Project Goal

The purpose of the face recognition system is to monitor attendees of video conference systems and to manage known attendees by using face AI. Especially the system must be secured from any threats as specified.

Project Requirements

- Documentation describing the requirements for the CMU project.

Review result of “Project Requirements”

No comments

User requirements

- Document includes each specification of Functional, Non Functional, Implementation, Delivery and Security requirements.
- A total of six security requirements are defined as follows.
  (1) Ensure application architecture is secure
  (2) Ensure code is written and implemented in a secure manner
  (3) Ensure application network communication is secure
  (4) Practice finding security flaws in code / applications both statically and dynamically
  (5) Ensuring that all software in both applications are architected and coded to be secure and free of vulnerabilities.
  (6) Analyzing the provided initial implementation for vulnerabilities and developing solutions to mitigate.

Review result of “User requirements”

This document contains an analysis of Dan Plakosh's project information.

Software Requirement Specification

The Laptop client application connects to Jetson Nano server and the user can choose a communication mode as secure or insecure. Only an authenticated client can connect to the target server. Jetson Nano Server supplies image and amplified data of video conference attendees to client applications over the internet.

Use case

(1) Manage Authentication
(2) Control Communication Mode

(3) Execute Operation Live Mode
(4) Execute Operation Test Mode
(5) Execute Operation Learning Mode

Functional Requirements

(1) The client app shall have a user selection menu.
(2) The client app shall be able to change communication mode with the server app to secure mode.
(3) The client app shall be able to change communication mode with the server app to insecure mode.
(4) The client app shall be able to add new user images to the image database with a user-specified name.
(5) The client app shall be able to display camera video stream and face recognition results from the server app.
(6) The client app shall be able to receive video file streams and face recognition results from the server app with a user-specified filename.
(7) The client app shall be able to detect fault/error and then recover and report.

Quality Attribute Requirements

(1) Ensure application architecture is secure.
(2) Ensure code is written and implemented in a secure manner
(3) Ensure application network communication is secure
(4) Practice finding security flaws in code / applications both statically and dynamically
(5) Ensuring that all software in both applications are architected and coded to be secure and free of vulnerabilities
(6) Analyzing the provided initial implementation for vulnerabilities and developing solutions to mitigate.

Review result of “Software Requirement Specification”

Use case

- Test Mode is not supported in the final product. But the GUI has a playback menu and selecting it forces the Client program to shut down.

Functional Requirements

- The Client can select secure mode or secure mode to run. However, Client cannot change the mode again after disconnect.
- we couldn't find any implementations regarding FR7(The client app shall be able to detect fault/error and then recover and report)..

Quality Attribute Requirements

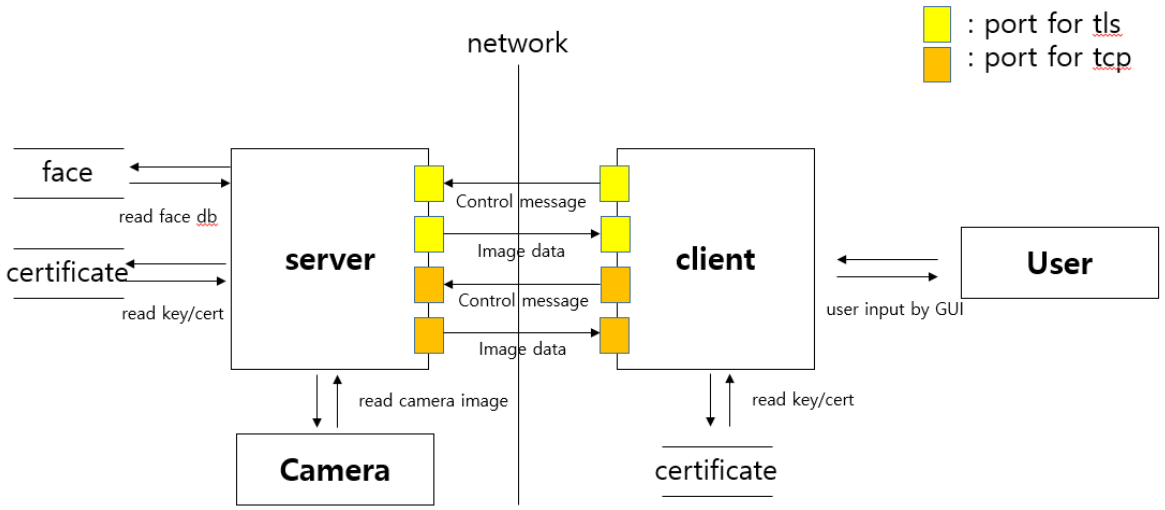
- Is there any verification material that the code is written securely?
- Static analysis data, etc.

