. mode
- CCTV is operating

Primary Flow

1. A developer runs the Monitoring System.
2. After the Monitoring System is running, the video feed currently being sent by the CCTV is displayed on the monitor.
3. When an Authorized person enters the server room where CCTV is installed, their name is displayed in the video feed.

Alternative Flow 1

1. A developer runs the Monitoring System.
2. After the Monitoring System is running, the video feed currently being sent by the CCTV is displayed on the monitor.
3. When an unauthorized person enters the server room where CCTV is installed, "Unauthorized" is displayed in the video feed.

Use case 2-01-2

User: developer

Preconditions:

- The Tartan monitoring system is dev. mode
- The Monitoring System is running.
- CCTV is operating.

Primary Flow

1. The connection between the monitoring system and CCTV that was observed is disconnected.
2. A message stating that the connection is trying is displayed on the screen.
3. It is connected to the CCTV again and the video feed currently being sent by the CCTV is displayed on the monitor.

4.1.2.2 FR-2-02 Register Authorized

The Monitoring system manager can access CCTV and register a new Authorized Person.

Use case 2-02-1

User: developer

Preconditions:

- The Tartan monitoring system is dev. mode
- The name and photo of the Authorized Person to be added are saved in the PC
- The developer logged into CCTV via ssh

Primary Flow

1. The developer uploads a photo of the Authorized Person in the storage of the CCTV via scp.
2. The developer executes User Register with the photo path uploaded and the name of the Authorized Person as arguments.
3. The User Register encrypts the photos, stores them in secured storage, and deletes the original photos.

Alternative Flow

1. The developer uploads a photo without the Authorized Person's face in the storage of the CCTV via scp.
2. The developer executes User Register with the photo path uploaded from the shell and the name of the Authorized Person as arguments.
3. User Register displays a message saying that the face is not recognized as an invalid picture.

4.1.2.3 FR-2-03 Unregister Authorized

The Monitoring system manager can access CCTV and unregister an Authorized Person.

Use case 2-03-1

User: developer

Preconditions:

- The Tartan monitoring system is dev. mode
- Having a list of people to exclude from Authorized Person
- The monitoring system manager logged into CCTV via ssh

Primary Flow

1. A developer executes the User Register with the name of the person to be excluded from the Authorized Person as an argument.
2. The User Register deletes photos in secured storage.

Alternative Flow

1. A developer executes User Register with a name not included in Authorized Person as an argument.
2. User Register displays a message saying that the name does not exist.

4.1.2.4 FR-2-04 Learning mode

Developers can capture the contents of the video feed for face recognition learning and testing and register the person in the video as an Authorized person.

Use case 2-03-1

User: developer

Preconditions:

- The Tartan monitoring system is dev. mode
- Having a list of people to exclude from Authorized Person
- The monitoring system manager logged into CCTV via ssh

Primary Flow

1. The developer runs the CCTV process in the foreground in the shell.
   The developer shoots a person with a camera.
2. The developer presses 'n' key.
3. The developer inputs the person's name.
4. The entered person and name are learned and registered as an Authorized person.

4.2 Security Requirements

Mitigation was derived by analyzing the selected security threats, and security requirements were defined for this.

4.2.1 SR-01 Personal photo protection

Image should be encrypted before saved to storage in CCTV.

4.2.2 SR-02 Separation and minimization of privileges

Access to the image storage in CCTV should only be possible with the cctv account.
The access of the cctv account to the image storage in CCTV should have read/write/execute rights.
Access to the log directory in CCTV should only be possible with the cctv account and the manager.
The access of the cctv account to the log directory in CCTV should have read/write/execute rights.
The access rights of the manager account to the log directory in CCTV should have read/execute rights.

4.2.3 SR-03 Secure connection

Network sections between CCTV and monitoring systems should be encrypted.
Network between CCTV and the monitoring system is secured by using TLSv1.2.

