CMU Security Specialist Course

Team Project Phase 1

Six senses Team 6

Seongju Moon (L)

Kyungnam Bae (E)

Jinmo Kim (A)

Jeonghwan Ahn (S)

* Byungchul Park (C)


Mr. Bae
Mr. Kim
Mr. Park
Mr. Moon
Mr. Ahn

Define security goal

Define assets to protect

Do threat modeling

Do risk assessment to prioritize items

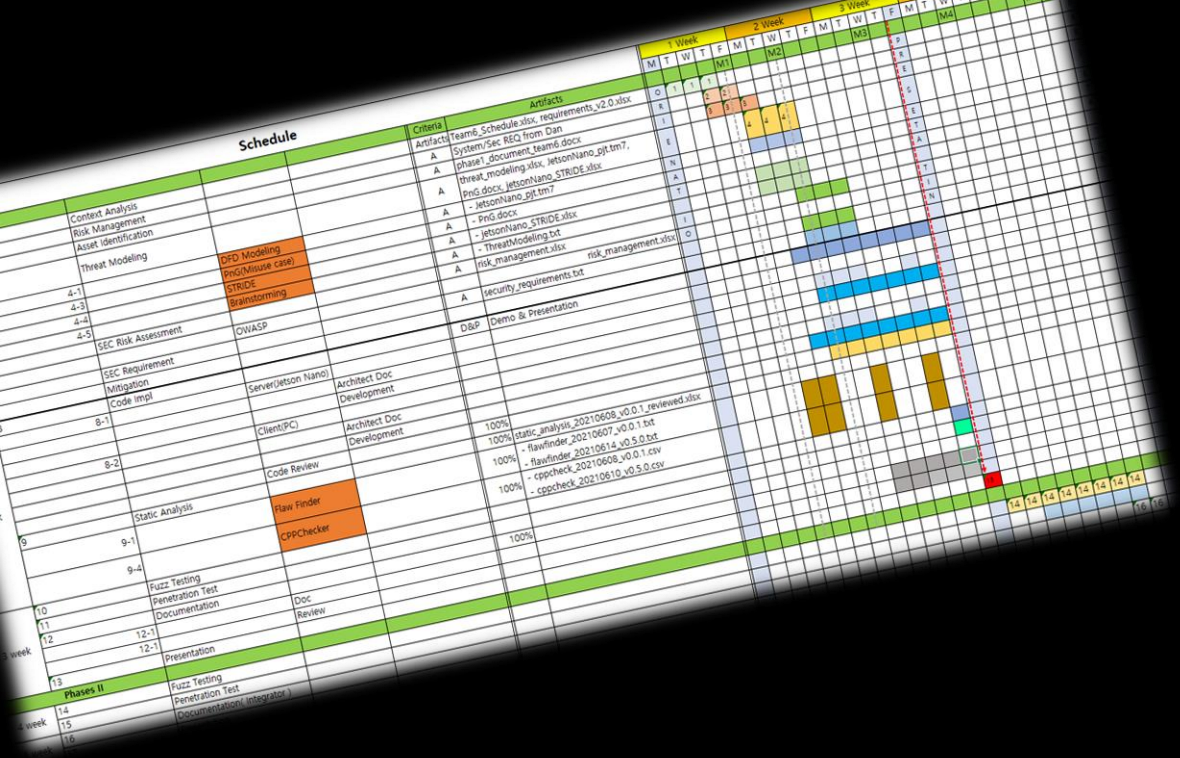
Define security requirements

Derive mitigations

Construct architecture

Implement the mitigations

Verify the mitigations



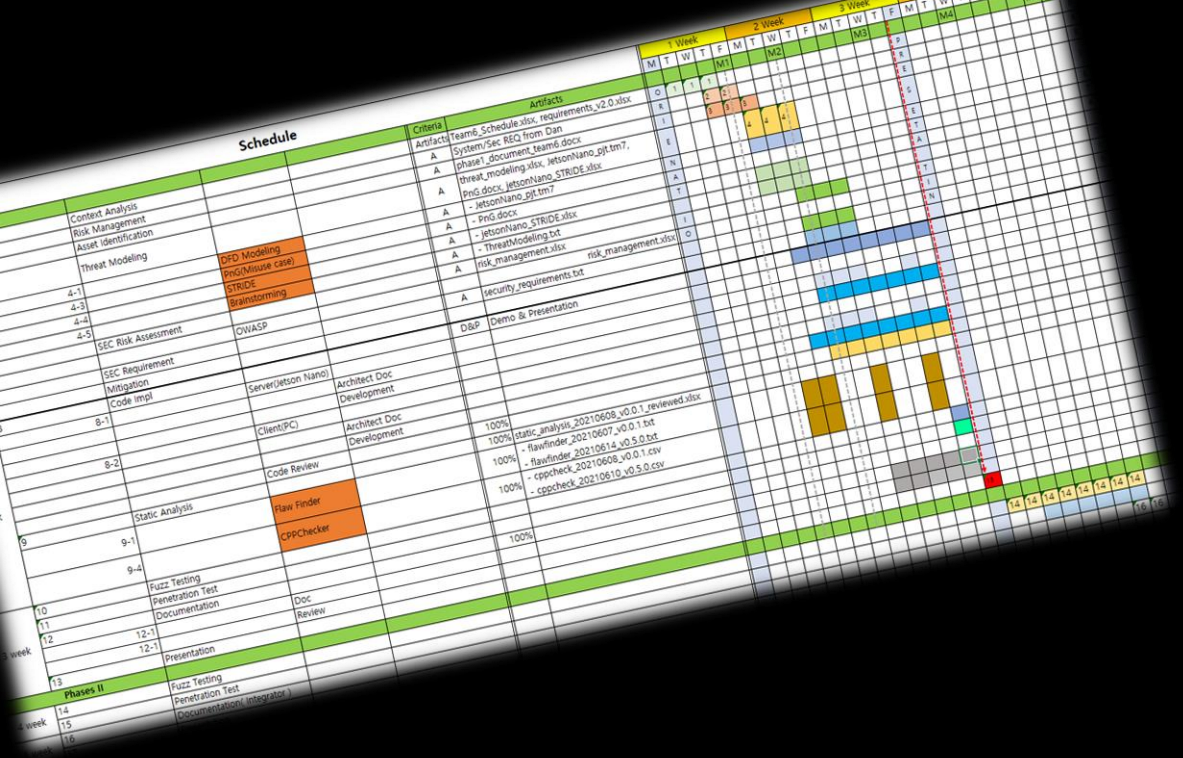
Schedule

					Criteria	Artifacts
	Context Analysis				Artifacts	Team6_Schedule.xlsx, requirements_v2.0.xlsx
	Risk Management				A	System/Sec REQ from Dan
	Asset Identification				A	phase1_document_team6.docx
	Threat Modeling	DFD Modeling			A	threat_modeling.xlsx, JetsonNano_pjt.tm7,
4-1		PnG(Misuse case)			A	PnG.docx, JetsonNano_STRIDE.xlsx
4-3		STRIDE			A	- JetsonNano_pjt.tm7
4-4		Brainstorming			A	- PnG.docx
4-5	SEC Risk Assessment	OWASP			A	- JetsonNano_STRIDE.xlsx
	SEC Requirement				A	- ThreatModeling.txt
	Mitigation				A	risk_management.xlsx
	Code impl	Server(Jetson Nano)	Architect Doc		A	risk_management.xlsx
8-1			Development		A	security_requirements.txt
		Client(PC)	Architect Doc			
8-2			Development		D&P	Demo & Presentation
		Code Review				
	Static Analysis	Flaw Finder		100%		
9 9-1		CPPChecker		100%	static_analysis_20210608_v0.0.1_reviewed.xlsx	
9-4	Fuzz Testing			100%	- flawfinder_20210607_v0.0.1.txt - flawfinder_20210614_v0.5.0.txt	
10	Penetration Test			100%	- cppcheck_20210608_v0.0.1.csv - cppcheck_20210610_v0.5.0.csv	
11	Documentation	Doc				
12		Review		100%		
12-1						
12-3	Presentation					
13	Fuzz Testing					
Phases II 14	Penetration Test					
15	Documentation(Integrator)					
16						

1 Week 2 Week 3 Week

M1 M2 M3 M4

14 14 14 14 14 14 14 14 14 14 16 16



Requirements of Secure Coding Training Program, Project Description-1,2,3

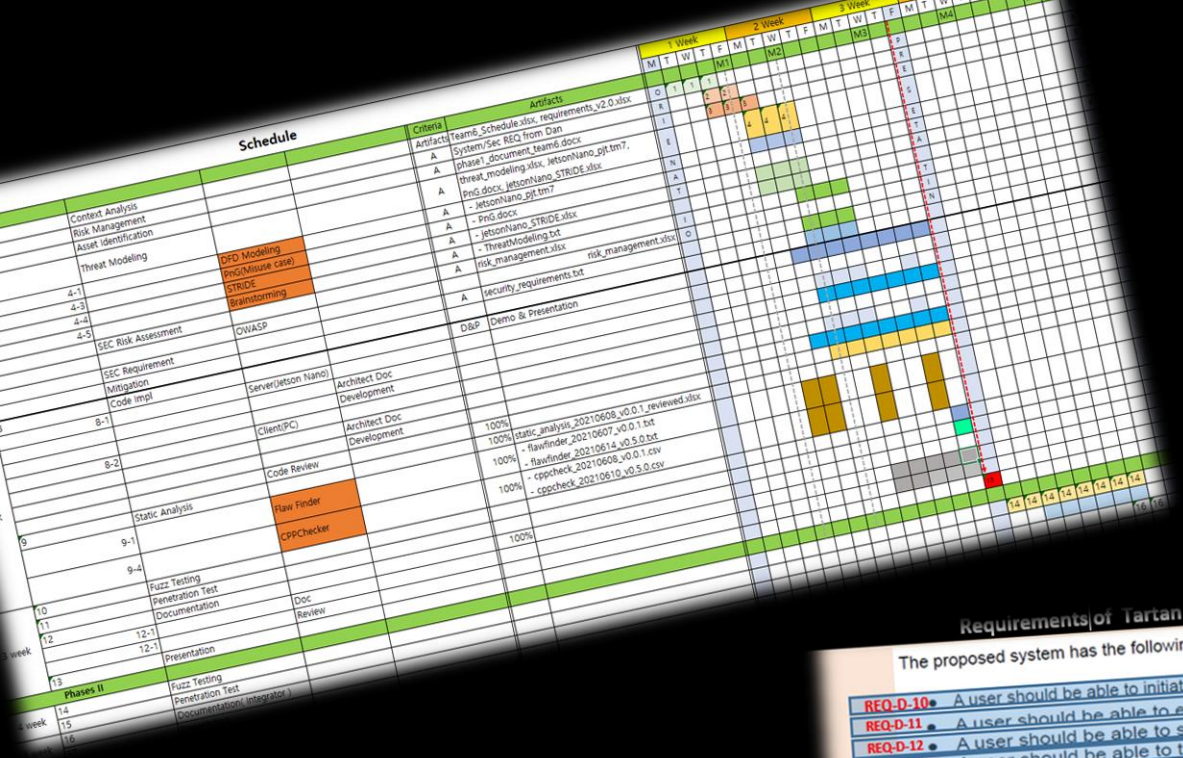
The user display and system control application is responsible for the following:

1. Establishing secure and authenticated communication with the camera and image analysis application and user interface when secure mode is selected or requested. — REQ-D-01
2. Provides the user interface to control the system. User interface shall support the following modes of operation: — REQ-D-02
   a) Secure or non secure mode of communication. — REQ-D-03
   b) Learning Mode - User images can be added to the image database. In this mode the interface should query for the name of the person in front of the camera and the number of samples to be collected. — REQ-D-04
   c) Run Mode – System utilizes camera to identify faces and perform facial recognition. — REQ-D-05
   d) Test Run Mode – System utilizes a video file to identify faces and perform facial recognition. — REQ-D-06
3. Communicating with the camera and image analysis application as specified. — REQ-D-07
4. Display image frames and any accompanying amplifying analysis information received from the camera and image analysis application in the format specified.