Software Architecture Design

- Block diagram about software
- Layered Software Architecture
- Sequence diagram about connect/disconnect scenario

Review result of “Software Architecture Design”

- System view and data interaction between each module



Project Asset List

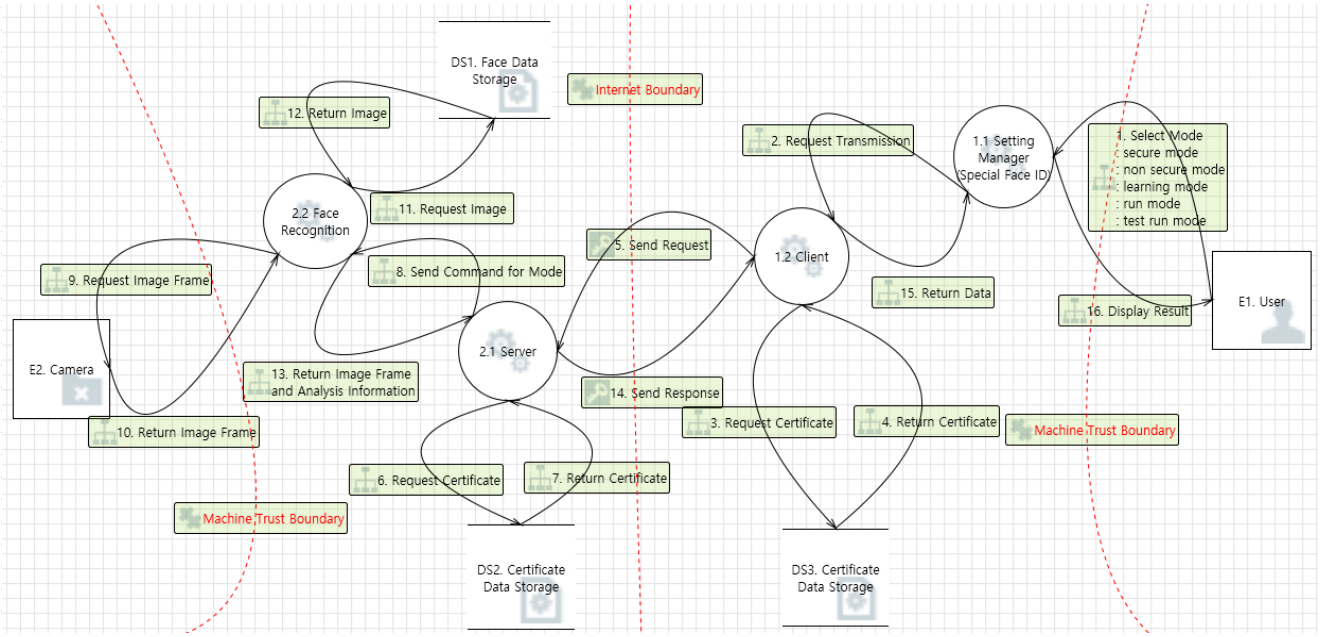
Document about project assets and each damage scenario.

Review result of “Project Asset List”

No comments

Threat Modeling

Team5 uses DFD tools of Microsoft to get thread lists.



There are 58 threats total.