4.2.4 SR-04 Mutual authentication

CCTV and monitoring systems must be mutual authentication.

4.25 SR-05 Certificate protection

It should be protected from attacks so that the authentication key required for mutual authentication is not stolen.

3.4.6 SR-06 Availability guaranteed

The Tartan monitoring system shall not be shutdown at any time other than daily, periodic maintenance.
If CCTV is abnormally terminated due to an external attack or unexpected internal problem, it must be connected to the monitoring system again within 5 minutes to resume its function.

4.3 Quality Attributes

4.3.1 List of Quality Attributes

ID	Attribute	Title	Priority	Difficulty
QA-01	Performance	High quality video	Medium	Hard
QA-02	Availability	CCTV uptime	High	Hard
QA-03	Confidentiality	Video stream data and stored personal data in the system should be protected	High	Medium
QA-04	Integrity	Video stream data and logs must not be attacked or modified arbitrarily	High	Medium

4.3.2 Quality Attribute Scenarios

4.3.2.1 QA-01 High quality video

ID: QA-01	**Attribute:** Performance
CCTV should guarantee a resolution quality enough to recognize the face of a person entering and exit, a frame quality to check the movement, and a delay time enough to take action against unauthorized personnel.	
Stimulus: Video stream is received from the CCTV	
Source: Security Agents (Monitoring System client)	
Environment: Normal operation	
Artifact: CCTV	
Response: Security Agents receive a video stream that is sufficient to identify.	
Response measure: resolution: 640 x 480 frame rates: 7fps End-to-End latency within 500ms	

4.3.2.2 QA-02 CCTV uptime

ID: QA-02	**Attribute:** Availability
The Tartan monitoring system shall not be shutdown at any time other than daily, periodic maintenance. If CCTV is abnormally terminated due to an external attack or unexpected internal problem, it must be connected to the monitoring system again within 5 minutes to resume its function.	
Stimulus: CCTV is terminated abnormally while receiving video stream by CCTV	
Source: CCTV	
Environment: Normal operation	
Artifact: CCTV	
Response: CCTV service resumes, restores the disconnected connection with the monitoring system, and continues to transmit video streams.	
Response measure: recovery time: time to reconnection, within 5 min.	

4.3.2.3 QA-03 Communication Confidentiality

ID: QA-03	**Attribute:** Confidentiality
Video stream data and stored personal data in the system should be protected	
Stimulus: Attempting unauthorized access to stream data and stored data	
Source: unauthorized one	
Environment: all the time (include shutdown time)	
Artifact: video stream data, personal image, log data	
Response: Attempting unauthorized access to data should be refused or unreadable.	
Response measure: possibility of information leak	

4.3.2.4 QA-04 Communication Confidentiality

ID: QA-04	**Attribute:** Integrity
Video stream data and logs must not be attacked or modified arbitrarily	
Stimulus: Attempting change the stream data and stored data	
Source: unauthorized one	
Environment: all the time (include shutdown time)	
Artifact: video stream data, personal image, log data	
Response: Attempting unauthorized access to data should be refused or detected.	
Response measure: possibility of tampering	

5. Design Decisions

5.1 QA-01 High quality video

The video stream of CCTV must support a resolution high enough to recognize a human face and a speed as close to real-time as possible.

5.1.1 Solutions

1. Increase speed by reducing frame size
    a. The current resolution is width = 640, height = 480, and check the optimal size to increase speed while reducing the size of width and height.
2. optimizing per-frame processing operations
    a. Improve performance on NVIDIA Jetson Nano

solution	pros	cons.
1	Reducing the frame size will speed things up.	Decreased face recognition rate
2	Increase processing speed	Requires a lot of resource input limitation upper bound

5.1.2 Decision

Keep the current level

- Keep the current size by determining that the face recognition rate has priority over speed in the quality goal
- Considering the short development time, it is expected that a lot of resource input will be required.