Project Responsibilities

1. Implementing the specified enhancements to the applications — additional consideration
2. Ensuring that all software in both applications are architected and coded to be secure and free of vulnerabilities. — REQ-Q-01, REQ-Q-02
3. Modifying the implementation so the applications support two modes of communications: 1) a secure mode with all data properly encrypted (including authentication) and 2) a plain text mode without encryption. — REQ-D-08, REQ-D-09
4. Proper fault/error detection, recovery, and reporting. — REQ-Q-03
5. Analyzing the provided initial implementation for vulnerabilities and developing solutions to mitigate. — REQ-Q-04, REQ-Q-05
6. Analyze another team's implementation assigned to you for security flaws and vulnerabilities. — Phase 2

* reference : LG May 2021 Lecture Secure Coding Project Intro V1.1.pptx.pdf



Schedule

				Criteria	Artifacts
	Context Analysis			Artifacts	Team6_Schedule.xlsx, requirements_v2.0.xlsx
	Risk Management			A	System/Sec REQ from Dan
	Asset Identification			A	phase1_document_team6.docx
	Threat Modeling	DFD Modeling		A	threat_modeling.xlsx, JetsonNano_pjt.tm7,
4-1		PnG(Misuse case)		A	PnG.docx, JetsonNano_STRIDE.xlsx
4-3		STRIDE		A	- JetsonNano_pjt.tm7
4-4		Brainstorming		A	- PnG.docx
4-5	SEC Risk Assessment	OWASP		A	- JetsonNano_STRIDE.xlsx
	SEC Requirement			A	- JetsonNano.txt
	Mitigation			A	- ThreatModeling.txt
	Code Impl	Server(Jetson Nano)	Architect Doc	A	risk_management.xlsx
8-1			Development	A	risk_management.xlsx
		Client(PC)	Architect Doc	A	security_requirements.txt
8-2			Development		
		Code Review		D&P	Demo & Presentation
	Static Analysis	Flaw Finder			
9 9-1		CPPChecker			
9-4	Fuzz Testing				
10	Penetration Test				
11	Documentation	Doc			
12 12-1		Review			
12-1	Presentation				
13					
Phases II	Fuzz Testing				
14	Penetration Test				
15	Documentation(Integrator)				
16					

	Artifacts
100%	static_analysis_20210608_v0.0.1_reviewed.xlsx
100%	static_analysis_20210607_v0.0.1.txt
100%	- flawfinder_20210614_v0.5.0.txt
100%	- flawfinder_20210608_v0.0.1.csv
	- cppcheck_20210610_v0.5.0.csv
100%	

1 Week 2 Week 3 Week M1 M2 M3 M4

Requirements of Secure Coding Training Program, Project Description-1,2,3

The user display and system control application is responsible for the following:

1. Establishing secure and authenticated communication with the camera and image analysis application and user interface when secure mode is selected or requested. REQ-D-01
2. Provides the user interface to control the system. User interface shall support the following modes of operation: REQ-D-02
   a) Secure or non secure mode of communication. REQ-D-03
   b) Learning Mode - User images can be added to the image database. In this mode the interface should query for the name of the person in front of the camera and the number of samples to be collected. REQ-D-04
   c) Run Mode – System utilizes camera to identify faces and perform facial recognition. REQ-D-05
   d) Test Run Mode – System utilizes a video file to identify faces and perform facial recognition. REQ-D-06
3. Communicating with the camera and image analysis application as specified.
4. Display image frames and any accompanying amplifying analysis information received from the camera and image analysis application in the format specified. REQ-D-07

Project Responsibilities

1. Implementing the specified enhancements to the applications additional consideration
   REQ-Q-01 Ensuring that all software in both applications are architected and coded to be secure and free of vulnerabilities.
   REQ-Q-02 odifying the implementation so the applications support two des of communications: 1) a secure mode with all data perly encrypted (including authentication) and 2) a plain text e without encryption. REQ-D-09
   er fault/error detection, recovery, and reporting.
   yzing the provided initial implementation for vulnerabilities eveloping solutions to mitigate.
   ze another team's implementation assigned to you for y flaws and vulnerabilities. Phase 2

: LG May 2021 Lecture Secure Coding Project Intro V1.1.pptx.pdf

Requirements of Tartan Secure Camera Application

The proposed system has the following basic functional requirements. Note

REQ-D-10 • A user should be able to initiate a video feed, end a feed.
REQ-D-11 • A user should be able to end a video feed.
REQ-D-12 • A user should be able to save a video feed for offline review.
REQ-D-13 • A user should be able to tune image analysis.

The system also has the following architectural concerns (i.e. quality attributes)

REQ-Q-06 • Performance: The system must deliver video as close to real time as possible, especially in real-time mode.

REQ-D-14 • Authentication:The system must use two factor authentication for sign on and
REQ-D-15 user credentials must be protected. Lost or compromised credentials must be handled in a reasonable way. REQ-D-16

REQ-D-17 • Communication privacy: When in the desired mode the system must ensure that data sent to a user remains private while in transit. No intermediary should be able to snoop or spy on an ongoing video feed.

REQ-D-18 • Proof of identity (nonrepudiation): Users should be confident that the camera they are using is the one that they believe it is.

REQ-D-19 • Multi-user privacy: The system must ensure that multiple video feeds remain private between the intended users.

REQ-D-20 • reliability: The system must ensure that video is reliably delivered. The system
REQ-D-21 should recover from networking errors as soon as possible. The goal is to maintain a secure, performant connection at all costs.

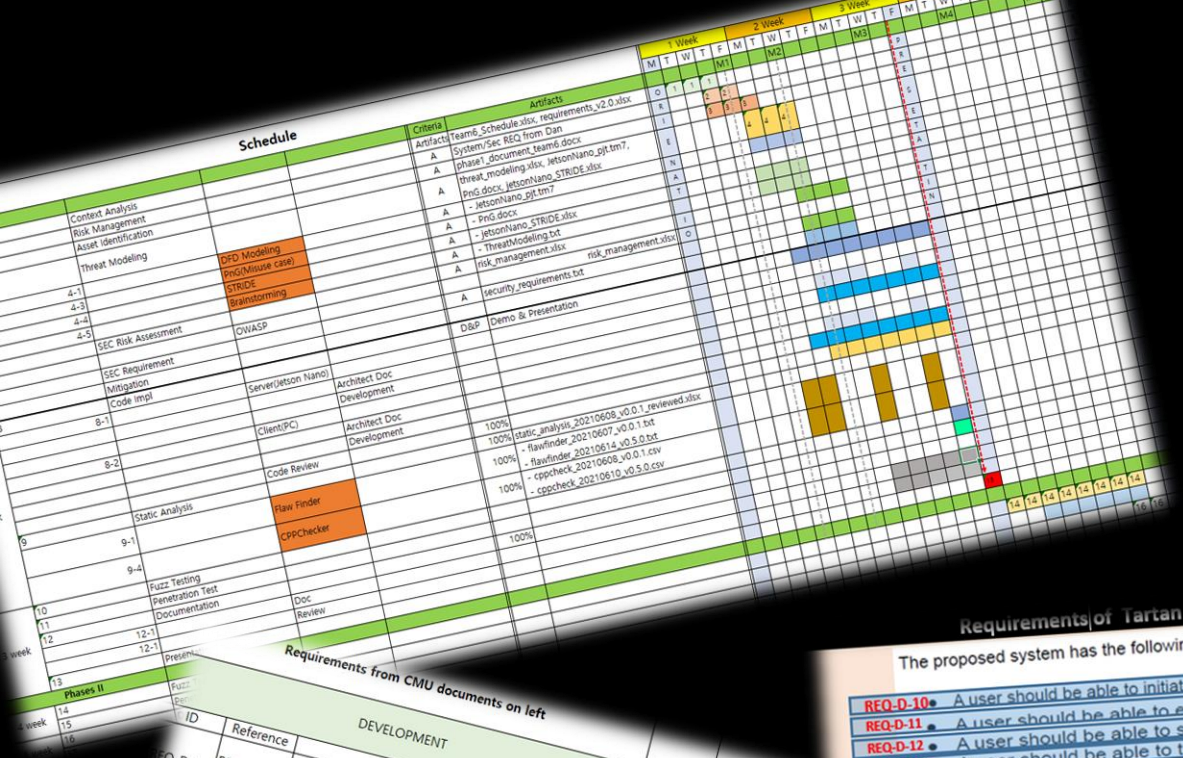
Aside from these requirements, there are a number of basic quality concerns that must be addressed during development.

REQ-Q-07 1. Ensuring that **all software** in both applications are architected and coded to be secure and free of vulnerabilities.

REQ-Q-08 2. Conduct proper fault/error detection, recovery and reporting.
???

REQ-Q-09 3. Ensure the developed software adheres to the company coding standard and

REQ-Q-10 quality standards.



Schedule

				Criteria	Artifacts
	Context Analysis			Artifacts	Team6_Schedule.xlsx, requirements_v2.0.xlsx
	Risk Management			A	System/Sec REQ from Dan
	Asset Identification			A	phase1_document_team6.docx
	Threat Modeling	DFD Modeling		A	threat_modeling.xlsx, JetsonNano_pjt.tm7,
4-1		PnG(Misuse case)		A	threat_modeling.xlsx, JetsonNano_STRIDE.xlsx
4-3		STRIDE		A	PnG.docx, JetsonNano_pjt.tm7
4-4		Brainitorming		A	- JetsonNano_pjt.tm7
4-5	SEC Risk Assessment	OWASP		A	- PnG.docx
	SEC Requirement			A	- JetsonNano_STRIDE.xlsx
	Mitigation			A	- ThreatModeling.txt
	Code Impl	Server(Jetson Nano)	Architect Doc	A	risk_management.xlsx
8-1			Development		risk_management.xlsx
		Client(PC)	Architect Doc	A	security_requirements.txt
8-2			Development		
		Code Review		D&P	Demo & Presentation
	Static Analysis	Flaw Finder			
9 9-1		CPPChecker		100%	
9-4	Fuzz Testing			100%	static_analysis_20210608_v0.0.1_reviewed.xlsx
	Penetration Test			100%	- flawfinder_20210607_v0.1.txt
10	Documentation	Doc		100%	- flawfinder_20210614_v0.5.0.txt
11		Review		100%	- cppcheck_20210608_v0.0.1.csv
12 12-1					- cppcheck_20210610_v0.5.0.csv
12-1				100%	
19	Presen				

Phases II

1 Week 2 Week 3 Week

M1 M2 M3 M4

Requirements of Secure Coding Training Program, Project Description-1,2,3

The user display and system control application is responsible for the following:

1. Establishing secure and authenticated communication with the camera and image analysis application and user interface when secure mode is selected or requested.
2. Provides the user interface to control the system. User interface shall support the following modes of operation:
   a) Secure or non secure mode of communication.
   b) Learning Mode - User images can be added to the image database. In this mode the interface should query for the name of the person in front of the camera and the number of samples to be collected.
   c) Run Mode – System utilizes camera to identify faces and perform facial recognition.
   d) Test Run Mode – System utilizes a video file to identify faces and perform facial recognition.
3. Communicating with the camera and image analysis application as specified.
4. Display image frames and any accompanying amplifying analysis information received from the camera and image analysis application in the format specified.

