4tential

Tartan
Monitoring System Requirements

1. Introduction

1.1 Purpose

This document is intended to specify and explain the objectives, functions, constraints, etc. that the tartan monitoring system must achieve.

1.2 Scope

The content covered in this document is as follows.

- Purpose of the system and background of development
- Quality Objectives for Systems
- The capabilities the system
- Conditions and constraints under which the system operates

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
- MVP: Minimum Viable Product.

1.4 References

- Threat List
- Risk Assessment
- CCTV Installation Guide
- Monitoring system Installation Guide

2. Overall description

The tartan monitoring system is installed in the server room, etc. of a company that requires security of access, and provides real-time video information to recognize the faces of people entering and leaving and to help determine whether they are authorized to enter or not.

2.1 System purpose / background

In the case of using the surveillance CCTV system, which provides only real-time video, it may be difficult for security agents to remember the faces and identities of authorized personnel, which may not prevent unauthorized personnel from entering. In addition, manually replaying the entire video to check the access history of which people entered and left the video takes a lot of time and money and there is a risk that identification of access records may be omitted.

The tartan monitoring system provides a function to analyze the faces of visitors and display the authorized number of people in real-time images, helping them identify themselves and keeping records of the number of people entering and leaving them easy and accurate.

2.2 Business goals

In this project, essential functions to identify entrants and verify access records should be provided as soon as possible so that they can be used as the Minimum Possible Project (MVP).

However, even products in MVP form should not be hindered by external attacks or misuse in the operation of essential functions of the tartan monitoring system.

In addition, as MVP, the following should be achieved due to the nature of the system that needs to be continuously improved and developed.

- Rather than the usability of the system, the focus should be on identifying functional usability and feasibility in the near future.
- For developmental convenience, it should provide the ability to save and learn non-secure mode and video feed that are used only during development.

2.3 Security goals

The tartan monitoring system must meet the security objectives below.

- 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 operated uninterrupted except for a fixed daily inspection time.
- Non-repudiation - Tartan service should be able to trace the usage history of the service and records of access to the server room.
- The authorized person shall be updated through a specified procedure and shall not be changed at any time except specified time.
- We need to be prepared for predictable threats and avoid exposing vulnerabilities due to security-weak codes.

2.4 Product components

The tartan monitoring system consists of the following elements.

- CCTV box with camera that can be connected by wireless network
- A Windows PC that displays video streams on the screen.
- PC that manages authorized person lists and checks surveillance history.

2.5 Product functions

The tartan monitoring system should provide the following key functions.

1. Security agents can view real-time video (video + personnel name) with the monitoring system.
2. The Monitoring system manager can access CCTV and register a new Authorized Person.
3. The Monitoring system manager can access CCTV and unregister an Authorized Person.
4. The Monitoring system manager can check the past entry/exit history of the server room(time + person name)
5. The Monitoring system manager can check the past connection/disconnection records of the Monitoring System.

2.6 User characteristics

Below are the main users of this system.

- Security Agents: As a security guard, observe the screen monitored by CCTV in the security room to ensure that unauthorized personnel are not entering. There is no authorised authority other than access to CCTV footage. It does not require special skills or expertise.
- Monitoring system manager: As a security manager, the list of authorized personnel can be controlled and access records and system operation records can be accessed. It is responsible for the operation of the system and allows basic operation of the Linux system.

2.7 Assumptions and dependencies

CCTV equipment and H/W components that make up the Tartan monitoring system must be physically protected. If CCTV equipment is physically damaged or stolen, the system cannot achieve its purpose.
In addition, the system cannot achieve its purpose even if the network and power supply required by the tartan monitoring system are not smooth.

In this project, it is assumed that the physical protection of CCTV equipment installed is prepared, and unnecessary connection port removal work is completed.

The following items are excluded from the scope of the project and its achievement objectives.