5.2 QA-02 CCTV uptime

In the case of cctv, which is a component of the Tartan system, it should always be activated for the security of the server room.

5.2.1 Solutions

It checks whether the CCTV program is running normally, and in case of abnormal termination, the system should be re-executed to keep the CCTV program alive.

There are three ways to satisfy the above.

1. Using Redundancy
2. A new person in charge who can check whether the CCTV system is operating normally is assigned, and the execution authority of the CCTV system is given.

3. The CCTV system is configured so that it can be executed automatically when it is automatically booted after power is supplied, and it is automatically restarted when the CCTV program dies due to unknown reasons.

solution	pros	cons.
1	Stable backup is possible	Additional system resources are required, and additional structural design such as Spanning Tree Protocol is required.
2	Only necessary privileges can be granted to the security agent.	A resource to continuously check the CCTV program is needed.
3	No separate resource is required.	If the program falls into an unknown state where it does not die and does not work, it is necessary to restart the CCTV.

5.2.2 Decision

Solution 3 was selected to minimize the scope of threats by minimizing additional resources and separating privileges as much as possible. When the CCTV is powered on and booted, the systemd function is used to automatically execute the program, and the program is executed in the following principle through systemd.

- Make sure that the CCTV program starts immediately after the CCTV equipment is turned on (after network connection?).
- If the CCTV program is terminated, it is automatically restarted after 5 seconds by systemd.
- At this time, in case the camera module is also abnormally terminated, when the CCTV program is restarted, the camera module is automatically restarted.

5.3 QA-03 QA-04 SR-01 encrypt images data in CCTV storage

Photos of authorized personnel stored in CCTV devices must be encrypted and stored to determine whether the server room is accessible. The file name should also be encrypted so that it cannot be recognized in order to not be able to identify which personnel are authorized through the file name.

5.3.1 Solutions

The encryption method has the following methods.

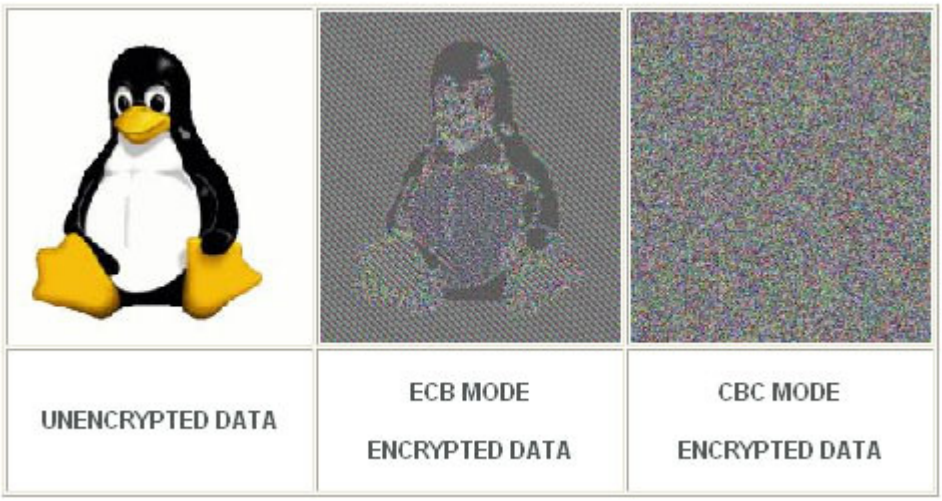
topic	type	pros.	cons.

Encryption key type	symmetric		speed is fast	The key should be kept well.
	unsymmetric		speed is too slow compared to symmetric key.	
Encryption key size	aes	128	The longer the key, the higher the encryption intensity.	The longer the key, the longer the encryption time.
		192		
		256		
	rsa	1024		
		2048		
Encryption mode	cbc		There is an association between encryption blocks, and decryption is not possible if you know the encryption key and you don't know the iv.	
	ecb		There is no association between encryption blocks. When an error occurs in one block, the error is not propagated to the other block.	