REQ-D-01 REQ-D-02 REQ-D-03 REQ-D-04 REQ-D-05 REQ-D-06 REQ-D-07

Project Responsibilities

1. Implementing the specified enhancements to the applications additional consideration
2. Ensuring that all software in both applications are architected and coded to be secure and free of vulnerabilities.
3. Modifying the implementation so the applications support two modes of communications: 1) a secure mode with all data properly encrypted (including authentication) and 2) a plain text mode without encryption. REQ-D-09
4. Performing fault/error detection, recovery, and reporting.
5. Analyzing the provided initial implementation for vulnerabilities and developing solutions to mitigate.
6. Analyze another team's implementation assigned to you for security flaws and vulnerabilities.

REQ-Q-01 REQ-Q-02

Phase 2

: LG May 2021 Lecture Secure Coding Project Intro V1.1.pptx.pdf

Requirements of Tartan Secure Camera Application

The proposed system has the following basic functional requirements. Note

REQ-D-10 • A user should be able to initiate a video feed, end a feed.
REQ-D-11 • A user should be able to end a video feed
REQ-D-12 • A user should be able to save a video feed for offline review
REQ-D-13 • A user should be able to tune image analysis.

The system also has the following architectural concerns (i.e. quality attributes)

Re-define Requirement from REQ08: The system must deliver video as close to real time as possible, ...al-time mode.

Finalize REQs with DAN

To Do (excluding req of an Architecure Doc)

...use two factor authentication for sign on and ...t or compromised credentials must be ...

... mode the system must ensure that ... transit. No intermediary should be ...feed.

...should be confident that the camera ...e it is.

...ensure that multiple video feeds remain ...

...that video is reliably delivered. The system ...rors as soon as possible. The goal is to ...nnection at all costs.

...are a number of basic quality concerns that must ...

... both applications are architected and coded to be ...ities

... detection, recovery and reporting.

...oftware adheres to the company coding standard and ...

Requirements from CMU documents on left

Merged the duplicated 'REQ-*' to 'CMU-REQ-*'

ID	Reference	DEVELOPMENT Description	
CMU-REQ-D-01	REQ-D-02 REQ-D-03	Establishing connection between Client and Server	Mandatory
CMU-REQ-D-02		Support Secure Mode	Mandatory
CMU-REQ-D-03		Support Non Secure Mode	Mandatory
CMU-REQ-D-04		Support Learning Mode - Register new person to the Server	Mandatory
CMU-REQ-D-05		Support Run Mode - System identifies faces and performs facial recognition	Mandatory
CMU-REQ-D-06	REQ-D-02	Support Test Run Mode - A user should be able to tune image analysis with local file	Mandatory
CMU-REQ-D-07	REQ-D-03	Display Result - Face-recognized images	Mandatory
CMU-REQ-D-08	REQ-D-02 REQ-D-03	A user should be able to save a video feed for offline review	Excluded
CMU-REQ-D-09	REQ-D-06	The system must use 2FA	Mandatory
CMU-REQ-D-10		User credentials must be protected	Mandatory
CMU-REQ-D-11	REQ-D-02	Lost or compromised credentials must be handled in a reasonable way	Excluded
CMU-REQ-D-12		Wiretapping, Users should be confident that the camera they are using is the one that they believe it is	Excluded
CMU-REQ-D-13		Multi-user Privacy , multiple video feeds remain private between the users	Excluded
CMU-REQ-D-14		Reliability, the video is reliably delivered.	

ID	DEVELOPMENT Description
CMU-REQ-D-01	Establishing connection between Client and Server
CMU-REQ-D-02	A user should be able to initiate a video feed, and a feed in Support Secure Mode
CMU-REQ-D-03	A user should be able to initiate a video feed, and a feed in Support Non Secure Mode
CMU-REQ-D-04	Support Learning Mode - Register new person to the Server
CMU-REQ-D-05	Support Run Mode - System identifies faces and performs facial recognition
CMU-REQ-D-06	Support Test Run Mode - A user should be able to tune image analysis with local file
CMU-REQ-D-07	Display Result - Face-recognized images
CMU-REQ-D-08	A user should be able to save a video feed for offline review
CMU-REQ-D-09	The system must use 2FA
CMU-REQ-D-10	User credentials must be protected
CMU-REQ-D-11	Lost or compromised credentials must be handled in a reasonable way
CMU-REQ-D-12	Wiretapping, Users should be confident that the camera they are using is the one that they believe it is
CMU-REQ-D-13	Multi-user Privacy , multiple video feeds remain private between the users
CMU-REQ-D-14	Reliability, the video is reliably delivered.

Schedule

				Criteria	Artifacts
	Context Analysis			Artifacts	Team6_Schedule.xlsx, requirements_v2.0.xlsx
	Risk Management			A	System/Sec REQ from Dan
	Asset Identification			A	phase1_document_team6.docx
	Threat Modeling	DFD Modeling		A	threat_modeling.xlsx, JetsonNano_pjt.tm7,
		PnG(Misuse case)		A	PnG.docx, JetsonNano_STRIDE.xlsx
4-1		STRIDE		A	- JetsonNano_pjt.tm7
4-3		Brainitorming		A	- PnG.docx
4-4				A	- JetsonNano_STRIDE.xlsx
4-5	SEC Risk Assessment	OWASP		A	- ThreatModeling.txt
	SEC Requirement			A	risk_management.xlsx
	Mitigation			A	risk_management.xlsx
	Code Impl	Server(Jetson Nano)	Architect Doc	A	security_requirements.txt
8-1			Development		
		Client(PC)	Architect Doc	D&P	Demo & Presentation
8-2			Development		
		Code Review		100%	
	Static Analysis	Flaw Finder		100%	static_analysis_20210608_v0.0.1_reviewed.xlsx
9	9-1	CPPChecker		100%	- flawfinder_20210607_v0.1.txt
	9-4			100%	- flawfinder_20210614_v0.5.0.txt
	Fuzz Testing			100%	- cppcheck_20210608_v0.0.1.csv
	Penetration Test				- cppcheck_20210610_v0.5.0.csv
10	Documentation	Doc		100%	
11		Review			
12	12-1				
	12-1				
13	Presen...				

Phases II

1 Week | 2 Week | 3 Week

M1 M2 M3 M4

14 14 14 14 14 14 14 14 14 14 14 14 14 14 16 16

Requirements of Secure Coding Training Program, Project Description-1,2,3

The user display and system control application is responsible for the following:

1. Establishing secure and authenticated communication with the camera and image analysis application and user interface when secure mode is selected or requested.
2. Provides the user interface to control the system. User interface shall support the following modes of operation:
   a) Secure or non secure mode of communication.
   b) Learning Mode - User images can be added to the image database. In this mode the interface should query for the name of the person in front of the camera and the number of samples to be collected.
   c) Run Mode – System utilizes camera to identify faces and perform facial recognition.
   d) Test Run Mode – System utilizes a video file to identify faces and perform facial recognition.
3. Communicating with the camera and image analysis application as specified.
4. Display image frames and any accompanying amplifying analysis information received from the camera and image analysis application in the format specified.

REQ-D-01
REQ-D-02
REQ-D-03
REQ-D-04
REQ-D-05
REQ-D-06
REQ-D-07

Project Responsibilities

1. Implementing the specified enhancements to the applications additional consideration
2. Ensuring that all software in both applications are architected and coded to be secure and free of vulnerabilities.
3. Modifying the implementation so the applications support two modes of communications: 1) a secure mode with all data properly encrypted (including authentication) and 2) a
4. Performing fault/error detection, recovery, and re
5. Analyzing the provided initial implement
6. Developing solutions to mitigat
7. Analyze another team's impl
8. Identify flaws and vulnera

REQ-Q-01
REQ-Q-02

Requirements from CMU documents on left

ID	Reference	DEVELOPMENT Description
REQ-D-01	REQ-D-02 REQ-D-03	Establishing connection between Client and Server
REQ-D-02		Support Secure Mode
REQ-D-03		Support Non Secure Mode
REQ-D-04		Support Learning Mode - Register new person to the Server
REQ-D-05		Support Run Mode - System identifies faces and performs facial recognition
REQ-D-06		Support Test Run Mode
REQ-D-07		Display Result - Face-recognized images
REQ-D-08	REQ-D-02	
REQ-D-09	REQ-D-03	
REQ-D-10	REQ-D-02 REQ-D-03	A user should be able to initiate a video feed, end a feed
REQ-D-11	REQ-D-02 REQ-D-03	A user should be able to end a video feed
REQ-D-12		A user should be able to save a video feed for offline review
REQ-D-13	REQ-D-06	A user should be able to tune image analysis
REQ-D-14		The system must use 2FA
REQ-D-15		User credentials must be protected
REQ-D-16		Lost or compromised credentials must be handled in a reasonable way
REQ-D-17	REQ-D-02	Data send to a user remains private while in transit. No intermediary to be snoop or spy
REQ-D-18		Noninpudiation. Users should be confident that the camera they are using is the one that they believe it is
REQ-D-19		Multi-user Privacy , multiple video feeds remain private between the users
REQ-D-20		Reliability, the video is reliably delivered.

Requirements of Tartan Secure Camera Application

The proposed system has the following basic functional requirements. Note

REQ-D-10 • A user should be able to initiate a video feed, end a feed.
REQ-D-11 • A user should be able to end a video feed
REQ-D-12 • A user should be able to save a video feed for offline review
REQ-D-13 • A user should be able to tune image analysis.

The system also has the following architectural concerns (i.e. quality attributes)

Re-define Requirement from REQ-D: The system must deliver video as close to real time as possible, ...al-time mode.

Merged the duplicated 'REQ-*' to 'CMU-REQ-*'

ID	DEVELOPMENT Description	
CMU-REQ-D-01	Establishing connection between Client and Server	Mandatory
CMU-REQ-D-02	A user should be able to initiate a video feed, and a feed in Support Secure Mode	Mandatory
CMU-REQ-D-03	A user should be able to initiate a video feed, and a feed in Support Non Secure Mode	Mandatory
CMU-REQ-D-04	Support Learning Mode - Register new person to the Server	Mandatory
CMU-REQ-D-05	Support Run Mode - System identifies faces and performs facial recognition	Mandatory
CMU-REQ-D-06	Support Test Run Mode - A user should be able to tune image analysis with local file	Mandatory
CMU-REQ-D-07	Display Result - Face-recognized images	Mandatory
CMU-REQ-D-08	A user should be able to save a video feed for offline review	Excluded
CMU-REQ-D-09	The system must use 2FA	Mandatory
CMU-REQ-D-10	User credentials must be protected	Mandatory
CMU-REQ-D-11	Lost or compromised credentials must be handled in a reasonable way	Excluded
CMU-REQ-D-12	Noninpudiation. Users should be confident that the camera they are using is the one that they believe it is	Excluded
CMU-REQ-D-13	Multi-user Privacy , multiple video feeds remain private between the users	Excluded
CMU-REQ-D-14	Reliability, the video is reliably delivered.	

Finalize REQs with DAN

To Do (excluding req of an Architecure Doc)

...use two factor authentication for sign on and ...or compromised credentials must be ...

...mode the system must ensure that ... transit. No intermediary should be ... feed.

...should be confiden... ...e it is.

...ensure that multiple vide...