Interaction	number of threat	category
User -> Settings Manager	10	Spoofing, Elevation Of Privilege, Denial Of Service, Information Disclosure, Repudiation, Tampering
Camera->Face Recognition	10	Spoofing, Elevation Of Privilege, Denial Of Service, Information Disclosure, Repudiation, Tampering
Face Recognition -> Face data storage	2	Spoofing, Denial Of Service
Face data storage -> Face recognition	2	Spoofing, Information Disclosure
Face recognition -> Server	1	Elevation Of Privilege
Server -> Client	8	Elevation Of Privilege, Denial Of Service, Spoofing
Client -> Settings Manager	1	Elevation Of Privilege
Settings	3	Denial Of Service, Spoofing, Repudiation

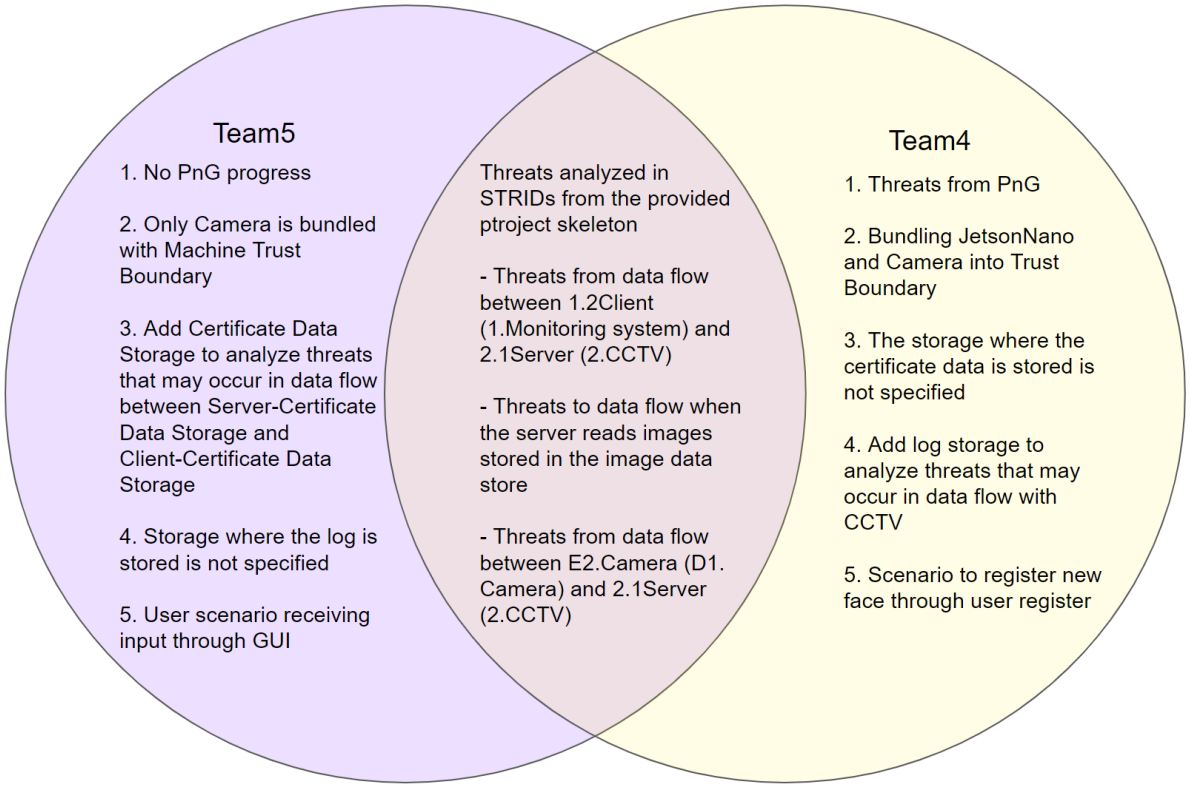
Manager -> User		
Settings Manager-> Client	1	Elevation Of Privilege
Client -> Certification Data Storage	2	Denial Of Service, Spoofing
Certification Data Storage -> Client	2	Spoofing, Information Disclosure
Client -> Server	8	Elevation Of Privilege, Denial Of Service, Spoofing, Repudiation
Server -> Certification Data Storage	2	Denial Of Service, Spoofing
Certification Data Storage -> Server	2	Spoofing, Information Disclosure
Server -> Face recognition	1	Elevation Of Privilege
Face recognition -> Camera	3	Denial Of Service, Spoofing, Denial Of Service

Review result of “Threat Modeling”

Many threats exist between clients and servers connected by network intervals. There are also many threats between CCTV and face recognition modules that go beyond the machine trust boundaries, and between settings managers that provide users and GUI.