5.3.2 Decision

To satisfy NIST's recommended encryption and minimize performance impact, we choose the aes_128 encryption method. The encryption mode is selected to cbc mode. Because if the ecb method is used to encrypt image files, the original file can be guessed.

Therefore, the encryption eventually uses aes_128_ecb mode.



The encryption of file names is also encrypted using the same aes_128_ecb mode, and then converted and saved via base64 encoding to store binary results as recognizable file names in the OS.

5.4 QA-03 Secure connection

Video streaming data delivered over a network must be secured against leaks or manipulation.

5.4.1 Solutions

Two solutions for data protection were reviewed.

1. Data encryption : Encrypt data using symmetric key on sender, then decrypt data on receiver. Same key is used on both sides.
2. Transport Layer Security : Apply TLS protocol with certificate pair which is signed by certificate authority.

Solution	Pros.	Cons.
Data encryption	Simple design and easy to apply	The same key should be kept on each side, and it is not easy to prevent leakage.
TLS	widely adopted security protocol	1. It cannot be implemented by ourselves, but can be applied through an open source library. 2. Each certificate pair should be signed by certificate authorities

5.4.2 Decision

TLS is chosen to use for the following reasons,

- TLS is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet.
- In the case of OpenSSL v1.0.1, a vulnerability such as "heart bleed" had been reported, but in the case of the latest version 1.1.1, the vulnerability has been fixed, and stability has been proven as a library that has been applied worldwide until now.
- For certificate pairs to use, there are issues of time and resources to obtain a certificate from an official CA, so in this project, a self-signed root CA is generated by ourselves and it replaces the official CA.

5.5 SR-02 apply ACLs

Access to the image storage in CCTV should only be possible with the cctv account.
The access of the cctv account to the image storage in CCTV should have read/write/execute rights.
Access to the log directory in CCTV should only be possible with the cctv account and the manager.
The access of the cctv account to the log directory in CCTV should have read/write/execute rights.
The access rights of the manager account to the log directory in CCTV should have read/execute rights.

5.5.1 Solutions

There are two methods reviewed for controlling access rights of image storage in CCTV.

1. Using the ACL function provided by Linux, set and separate image storage access rights for each of the cctv account, manager account, and other accounts.
2. eCryptfs: Restricts access between accounts by encrypting each file system of the cctv account, manager account, and other accounts using credential information for each account.

solution	pros	cons.
1	Linux ACL enables detailed access rights settings for each account for individual files and directories. Technology provided by default in Linux, with fewer additional learning curves.	There is no control method in case of account hijacking.
2	eCryptfs can support file system encryption based on credential for each account	It is not easy to set detailed settings for files and directories. Additional work (kernel build, library test) and learning curve exist to apply the technology

5.5.2 Decision

The reasons for selecting Linux ACL are as follows.

- Linux ACL is advantageous to apply detailed access permission restrictions for each cctv and manager account to the image file, log directory, and user register executable file.
- CCTV is a service that runs in a Linux environment, and it is advantageous to use Linux ACLs.

5.7 SR-04 Mutual authentication

To prevent spoofing attacks at both ends of the monitoring system and CCTV, authentication must be checked at each end.

5.7.1 Solutions

How to identify authentication between Monitoring System and CCTV is as follows.

1. Using IP, MAC
2. Using password
3. Using certificate

The pros and cons of applying each alternative to the current situation are as follows.

solution	pros.	cons.
1	Implementation is the simplest	Since an attack that modifies IP and MAC is possible, spoofing cannot be reliably prevented.
2	Implementation is simple.	To prevent the password from being exposed, the communication section must be encrypted, and a module for user credentials is required. If exposed to sniffing attacks, it can be neutralized.
3	This is the most effective authentication method.	There is a burden of creating, distributing, and managing certificates.