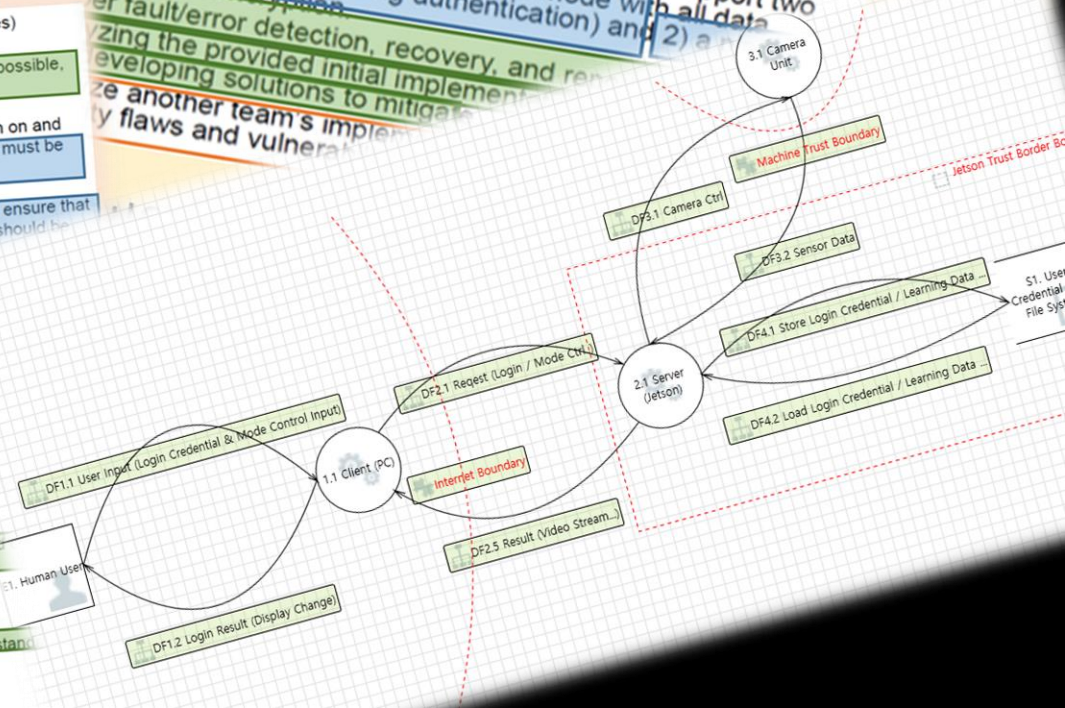
...that video is reliably deliver... ...rors as soon as possible. The ...nnection at all costs.

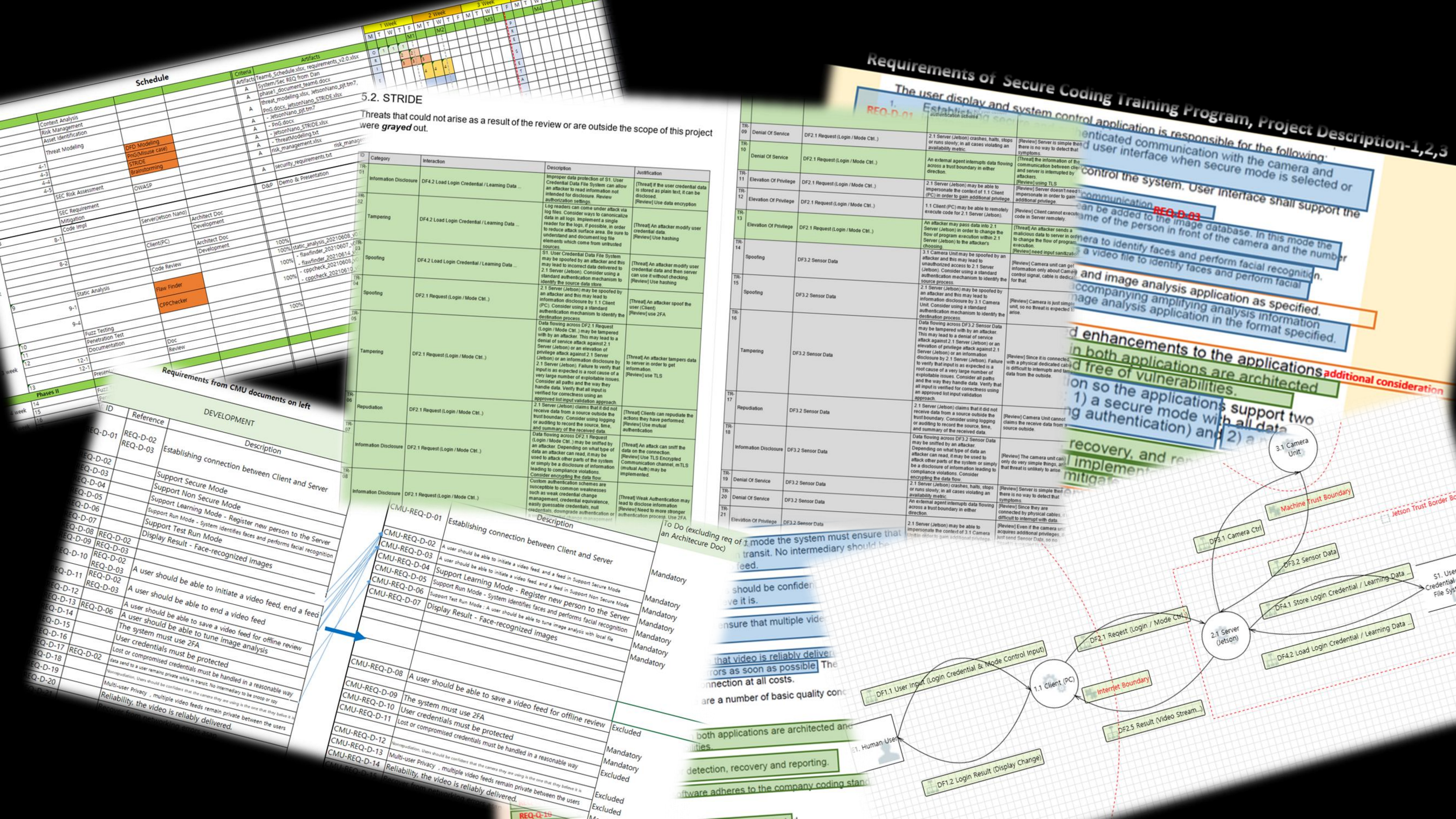
...are a number of basic quality conc...

...both applications are architected and ...ities

...detection, recovery and reporting.

...oftware adheres to the company coding stand...




Schedule
5.2. STRIDE
Threats that could not arise as a result of the review or are outside the scope of this project were grayed out.
Requirements of Secure Coding Training Program, Project Description-1,2,3
Requirements from CMU documents on left
DEVELOPMENT
Establishing connection between Client and Server
Support Secure Mode
Support Non Secure Mode
Support Learning Mode - Register new person to the Server
Support Test Run Mode
Display Result - Face-recognized images
A user should be able to initiate a video feed, end a feed
A user should be able to end a video feed
A user should be able to save a video feed for offline review
A user should be able to tune image analysis
The system must use 2FA
User credentials must be protected
Lost or compromised credentials must be handled in a reasonable way
Multi-user Privacy , multiple video feeds remain private between the users
Reliability, the video is reliably delivered.
additional consideration
3.1 Camera Unit
Machine Trust Boundary
Jetson Trust Border Boundary
DF3.1 Camera Ctrl
DF3.2 Sensor Data
DF4.1 Store Login Credential / Learning Data ...
DF4.2 Load Login Credential / Learning Data ...
DF2.1 Reqest (Login / Mode Ctrl.)
2.1 Server (Jetson)
1.1 Client (PC)
Internet Boundary
DF1.1 User Input (Login Credential & Mode Control Input)
DF2.5 Result (Video Stream...)
DF1.2 Login Result (Display Change)
S1. Human User

Schedule

				Criteria	Artifacts
	Context Analysis			Artifacts	Team6_Schedule.xlsx, requirements_v2.0.xlsx
	Risk Management			A	System/Sec REQ from Dan
	Asset Identification			A	phase1_document_team6.docx
	Threat Modeling	DFD Modeling		A	threat_modeling.xlsx, JetsonNano_pit.tm7,
		PnG(Misuse case)		A	threat_modeling.xlsx, JetsonNano_STRIDE.xlsx
		STRIDE		A	PnG.docx, JetsonNano_pit.tm7
		Brainitorming		A	- JetsonNano_pit.tm7
				A	- PnG.docx
	SEC Risk Assessment	OWASP		A	- JetsonNano_STRIDE.xlsx
	SEC Requirement			A	- ThreatModeling.txt
	Mitigation	Server(Jetson Nano)	Architect Doc	A	risk_management.xlsx
	Code Impl		Development	A	security_requirements.txt
		Client(PC)	Architect Doc	D&P	Demo & Presentation
			Development		
	Code Review			100%	
		Flaw Finder		100%	static_analysis_20210608_
	Static Analysis			100%	- flawfinder_20210607_
		CPPChecker			- flawfinder_20210614_
				100%	- cppcheck_20210608_
					- cppcheck_20210610_
	Fuzz Testing			100%	
	Penetration Test				
	Documentation	Doc			
		Review			
	Presentation				

Phases II

5.2. STRIDE

Threats that could not arise as a result of the review or are outside the scope of this project were ***grayed*** out.

ID	Category	Interaction	Description	Justification
TR-01	Information Disclosure	DF4.2 Load Login Credential / Learning Data ...	Improper data protection of S1. User Credential Data File System can allow an attacker to read information not intended for disclosure. Review authorization settings.	[Threat] If the user credential data is stored as plain text, it can be disclosed. [Review] Use data encryption
TR-02	Tampering	DF4.2 Load Login Credential / Learning Data ...	Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources.	[Threat] An attacker modify user credential data. [Review] Use hashing
TR-03	Spoofing	DF4.2 Load Login Credential / Learning Data ...	S1. User Credential Data File System may be spoofed by an attacker and this may lead to incorrect data delivered to 2.1 Server (Jetson). Consider using a standard authentication mechanism to identify the source data store.	[Threat] An attacker modify user credential data and then server can use it without checking. [Review] Use hashing
TR-04	Spoofing	DF2.1 Request (Login / Mode Ctrl..)	2.1 Server (Jetson) may be spoofed by an attacker and this may lead to information disclosure by 1.1 Client (PC). Consider using a standard authentication mechanism to identify the destination process.	[Threat] An attacker spoof the user (Client) [Review] use 2FA
TR-05	Tampering	DF2.1 Request (Login / Mode Ctrl..)	Data flowing across DF2.1 Request (Login / Mode Ctrl..) may be tampered with by an attacker. This may lead to a denial of service attack against 2.1 Server (Jetson) or an elevation of privilege attack against 2.1 Server (Jetson) or an information disclosure by 2.1 Server (Jetson) . Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	[Threat] An attacker tampers data to server in order to get information. [Review] use TLS
TR-06	Repudiation	DF2.1 Request (Login / Mode Ctrl..)	2.1 Server (Jetson) claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	[Threat] Clients can repudiate the actions they have performed. [Review] Use mutual authentication
TR-07	Information Disclosure	DF2.1 Request (Login / Mode Ctrl..)	Data flowing across DF2.1 Request (Login / Mode Ctrl..) may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	[Threat] An attack can sniff the data on the connection. [Review] Use TLS Encrypted Communication channel, mTLS (mutual Auth) may be implemented.
TR-08	Information Disclosure	DF2.1 Request (Login / Mode Ctrl..)	Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or	[Threat] Weak Authentication may lead to disclose information [Review] Need to more stronger authentication process. Use 2FA