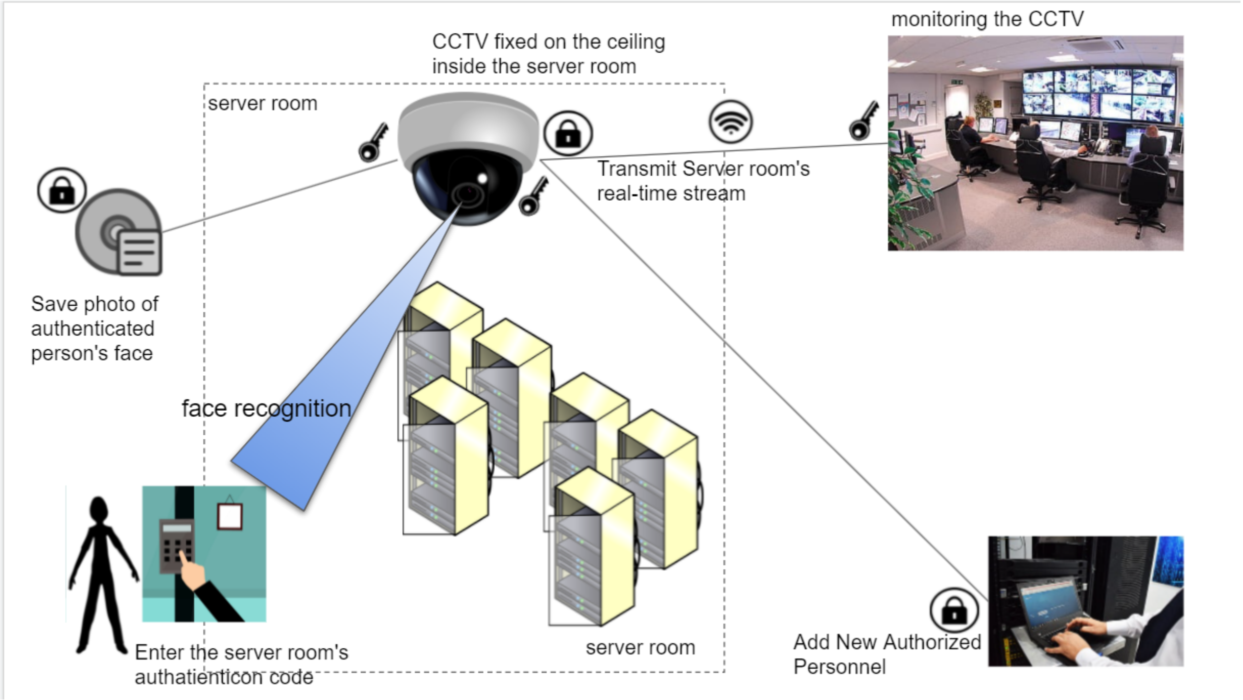
- Mitigation measures against side channel attacks are not considered.
- We do not consider mitigation measures against social attacks.
- Quality related to face recognition accuracy is not considered.

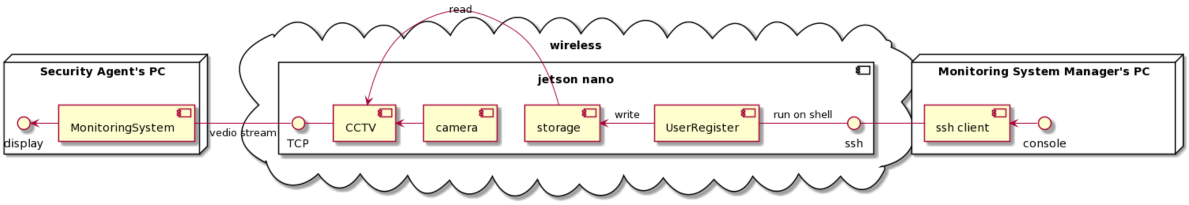
3. Specific requirements

3.1 Components and interfaces

The component configuration and interface of the Tartan system are approximately as follows.

System Concepts





- CCTV:
  It is installed in the server room and sends video streams to the monitoring system for checking visitors. It is transmitted using TCP based on wireless networks.
- Monitoring System:
  Display video streams sent from CCTV to security agents.
- UserRegister:
  When a request that adding new authorized person exists, the monitoring system manager accesses the CCTV via ssh and registers the new authorized person to the CCTV system.

3.2 Functions

The operation of the tartan monitoring system is divided into operation mode and dev. mode. Only operation mode is available while the actual product is deployed and running, and dev. mode is only available within the development team during the product development cycle. Switching between modes during execution is not possible.

3.2.1 operation mode

3.2.1.1 FR-1-01 Video stream

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

3.2.1.2 FR-1-02 Register Authorized

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

3.2.1.3 FR-1-03 Unregister Authorized

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

3.2.1.4 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)

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.