5.7.2 Decision

To use the most effective countermeasures rather than considering trade-offs, solution3. The authentication method using a certificate was selected. In order to use this solution, the process of generating, distributing, and storing certificates must be performed securely. How to safely store the certificate is treated as an additional requirement.

Consideration: Creating certificate

The types of certificates that can be used are as follows.

- Certificate issued by a trusted root CA
- Certificate issued by a self-signed root CA
- self-signed certificate

I chose the certificate issued by a self-signed root CA.
The most reliable method is a certificate issued by a trusted root CA, but it cannot be used because the time required to issue a certificate to the trusted root CA does not appropriate the target schedule of this project. Also, self-signed certificates were excluded because they were vulnerable to MITM attacks. Also, self-signed certificates were excluded because they were vulnerable to MITM attacks.

5.11 SR-06 Management of certificate of the monitoring system (windows)

If the certificate used for authentication is stolen, the spoofing defense, sniffing defense, and tempering defense are neutralized, so the certificate must be kept secure.

5.11.1 Solutions

Alternatives to keeping the certificate are as follows.

1. hide certificate file(public key, private key)
2. Put the certificate file in the .ssh directory and set the file access permission so that only the user can access it.
3. It is stored in the windows certificate store and retrieved from the monitoring system application through cryptoAPI.

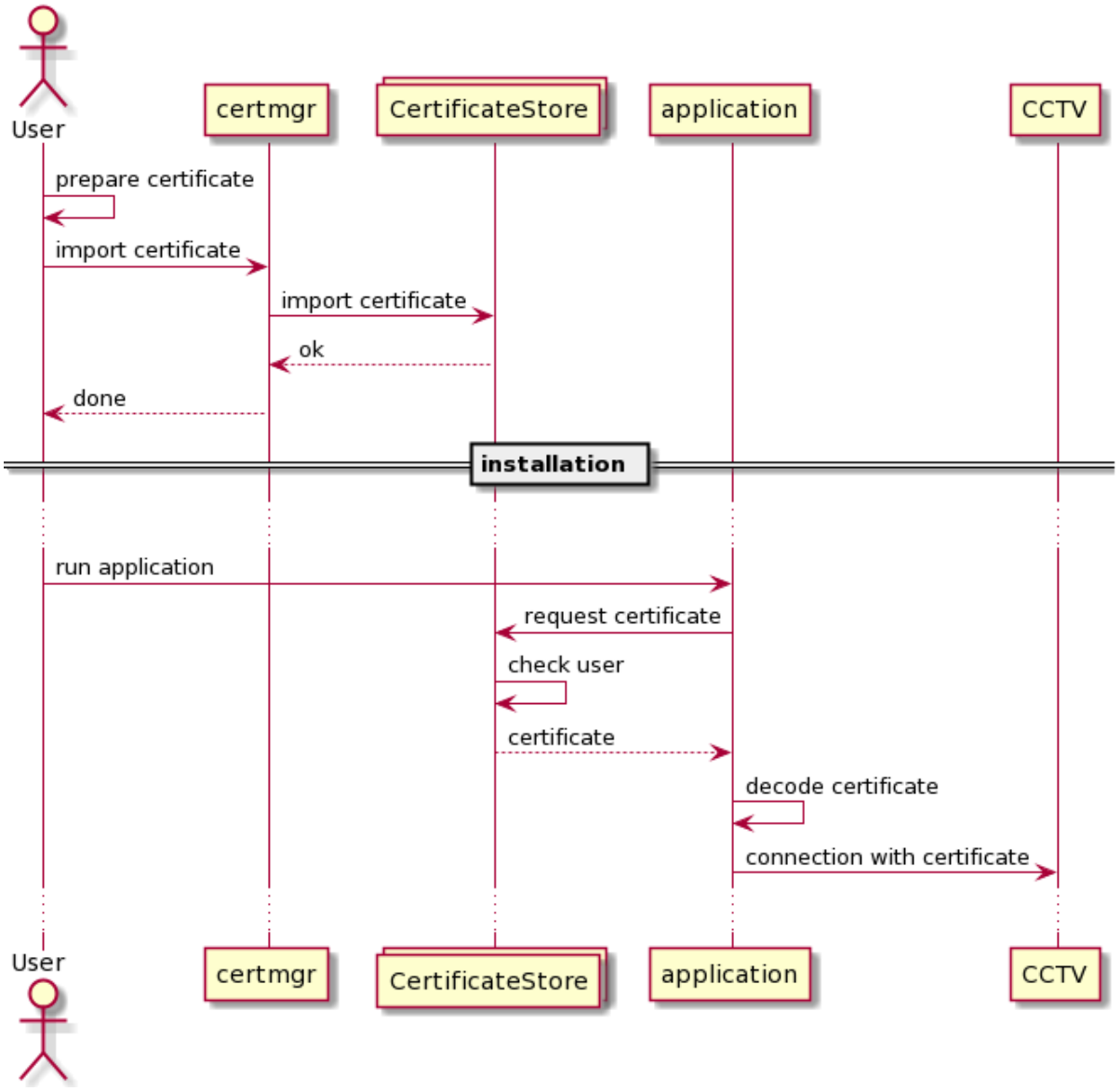
The pros and cons of applying each alternative to the current situation are as follows.