Requirements from CMU documents on left

ID	Reference	DEVELOPMENT Description
CMU-REQ-D-01	REQ-D-02 REQ-D-03	Establishing connection between Client and Server
CMU-REQ-D-02		Support Secure Mode
CMU-REQ-D-03		Support Non Secure Mode
CMU-REQ-D-04		Support Learning Mode - Register new person to the Server
CMU-REQ-D-05		Support Run Mode - System identifies faces and performs facial recognition
CMU-REQ-D-06	REQ-D-02	Support Test Run Mode
CMU-REQ-D-07	REQ-D-03	Display Result - Face-recognized images
CMU-REQ-D-08	REQ-D-02 REQ-D-03	A user should be able to initiate a video feed, end a feed
CMU-REQ-D-09	REQ-D-02 REQ-D-03	A user should be able to end a video feed
CMU-REQ-D-10	REQ-D-06	A user should be able to save a video feed for offline review
CMU-REQ-D-11		A user should be able to tune image analysis
CMU-REQ-D-12		The system must use 2FA
CMU-REQ-D-13	REQ-D-02	User credentials must be protected
CMU-REQ-D-14		Lost or compromised credentials must be handled in a reasonable way
CMU-REQ-D-15		Nonrepudiation. Users should be confident that the camera they are using is the one that they believe it is
CMU-REQ-D-16		Multi-user Privacy , multiple video feeds remain private between the users
CMU-REQ-D-17		Reliability, the video is reliably delivered.
CMU-REQ-D-18		
CMU-REQ-D-19		
CMU-REQ-D-20		

CMU-REQ-D-01	Establishing connection between Client and Server	Mandatory
CMU-REQ-D-02	A user should be able to initiate a video feed, and a feed in Support Secure Mode	Mandatory
CMU-REQ-D-03	A user should be able to initiate a video feed, and a feed in Support Non Secure Mode	Mandatory
CMU-REQ-D-04	Support Learning Mode - Register new person to the Server	Mandatory
CMU-REQ-D-05	Support Run Mode - System identifies faces and performs facial recognition	Mandatory
CMU-REQ-D-06	Support Test Run Mode - A user should be able to tune image analysis with local file	Mandatory
CMU-REQ-D-07	Display Result - Face-recognized images	Mandatory
CMU-REQ-D-08	A user should be able to save a video feed for offline review	Excluded
CMU-REQ-D-09	The system must use 2FA	Mandatory
CMU-REQ-D-10	User credentials must be protected	Mandatory
CMU-REQ-D-11	Lost or compromised credentials must be handled in a reasonable way	Excluded
CMU-REQ-D-12	Nonrepudiation. Users should be confident that the camera they are using is the one that they believe it is	Excluded
CMU-REQ-D-13	Multi-user Privacy , multiple video feeds remain private between the users	Excluded
CMU-REQ-D-14	Reliability, the video is reliably delivered.	

TR-09	Denial Of Service	DF2.1 Request (Login / Mode Ctrl..)	
TR-10	Denial Of Service	DF2.1 Request (Login / Mode Ctrl..)	
TR-11	Elevation Of Privilege	DF2.1 Request (Login / Mode Ctrl..)	
TR-12	Elevation Of Privilege	DF2.1 Request (Login / Mode Ctrl..)	
TR-13	Elevation Of Privilege	DF2.1 Request (Login / Mode Ctrl..)	
TR-14	Spoofing	DF3.2 Sensor Data	
TR-15	Spoofing	DF3.2 Sensor Data	
TR-16	Tampering	DF3.2 Sensor Data	
TR-17	Repudiation	DF3.2 Sensor Data	
TR-18	Information Disclosure	DF3.2 Sensor Data	
TR-19	Denial Of Service	DF3.2 Sensor Data	
TR-20	Denial Of Service	DF3.2 Sensor Data	
TR-21	Elevation Of Privilege	DF3.2 Sensor Data	

Type	Internal Engineer
Goal	Ruin the administrator's reputation
Motivation	Revenge to the administrator
Skill	manipulate the user credential data, administrator's password from the previous one to other system
Misuse case	(TR-56) Change the image data not to recognize registered users. (TR-57) Disclose administrator's ID/Password to the employees in the company.

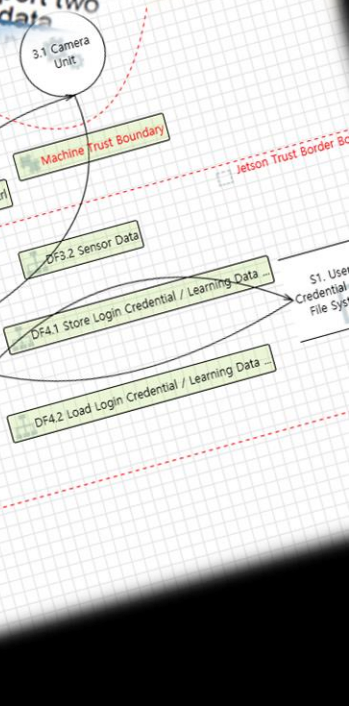
PnG 1

Type	Spy
Goal	Steal all components of the system
Motivation	Competitors request
Skill	Physical power and ability to use various equipment
Misuse case	(TR-58) Steal the client and server => Out of S/W boundary

PnG 2

Type	Hacker
Goal	Post the achievements of hacking on the internet
Motivation	Strives for recognition
Skill	Extensive knowledge of network protocols and program.
Misuse case	(TR-59) Sniff the communication channel between s client to get user credential data.

PnG 3



Schedule

		Criteria	Artifacts
Context Analysis		Artifacts	Team6_Schedule.xlsx, requirements_v2.0.xlsx
Risk Management		A	System/Sec REQ from Dan
Asset Identification		A	phase1_document_team6.docx
Threat Modeling	DFD Modeling PnG(Misuse case) STRIDE Brainstorming	A	threat_modeling.xlsx, JetsonNano_pit.tm7, PnG.docx, JetsonNano_STRIDE.xlsx
4-1		A	- JetsonNano_pit.tm7
4-2		A	- PnG.docx
4-3		A	- JetsonNano_STRIDE.xlsx
4-4		A	- ThreatModeling.txt
4-5		A	risk_management.xlsx
SEC Risk Assessment	OWASP	A	security_requirements.txt
SEC Requirement		D&P	Demo & Presentation
Mitigation	Server(Jetson Nano)		
Code Impl			
8-1	Client(PC)		
8-2			
Static Analysis	Code Review		
	Flaw Finder		
9	CPPChecker		
9-1			
9-4			
Fuzz Testing			
Penetration Test			
Documentation	Doc		
10	Review		
11			
12			
12-1			
12-1			
13			
Phases II			
14			
15			
16			

Architect Doc / Development

Architect Doc / Development

100% static_analysis_20210608_yo...

100% - flawfinder_20210607_y...

100% - flawfinder_20210614_...

100% - cppcheck_20210608_yo...

100% - cppcheck_20210610_...

100%

Requirements from CMU documents on left

DEVELOPMENT

5.2. STRIDE

Threats that could not arise as a result of the review or are outside the scope of this project were ***grayed*** out.

ID	Category	Interaction	Description	Justification
TR-01	Information Disclosure	DF4.2 Load Login Credential / Learning Data ...	Improper data protection of S1. User Credential Data File System can allow an attacker to read information not intended for disclosure. Review authorization settings.	[Threat] If the user credential data is stored as plain text, it can be disclosed. [Review] Use data encryption
TR-02	Tampering	DF4.2 Load Login Credential / Learning Data ...	Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources.	[Threat] An attacker modify user credential data. [Review] Use hashing
TR-03	Spoofing	DF4.2 Load Login Credential / Learning Data ...	S1. User Credential Data File System may be spoofed by an attacker and this may lead to incorrect data delivered to 2.1 Server (Jetson). Consider using a standard authentication mechanism to identify the source data store.	[Threat] An attacker modify user credential data and then server can use it without checking. [Review] Use hashing
TR-04	Spoofing	DF2.1 Request (Login / Mode Ctrl..)	2.1 Server (Jetson) may be spoofed by an attacker and this may lead to information disclosure by 1.1 Client (PC). Consider using a standard authentication mechanism to identify the destination process.	[Threat] An attacker spoof the user (Client) [Review] use 2FA
TR-05	Tampering	DF2.1 Request (Login / Mode Ctrl..)	Data flowing across DF2.1 Request (Login / Mode Ctrl..) may be tampered with by an attacker. This may lead to a denial of service attack against 2.1 Server (Jetson) or an elevation of privilege attack against 2.1 Server (Jetson) or an information disclosure by 2.1 Server (Jetson) . Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	[Threat] An attacker tampers data to server in order to get information. [Review] use TLS
TR-06	Repudiation	DF2.1 Request (Login / Mode Ctrl..)	2.1 Server (Jetson) claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	

ID	Reference
REQ-D-01	REQ-D-02 REQ-D-03
REQ-D-02	
REQ-D-03	
REQ-D-04	
REQ-D-05	
REQ-D-06	
REQ-D-07	
REQ-D-08	REQ-D-02
REQ-D-09	REQ-D-03
REQ-D-10	REQ-D-02 REQ-D-03
REQ-D-11	REQ-D-02
REQ-D-12	REQ-D-03
REQ-D-13	REQ-D-06
REQ-D-14	
REQ-D-15	
REQ-D-16	
REQ-D-17	REQ-D-02
REQ-D-18	
REQ-D-19	
REQ-D-20	

5.4. Brainstorming

Many threats have already been detected by the previous tools, but several threats have emerged.

ID	Threat	Review
TR-60	Compromise the connection of network physically by an attacker	
-	Sniffing in the middle of communication between camera and Jetson	Same as TR-18
-	Sniffing in the middle of communication between client and server	Same as TR-07
-	Leak pictures from the directory to unauthorized users	Same as TR-35
-	Anyone can view video stream from Jetson	Same as TR-48
TR-61	By changing the server/client's certificate or key, an attacker may attempt to connect to an unauthorized client. And attacker can try to steal the information of the encryption channel.	
TR-62	By modifying the face recognition data, an attacker may cause an error or abnormal operation in the face recognition result. By stealing facial recognition data, an attacker can	

Type	Internal Engineer
Goal	Ruin the administrator's reputation
Motivation	Revenge to the administrator
Skill	manipulate the user credential data, administrator's password from the previous one to other system
Misuse case	(TR-56) Change the image data not to recognize registered users. (TR-57) Disclose administrator's ID/Password to the employees in the company.