3.2.2 dev. mode

It is a feature that is not included when installed as a real product.
This mode exists only for testing during development and is not included when installed as a product.

3.2.2.1 FR-2-01 Video stream

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

3.2.2.2 FR-2-02 Register Authorized

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

3.2.2.3 FR-2-03 Unregister Authorized

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

3.2.2.4 FR-2-04 Learning mode

Developers can capture the contents of camera images for face recognition learning and testing and register the person in the captured images as Authorized Person..

3.3 Performance requirements

CCTV should guarantee the quality of resolution enough to check the face of the person entering and leaving, the level of frame to check the movement, and the delay time enough to take action against unauthorized personnel.
Therefore, the monitoring system must provide the video stream with the following performance.

- Resolution : 640 x 480
- Frames per second : 7 fps
- Latency : 0.5s

3.4 Security requirements

We define security requirements below to apply mitigation derived from identifying and analyzing possible threats to achieve the security goals of 2.4.
These requirements are derived through threat analysis and mitigation work.

See document below.

- Security_Requirement_Mitigation
- Treat List
- Risk Assessment

3.4.1 SR-01 Personal photo protection

Image should be encrypted before saved to storage in CCTV.

3.4.2 SR-02 Separation and minimization of privileges

Access to image storage in CCTV is limited to manager groups and a cctv user.
Permission of files in image storage are set to execute/read only.

3.4.3 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.

3.4.4 SR-04 Mutual authentication

CCTV and monitoring systems must be mutual authentication.

3.4.5 SR-05 Certificate protection

Requirements derived from Design decisions.
The certificates required to authenticate mutually must be protected from attacks.

3.4.6 SR-06 Availability guaranteed

The tartan monitoring system should not be shut down at any time other than the daily routine inspection.
In the event of an abnormal shutdown due to an external attack or an unexpected internal problem, CCTV should be connected to the monitoring system again within five minutes to resume functional performance.

3.5 Design & implementation constraints

The tartan monitoring system should be configured as follows.

3.5.1 H/W, platform constraints

It has the following H/W, platform constructs.

- CCTV should be implemented on Jetsonano H/W and Linux operating systems.
- The monitoring system must operate on the Windows 10 operating system.
- The tartan monitoring system must operate in a wireless network environment.

3.5.2 S/W, component constraints

It has the following S/W, component constraints.

- Face recognition algorithms and modules require the use of provided facenetModels and MTCNN_FaceDetection_TensorRT modules.
- Video display, video/image processing should use the openCV library.

3.6 System Installation Requirements

3.6.1 Physical Installation Requirements

The physical devices comprising the Tartan system shall be installed as the following conditions.

CCTV Device

CCTV devices should be installed at the inside entrance of the server room. And the camera should be installed in the direction in which the entrants come in. It should be installed at the entrance where no people exist.

PC with the monitoring system running

It is installed in a controlled location, such as a situation room where no one other than Security Agents enters.

The PC used by the Monitoring system manager

It shall be installed in a controlled location, such as a situation room where no one other than the designated number of people enters.

3.6.2 Network Installation Requirements

The Tartan system should be installed in the following network environments.

- 802.11ac or higher specification, 100 Mbps or higher
- Where there is no jammer that interferes with wireless network use.
- The PC working with CCTV, monitoring system and monitoring system manager should be disconnected from the external network. At the very least, CCTV should be quarantined from the company's external network.

3.6.3 Product Configuration Installation Requirements

The device comprising the Tartan system shall comprise the following conditions.

CCTV Device

CCTV devices should be installed as the following components.

- cuda 10.2 + cudnn 8.0
- TensorRT 7.x
- OpenCV 4.1.1
- TensorFlow r1.14
- python3

In addition, CCTV S/W components should be installed according to the procedures of the installation guide below.
Be sure to refer to the "CCTV installation guide"

PC with the monitoring system running.

The following components must be installed on a PC running the monitoring system.

- OpenCV 4.5.1

In addition, the monitoring system S/W component must be installed according to the procedures in the installation guide below.
Be sure to refer to the "Monitoring system installation guide"

The PC used by the Monitoring system manager.

The PC used by the Monitoring System Manager must have the following S/W installed.

- ssh client
- scp client

Appendixes

Index