solution	pros.	cons.
1	Implementation is the simplest	Because hidden locations are inevitably exposed, it is difficult to prevent hijacking.
2	Implementation is simple. It can be used only by that user, so it can be protected to some extent from stealing by other users without permission.	If the user's account is hijacked, the certificate is leaked. It is difficult to prevent being hijacked by malware or other attacks.
3	This is the most secure way to defend against the vulnerabilities of other solutions above.	The procedure for importing a certificate into the windows certificate store should still be protected.

5.7.2 Decision

To use the most effective countermeasures rather than considering trade-offs, solution3. has chosen To use this solution, the process of importing the certificate must be carried out securely.

The process of using the windows certificate store is as follows.



Consideration: import certificate

In this sequence, the part where the certificate is prepared before the user imports the certificate can be a vulnerable section where the certificate can be stolen.

5.12 SR-06 Management of certificate of the CCTV (linux)

If the certificate used for authentication is stolen, the spoofing defense, sniffing defense, and tempering defense are neutralized, so the certificate must be kept secure.

5.11.1 Solutions

Alternatives to keeping the certificate are as follows.

1. hide certificate file(public key, private key)
2. Put the certificate file in the .ssh directory and set the file access permission so that only the user can access it.
3. It is stored in the linux keystore and retrieved from the monitoring system application through API.