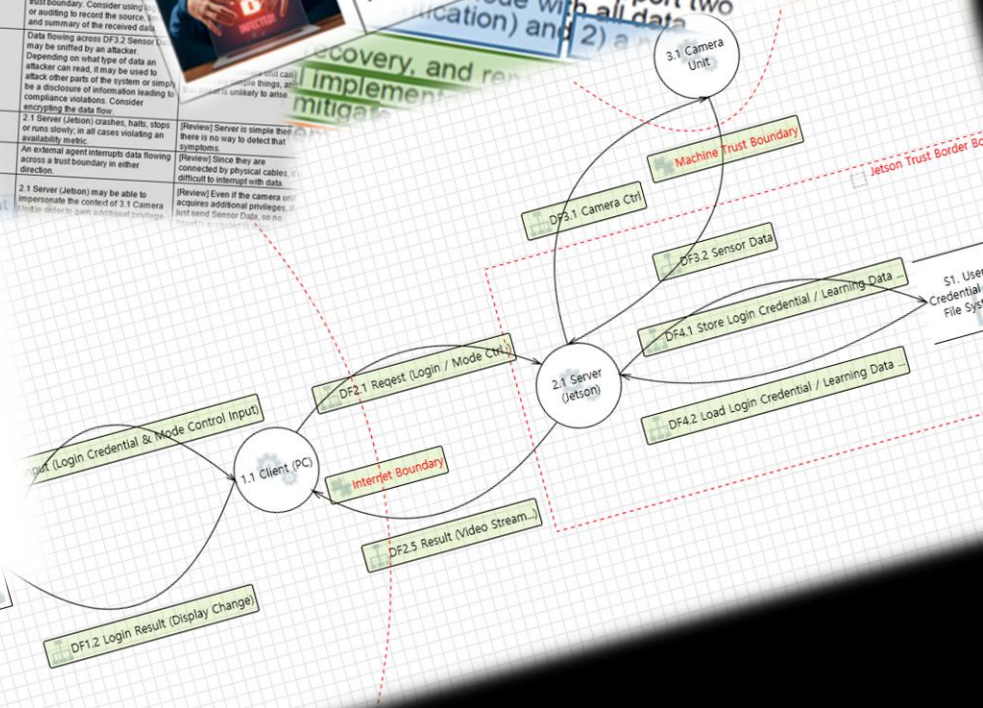
PnG 1

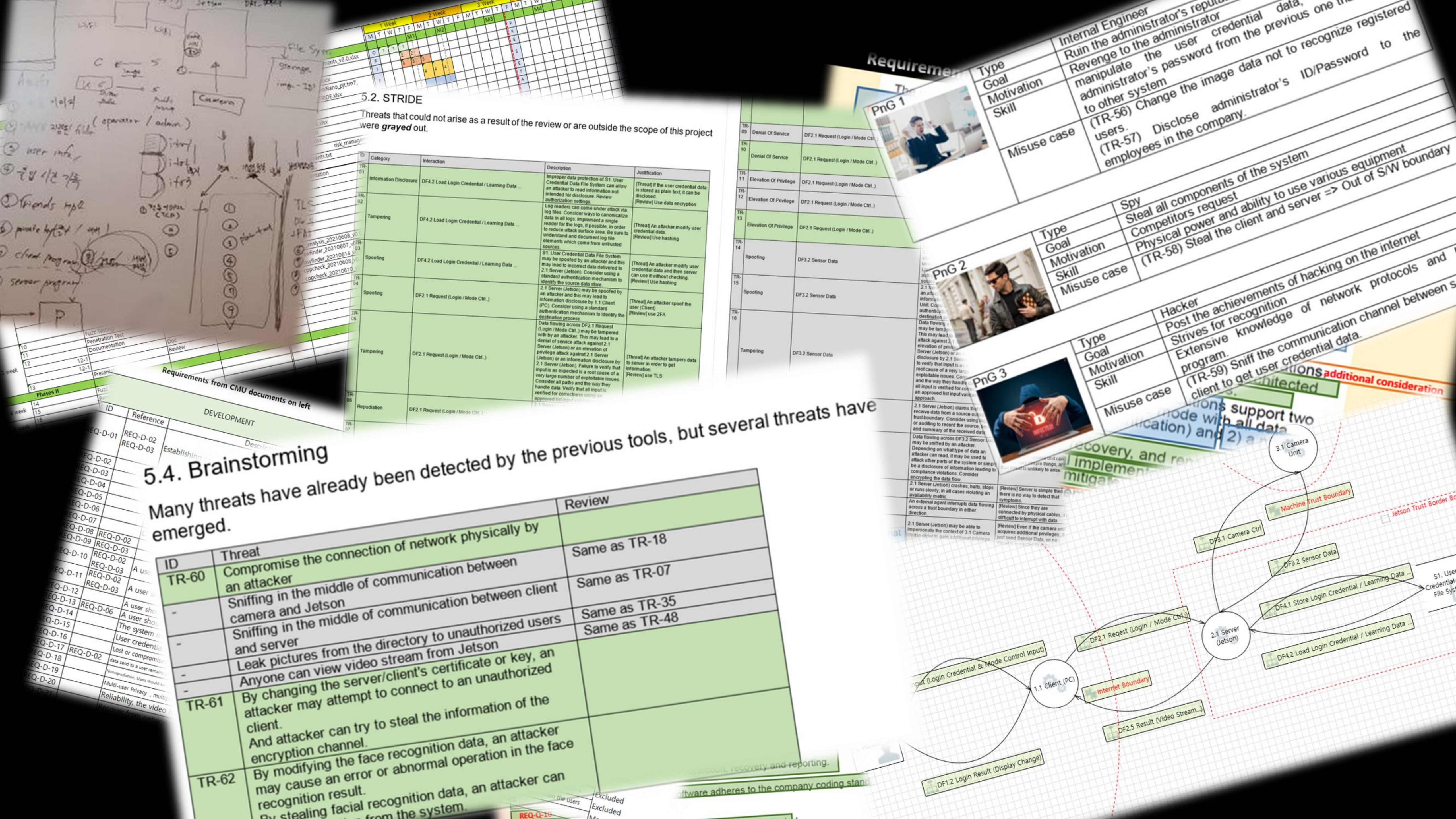
Type	Spy
Goal	Steal all components of the system
Motivation	Competitors request
Skill	Physical power and ability to use various equipment
Misuse case	(TR-58) Steal the client and server => Out of S/W boundary

PnG 2

Type	Hacker
Goal	Post the achievements of hacking on the internet
Motivation	Strives for recognition
Skill	Extensive knowledge of network protocols and
Misuse case	(TR-59) Sniff the communication channel between s client to get user credential data.

PnG 3





5.2. STRIDE
Threats that could not arise as a result of the review or are outside the scope of this project were grayed out.
Requirements from CMU documents on left
5.4. Brainstorming
Many threats have already been detected by the previous tools, but several threats have emerged.
ID
Threat
Review
TR-60
Compromise the connection of network physically by an attacker
Same as TR-18
Sniffing in the middle of communication between camera and Jetson
Same as TR-07
Sniffing in the middle of communication between client and server
Same as TR-35
Leak pictures from the directory to unauthorized users
Same as TR-48
Anyone can view video stream from Jetson
TR-61
By changing the server/client's certificate or key, an attacker may attempt to connect to an unauthorized client.
And attacker can try to steal the information of the encryption channel.
TR-62
By modifying the face recognition data, an attacker may cause an error or abnormal operation in the face recognition result.
PnG 1
Type
Internal Engineer
Goal
Ruin the administrator's reputation
Motivation
Revenge to the administrator
Skill
manipulate the user credential data, administrator's password from the previous one to other system
Misuse case
(TR-56) Change the image data not to recognize registered users.
(TR-57) Disclose administrator's ID/Password to the employees in the company.
PnG 2
Type
Spy
Goal
Steal all components of the system
Motivation
Competitors request
Skill
Physical power and ability to use various equipment
Misuse case
(TR-58) Steal the client and server => Out of S/W boundary
PnG 3
Type
Hacker
Goal
Post the achievements of hacking on the internet
Motivation
Strives for recognition
Skill
Extensive knowledge of network protocols and program.
Misuse case
(TR-59) Sniff the communication channel between client to get user credential data.
additional consideration
3.1 Camera Unit
Machine Trust Boundary
Jetson Trust Border Boundary
DF3.1 Camera Ctrl
DF3.2 Sensor Data
DF4.1 Store Login Credential / Learning Data ...
DF4.2 Load Login Credential / Learning Data ...
DF2.1 Reqest (Login / Mode Ctrl.)
2.1 Server (Jetson)
1.1 Client (PC)
Internet Boundary
DF2.5 Result (Video Stream...)
DF1.2 Login Result (Display Change)

5.2. STRIDE

Threats that could not arise as a result of the review or are outside the scope of this project were ***grayed*** out.

ID	Category	Interaction	Description	Justification
TR-01	Information Disclosure	DF4.2 Load Login Credential / Learning Data ...	Improper data protection of S1. User Credential Data File System can allow an attacker to read information not intended for disclosure. Review authorization settings.	[Threat] If the user credential data is stored as plain text, it can be disclosed. [Review] Use data encryption
TR-02	Tampering	DF4.2 Load Login Credential / Learning Data ...	Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources.	[Threat] An attacker modify user credential data. [Review] Use hashing
TR-03	Spoofing	DF4.2 Load Login Credential / Learning Data ...	S1. User Credential Data File System may be spoofed by an attacker and this may lead to incorrect data delivered to 2.1 Server (Jetson). Consider using a standard authentication mechanism to identify the source data store.	[Threat] An attacker modify user credential data and then server can use it without checking. [Review] Use hashing
TR-04	Spoofing	DF2.1 Request (Login / Mode Ctrl..)	2.1 Server (Jetson) may be spoofed by an attacker and this may lead to information disclosure by 1.1 Client (PC). Consider using a standard authentication mechanism to identify the destination process.	[Threat] An attacker spoof the user (Client) [Review] use 2FA
TR-05	Tampering	DF2.1 Request (Login / Mode Ctrl..)	Data flowing across DF2.1 Request (Login / Mode Ctrl..) may be tampered with by an attacker. This may lead to a denial of service attack against 2.1 Server (Jetson) or an elevation of privilege attack against 2.1 Server (Jetson) or an information disclosure by 2.1 Server (Jetson). Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	[Threat] An attacker tampers data to server in order to get information. [Review] use TLS
TR-06	Repudiation	DF2.1 Request (Login / Mode Ctrl..)		

Requirements from CMU documents on left

DEVELOPMENT

5.4. Brainstorming

Many threats have already been detected by the previous tools, but several threats have emerged.

ID	Threat	Review
TR-60	Compromise the connection of network physically by an attacker	
-	Sniffing in the middle of communication between camera and Jetson	Same as TR-18
-	Sniffing in the middle of communication between client and server	Same as TR-07
-	Leak pictures from the directory to unauthorized users	Same as TR-35
-	Anyone can view video stream from Jetson	Same as TR-48
TR-61	By changing the server/client's certificate or key, an attacker may attempt to connect to an unauthorized client. And attacker can try to steal the information of the encryption channel.	
TR-62	By modifying the face recognition data, an attacker may cause an error or abnormal operation in the face recognition result. By stealing facial recognition data, an attacker can	

Type	Internal Engineer
Goal	Ruin the administrator's reputation
Motivation	Revenge to the administrator
Skill	manipulate the user credential data, administrator's password from the previous one to other system
Misuse case	(TR-56) Change the image data not to recognize registered users. (TR-57) Disclose administrator's ID/Password to the employees in the company.

PnG 1

Type	Spy
Goal	Steal all components of the system
Motivation	Competitors request
Skill	Physical power and ability to use various equipment
Misuse case	(TR-58) Steal the client and server => Out of S/W boundary

PnG 2

Type	Hacker
Goal	Post the achievements of hacking on the internet
Motivation	Strives for recognition
Skill	Extensive knowledge of network protocols and program.
Misuse case	(TR-59) Sniff the communication channel between s client to get user credential data.