Communication between the client and the server is represented by a data flow that communicates in https. Although it is not an actual method of communication for http, it appears to be represented by https data flow to represent cryptographic intervals with tls applied.

Comparing the threat modeling (e.g., Stride, PnG) we originally did in Phase 1 with the threat modeling done by Team 5.



Risk Assessment

Of the 58 threats, 45 threats were assessed.
After assessment about threats, the evaluation results for each threat are as follows.

Theat level	Number of count	Threat id
Critical	1	170
High	16	9, 13, 23, 118, 4, 6, 8, 10, 12, 20, 22, 24, 105, 98, 115, 98, 115, 169
Medium	4	106, 99, 117, 113
Low	10	1, 5, 110, 109, 103, 102, 122, 176, 175, 116
Unknown	14	2, 3, 14, 15, 25, 111, 104, 121, 172, 178, 179, 171, 177, 112

Reviewed OWASP Risk assessment written by 5 teams

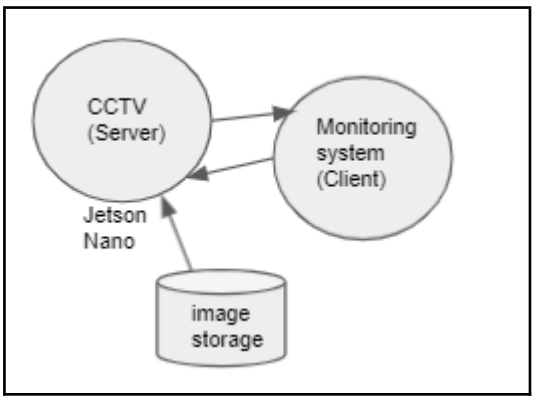
- https://docs.google.com/spreadsheets/d/1n4leAw5988FR0vAf-Oqep_eud3KlUM96sKL-zHnpHjE/edit?usp=sharing

- OWASP Risk assessment tab in document review_5team_Doc

Review result of “Risk Assessment”

- Some threats do not perform a risk assessment and do not explain why a risk assessment is not performed. (ID 2,3,14,15,25,111, 112, 121, 171, 172, 177, 178, 179)
- Some of the criteria listed as high cannot be traced to security requirements and mitigation. (TID 108, 107, 101, 100, 4, 24, 115, 169)
- Design is not considered for availability e.g.) after stopped or crashed, recovery is not working(100, 101, 107and 108 don’t mitigate.)

Comparing the vulnerability analysis we originally did in Phase 1 with the vulnerability analysis done by Team 5.



Threats	Team4	Team5
Threats from data flow between Monitoring system(Client) and CCTV(Server)	Mitigate with TLS	Mitigate with TLS
Threats to data flow when the server reads images stored in the image data store	1. Encryption algorithm uses AES-128 CBC mode. 2. Apply ACL to allow access only to CCTV accounts	cryptomount
Reputation-related threats	Connection/disconnection related and recognized person names logging	Logging only connection history
User input-related threats	-(no user input)	Apply input validation
Manage accounts with access to security assets	1. Separation of CCTV account and Monitoring system manager account 2. Apply ACL (CCTV account r/w/x, manager account -/-/-)	Admin account only

CCTV (Server) denial of service related threats	Isolate the network with CCTV, wireless router, and monitoring system.	-

Security Requirements

Finally, below security requirements are derived.There are a total of 14 security requirements in 6 categories.