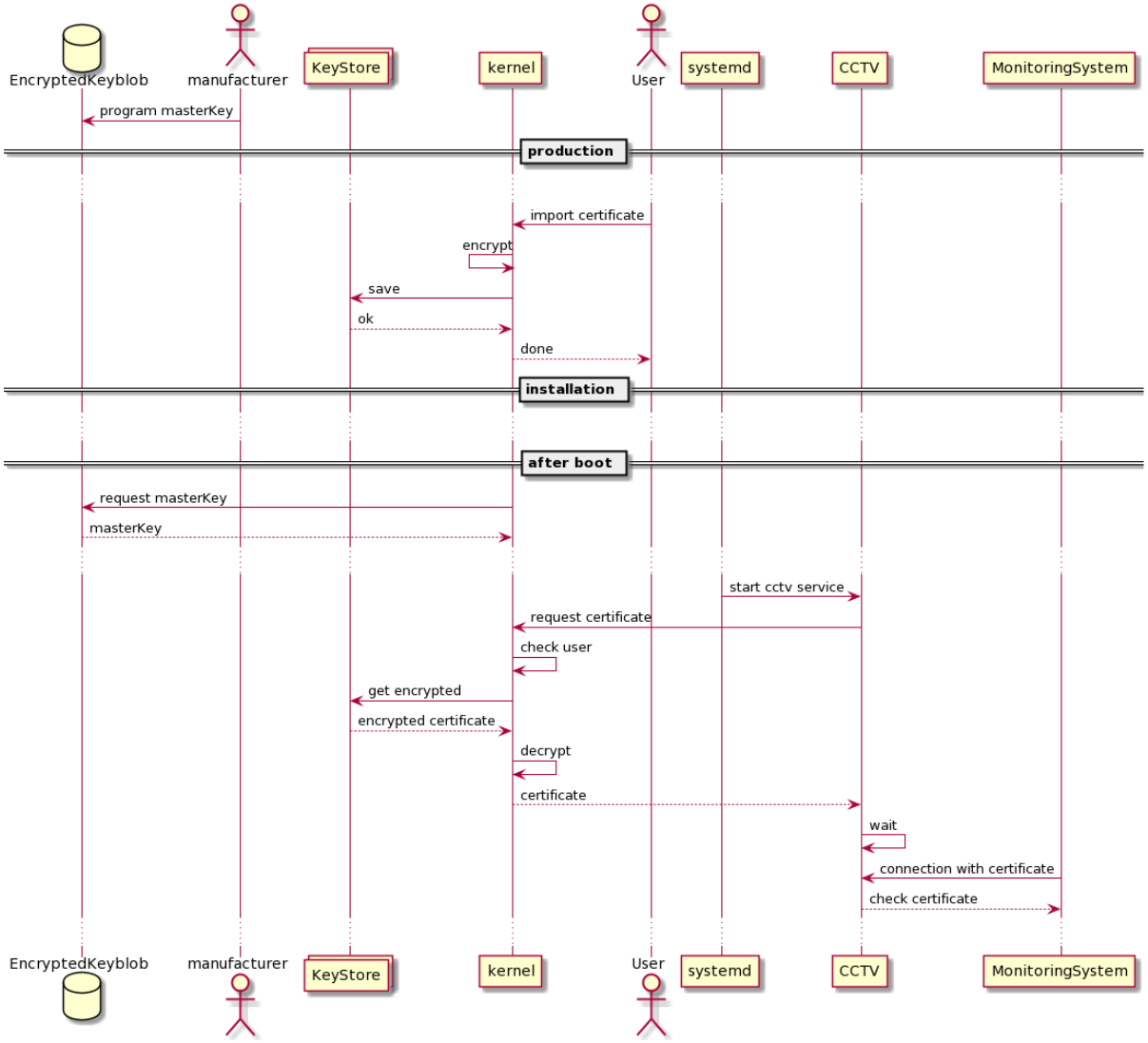
The pros and cons of applying each alternative to the current situation are as follows.

solution	pros.	cons.
1	Implementation is the simplest	Because hidden locations are inevitably exposed, it is difficult to prevent hijacking.
2	Implementation is simple. It can be used only by that user, so it can be protected to some extent from stealing by other users without permission.	If the user's account is hijacked, the certificate is leaked. It is difficult to prevent being hijacked by malware or other attacks.
3	This is the most secure way to defend against the vulnerabilities of other solutions above.	The procedure for importing a certificate into the linux keystore should still be protected. It needs a way to secure the master key to encrypt the certificate.

5.7.2 Decision

To use the most effective countermeasures rather than considering trade-offs, solution3. has chosen To use this solution, the process of importing the certificate must be carried out securely.

The process of using the linux keystore is as follows.