PnG 3

additional consideration

3.1 Camera Unit

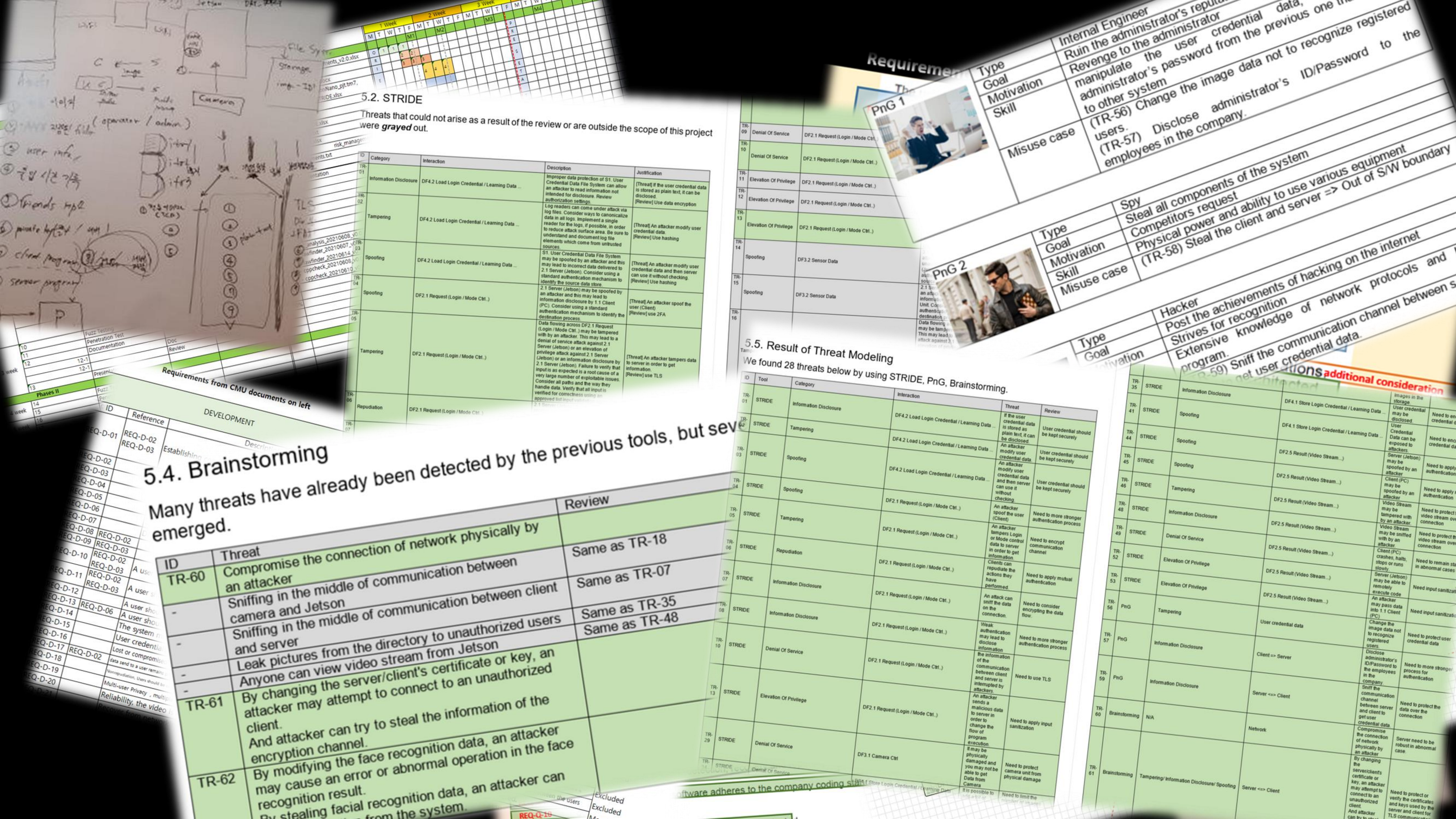
Machine Trust Boundary

1.1 Client (PC)

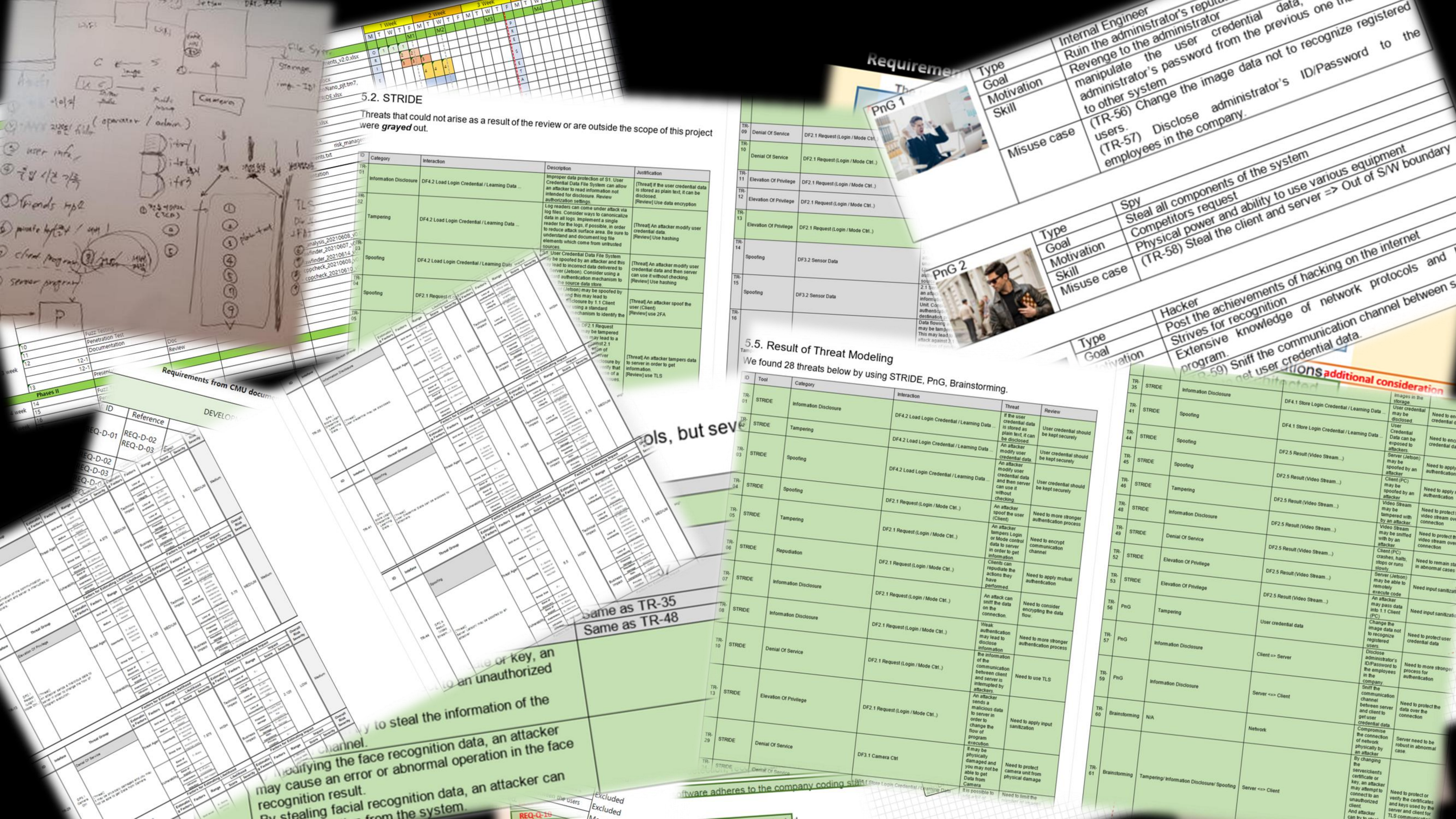
Interjet Boundary

DF1.2 Login Result (Display Change)

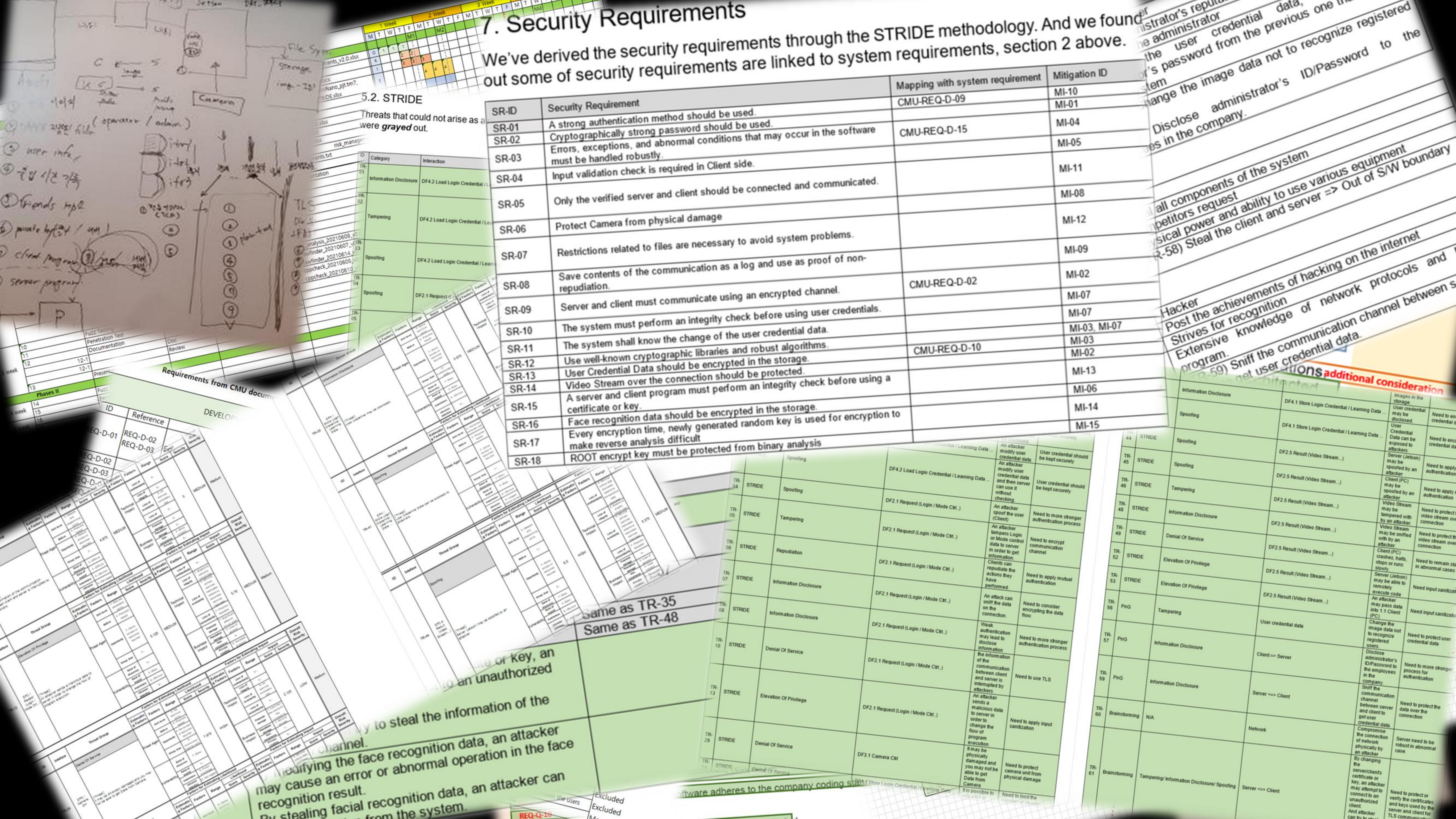
DF2.5 Result



5.2. STRIDE
Threats that could not arise as a result of the review or are outside the scope of this project were grayed out.
5.4. Brainstorming
Many threats have already been detected by the previous tools, but seve
emerged.
ID
Threat
Review
TR-60
Compromise the connection of network physically by an attacker
Same as TR-18
Sniffing in the middle of communication between camera and Jetson
Same as TR-07
Sniffing in the middle of communication between client and server
Same as TR-35
Leak pictures from the directory to unauthorized users
Same as TR-48
Anyone can view video stream from Jetson
TR-61
By changing the server/client's certificate or key, an attacker may attempt to connect to an unauthorized client.
And attacker can try to steal the information of the encryption channel.
TR-62
By modifying the face recognition data, an attacker may cause an error or abnormal operation in the face recognition result.
5.5. Result of Threat Modeling
We found 28 threats below by using STRIDE, PnG, Brainstorming.
Requirements from CMU documents on left
PnG 1
Type
Goal
Motivation
Skill
Misuse case
Internal Engineer
Ruin the administrator's reputa
Revenge to the administrator
manipulate the user credential data,
administrator's password from the previous one
to other system
(TR-56) Change the image data not to recognize registered users.
(TR-57) Disclose administrator's ID/Password to the employees in the company.
PnG 2
Spy
Steal all components of the system
Competitors request
Physical power and ability to use various equipment
(TR-58) Steal the client and server => Out of S/W boundary
Hacker
Post the achievements of hacking on the internet
Strives for recognition
Extensive knowledge of network protocols and
program.
(TR-59) Sniff the communication channel between s
get user credential data.
additional consideration