Category	Security requirements ID	Security Requirments
Input Validation for Client Application	SR1-1	Client Application must check if the format of input IP address is in valid format
	SR1-2	Server and Client should check respectively whether the input for Username field on the Register mode is valid as a filename.
	SR1-3	Client should check if the input of the Port field is within the valid port number range.
	SR1-4	Server and client should check input validation respectively whether the input for video file name field on the Playback mode has video file format such as .mp4.
	SR1-5	Client should check whether the image recevied from server is format of jpeg before displaying it.
	SR1-6	Client should compare the number of detected face and the number of its information, which are received from server, and they should be same.
Secure Data Transmission	SR2-1	After connection establishment all the data transferred between server and client must be securely encrypted
	SR2-2	Must check integrity of all the transmitted data between server and client
Secure Authentication	SR3-1	Server and Client must mutually authenticate each other with X.509 certificates
Secure Data Store	SR4-1	Images and name of registered users must be stored in secure storage to prevent access from unauthorized users

	SR4-2	Root and CA certificates must be stored in secure storage
	SR4-3	Client certificates must be stored in secure storage
Logging	SR5-1	Server and client should leave the message about the connection status as a log, respectively.
Policy	SR6-1	Client Application should run on legitimate Windows with firewall and surveillance enabled.

Tested and reviewed test cases written by 5 teams

- https://docs.google.com/spreadsheets/d/1n4IeAw5988FR0vAf-Oqep_eud3KlUM96sKL-zHnpHjE/edit?usp=sharing
- Security RQ tab in document review_5team_Doc

Review result of “Security Requirements”

Threat Id 107’s analysis level is high but it is not included to security requirements.

- description : Client crashes, halts, stops or runs slowly; in all cases violating an availability metric.
- If a crash occurs in response to the server's response in the client, availability is low.
- In the final product, the client is crashed when service is not launched or ip address is wrong.

Threat Id 100’s analysis level is high but it is not included to security requirements.

- description : Server crashes, halts, stops or runs slowly; in all cases violating an availability metric.
- If a crash occurs in response to the client’s response in the client, availability is low.
- In final product, cctv is not working after trying invalid client connect to server
- It's missing a design that securely stores the client's certificate and private key required for mutual authentication. (they only assume that APIs are safe related to it.)

Test Cases

There are 20 test cases defined. But 5 test cases are deprecated because function is not implemented.

Tested and reviewed test cases written by 5 teams

- https://docs.google.com/spreadsheets/d/1n4IeAw5988FR0vAf-Oqep_eud3KlUM96sKL-zHnpHjE/edit?usp=sharing
- TestCase tab in document review_5team_Doc

Review result of “Test Cases”

Test cases are not defined about security requirement (SR1-3, SR3-1)
SR1-3 : Client should check if the input of the Port field is within the valid port number range.
SR3-1 : Server and Client must mutually authenticate each other with X.509 certificates

And when we test SR1-3 and SR3-1 there is a problem below.

SR 1-3 : There is no input port field. So there is an invalid requirement.
SR 3-1 :

Server	**Client**	**Result**
Valid cert	Invalid Cert	Connection failed. But after that Client can't connect to the Server even if has a valid cert. After attempting an abnormal connection, the server must be restarted to allow normal clients to connect.
Invalid Cert	Valid Cert	Connection failed.

- TC-01~20: There is a step that the written test step does not match. (radio button can be selected after pressing the click button but the steps are written in reverse.)
- TC-05 : It is not actually saved in the images folder when extremely long characters input. -> violate their test case
- TC-14 : Admin can access the Jetson Nano imgs directory and image file can see without encryption after move image files to personal laptop -> violate their test case

Conclusion

Goal of review	Review the documents created by the team5 and find vulnerabilities in them.
Review Process	Top-Down Approach (This approach identifies design vulnerabilities first, followed by logical implementation vulnerabilities and then low-level implementation vulnerabilities.)
Found Vulnerability	Mitigation methods for Denial Of Service are not considered in the risk assessment.
Exploit	DOS attack is possible because it does not recover when the server or client stops or crashes.
Risk	High risk because availability is violated