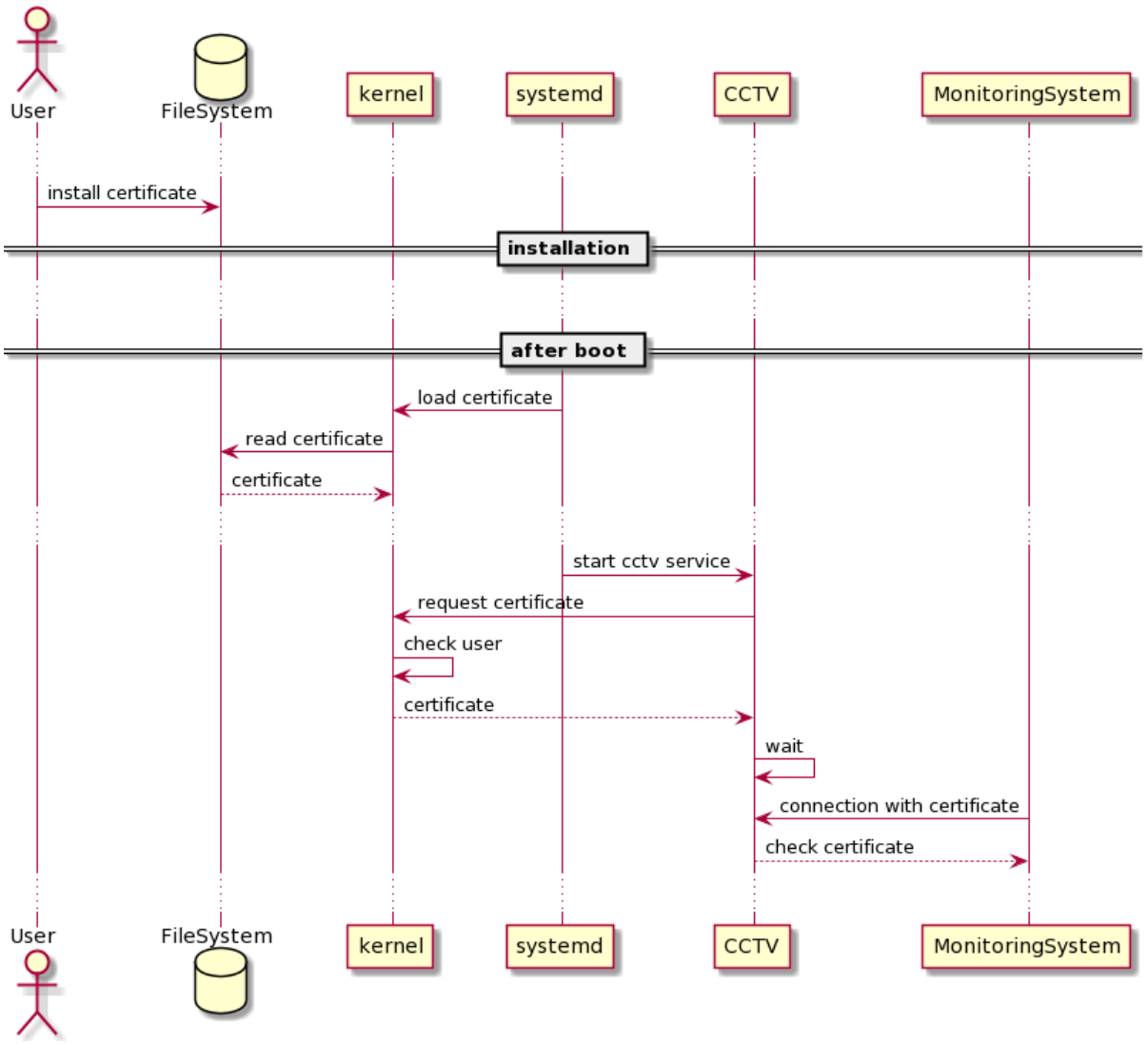
However, the implementation in this project was eventually replaced by other methods due to the issues below.

issue 1:

Master key program cannot be done in project scope.

issue 2:

There was a bug where the key registered in linux key management could not be properly imported. (systemd/systemd#5522) We tried another undocumented workaround because it was a known issue.



The compromised alternative to work now is the issue caused by issue 1 and issue 2, and will be implemented in the form of solution 3 in the actual product.