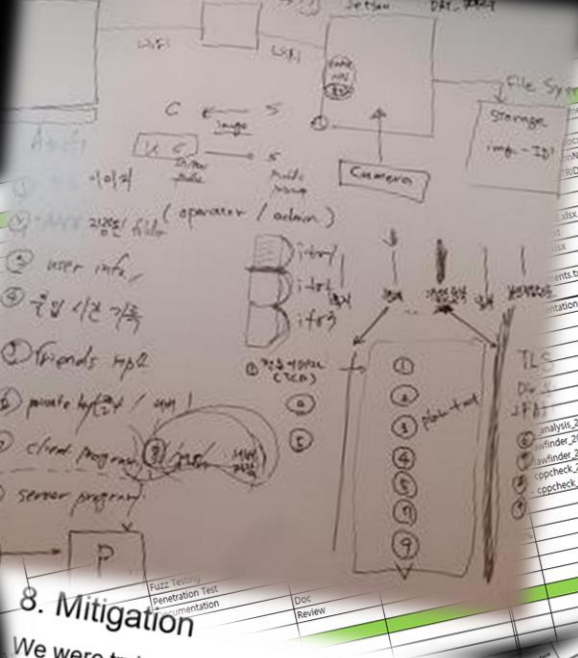
5.2. STRIDE
Threats that could not arise as a result of the review or are outside the scope of this project were grayed out.
5.5. Result of Threat Modeling
We found 28 threats below by using STRIDE, PnG, Brainstorming.
Requirements from CMU document
PnG 1
Type
Internal Engineer
Goal
Ruin the administrator's reputation
Motivation
Revenge to the administrator
Misuse case
(TR-56) Change the image data not to recognize registered users.
(TR-57) Disclose administrator's ID/Password to the employees in the company.
PnG 2
Type
Spy
Goal
Steal all components of the system
Motivation
Competitors request
Skill
Physical power and ability to use various equipment
Misuse case
(TR-58) Steal the client and server => Out of S/W boundary
Type
Hacker
Goal
Post the achievements of hacking on the internet
Motivation
Strives for recognition
Skill
Extensive knowledge of network protocols and
Same as TR-35
Same as TR-48
additional consideration



7. Security Requirements

We've derived the security requirements through the STRIDE methodology. And we found out some of security requirements are linked to system requirements, section 2 above.

SR-ID	Security Requirement	Mapping with system requirement	Mitigation ID
SR-01	A strong authentication method should be used.	CMU-REQ-D-09	MI-10
SR-02	Cryptographically strong password should be used.		MI-01
SR-03	Errors, exceptions, and abnormal conditions that may occur in the software must be handled robustly.	CMU-REQ-D-15	MI-04
SR-04	Input validation check is required in Client side.		MI-05
SR-05	Only the verified server and client should be connected and communicated.		MI-11
SR-06	Protect Camera from physical damage		MI-08
SR-07	Restrictions related to files are necessary to avoid system problems.		MI-12
SR-08	Save contents of the communication as a log and use as proof of non-repudiation.		MI-09
SR-09	Server and client must communicate using an encrypted channel.	CMU-REQ-D-02	MI-02
SR-10	The system must perform an integrity check before using user credentials.		MI-07
SR-11	The system shall know the change of the user credential data.		MI-07
SR-12	Use well-known cryptographic libraries and robust algorithms.		MI-03, MI-07
SR-13	User Credential Data should be encrypted in the storage.	CMU-REQ-D-10	MI-03
SR-14	Video Stream over the connection should be protected.		MI-02
SR-15	A server and client program must perform an integrity check before using a certificate or key.		MI-13
SR-16	Face recognition data should be encrypted in the storage.		MI-06
SR-17	Every encryption time, newly generated random key is used for encryption to make reverse analysis difficult		MI-14
SR-18	ROOT encrypt key must be protected from binary analysis		MI-15



7. Security Requirements

We've derived the security requirements through the STRIDE methodology. And we found out some of security requirements are linked to system requirements, section 2 above.

SR-ID	Security Requirement	Mapping with system requirement	Mitigation ID
SR-01	A strong authentication method should be used.	CMU-REQ-D-09	MI-10
SR-02	Cryptographically strong password should be used.		MI-01
SR-03	Errors, exceptions, and abnormal conditions that may occur in the software must be handled robustly.	CMU-REQ-D-15	MI-04
SR-04	Input validation check is required in Client side.		MI-05
SR-05	Only the verified server and client should be connected and communicated.		MI-11
SR-06	Protect Camera from physical damage		MI-08
SR-07	Restrictions related to files are necessary to avoid system problems.		MI-12
SR-08	Save contents of the communication as a log and use as proof of non-repudiation.		MI-09
SR-09	Server and client must communicate using an encrypted channel.	CMU-REQ-D-02	MI-02
SR-10	The system must perform an integrity check before using user credentials.		MI-07
SR-11	The system shall know the change of the user credential data.		MI-07
SR-12	Use well-known cryptographic libraries and robust algorithms.		MI-03, MI-07
SR-13	User Credential Data should be encrypted in the storage.	CMU-REQ-D-10	MI-03
SR-14	Video Stream over the connection should be protected.		MI-02
SR-15	A server and client program must perform an integrity check before using a certificate or key.		MI-13
SR-16	Face recognition data should be encrypted in the storage.		MI-06
SR-17	Every encryption time, newly generated random key is used for encryption to make reverse analysis difficult		MI-14
SR-18	ROOT encrypt key must be protected from binary analysis		MI-15

5.2. STRIDE

Threats that could not arise as a
were ***grayed*** out.

8. Mitigation

We were trying to mitigate the threat and mentioned in the Security Requirements, section 7. And we've derived the result below.

MI-ID	Mitigation
MI-01	Apply setting policy of cryptographically strong password - Enforce passwords longer than 7 characters. - Forces the use of mixed the letters of the alphabet and numbers.
MI-02	Communicate using Encrypted channel - using protocol TLS1.2 or higher - Consider mutual authentication between server and client
MI-03	Encrypt user credential data in storage - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than AES256 - Use CBC or GCM mode
MI-04	Implement robust system - Error handling - Exception handling - Finding countermeasures for predictable abnormal conditions
	Input validation check - Input sanitization
	Encrypt face recognition data in storage - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than AES256 - Use CBC or GCM mode
	Integrity Check with hash function - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than sha256
	Protect from physical damage - Wrap the camera module out of sight, or glue the cable to the camera.
	Save contents of communication as a log - Save log of the request and response between the server and the client
	Strong authentication method - Consider 2-Factor-Authentication method
	Use mutual authentication - Using protocol TLS1.2 or higher - Use mutual authentication between server and client
	Validation of image when file saving - File name verification(uniqueness) when image save : generate the name of file using random number. - File size validation when image save
	Certificate & Key file existence check Integrity Check with hash function Use OpenSSL library of latest version (1.1.1k) Use an algorithm that are stronger than sha256

Same as TR-35
Same as TR-48

TR-04	STRIDE	Spoofing	DF4.2 Load Login Credential / Learning Data ...	An attacker modify user credential data	User credential should be kept securely
TR-05	STRIDE	Tampering	DF2.1 Request (Login / Mode Ctrl..)	An attacker modify user credential data and then server can use it without checking	User credential should be kept securely
TR-06	STRIDE	Repudiation	DF2.1 Request (Login / Mode Ctrl..)	An attacker spoof the user (Client)	Need to more stronger authentication process
TR-07	STRIDE	Information Disclosure	DF2.1 Request (Login / Mode Ctrl..)	An attacker tampers Login or Mode control data to server in order to get information	Need to encrypt communication channel
TR-08	STRIDE	Information Disclosure	DF2.1 Request (Login / Mode Ctrl..)	Clients can repudiate the actions they have performed	Need to apply mutual authentication
TR-10	STRIDE	Denial Of Service	DF2.1 Request (Login / Mode Ctrl..)	An attack can sniff the data on the connection	Need to consider encrypting the data flow.
TR-13	STRIDE	Elevation Of Privilege	DF2.1 Request (Login / Mode Ctrl..)	Weak authentication may lead to disclose information	Need to more stronger authentication process
TR-29	STRIDE	Denial Of Service	DF3.1 Camera Ctrl	the information of the communication between client and server is interrupted by attackers	Need to use TLS
TR-	STRIDE			An attacker sends a malicious data to server in order to change the flow of program execution	Need to apply input sanitization
				It may be physically damaged and you may not be able to get Data from Camera	Need to protect camera unit from physical damage
				It is possible to	Need to limit the

44	STRIDE	Information Disclosure	DF4.1 Store Login Credential / Learning Data ...	Images in the storage	
		Spoofing	DF4.1 Store Login Credential / Learning Data ...	User credential may be disclosed.	Need to en credential d
TR-45	STRIDE	Spoofing	DF2.5 Result (Video Stream...)	User Credential Data can be exposed to attackers.	Need to enc credential da
TR-46	STRIDE	Tampering	DF2.5 Result (Video Stream...)	Server (Jetson) may be spoofed by an attacker	Need to appl authentication
TR-48	STRIDE	Information Disclosure	DF2.5 Result (Video Stream...)	Client (PC) may be spoofed by an attacker	Need to apply authentication
TR-49	STRIDE	Denial Of Service	DF2.5 Result (Video Stream...)	Video Stream may be tampered with by an attacker	Need to protect video stream ov connection
TR-52	STRIDE	Elevation Of Privilege	DF2.5 Result (Video Stream...)	Video Stream may be snifted with by an attacker	Need to protect video stream ove connection
TR-53	STRIDE	Elevation Of Privilege	DF2.5 Result (Video Stream...)	Client (PC) crashes, halts, stops or runs slowly.	Need to remain st in abnormal cases
TR-56	PnG	Tampering	User credential data	Server (Jetson) may be able to remotely execute code	Need input sanitizat
TR-57	PnG	Information Disclosure	Client => Server	An attacker may pass data into 1.1 Client (PC)	Need input sanitizat
TR-59	PnG	Information Disclosure	Server <=> Client	Change the image data not to recognize registered users.	Need to protect user credential data
TR-60	Brainstorming	N/A	Network	Disclose administrator's ID/Password to the employees in the company	Need to more stronger process for authentication
TR-61	Brainstorming	Tampering/ Information Disclosure/ Spoofing	Server <=> Client	Sniff the communication channel between server and client to get user credential data	Need to protect the data over the connection
				Compromise the connection of network physically by an attacker.	Server need to be robust in abnormal case.
				By changing the server/clients certificate or key, an attacker may attempt to connect to an unauthorized client. And attacker can try to get	Need to protect or verify the certificates and keys used by the server and client for TLS communi

additional consideration

- Hacker
- Post the achievements of hacking on the internet
- Strives for recognition
- Extensive knowledge of network protocols and
- program.

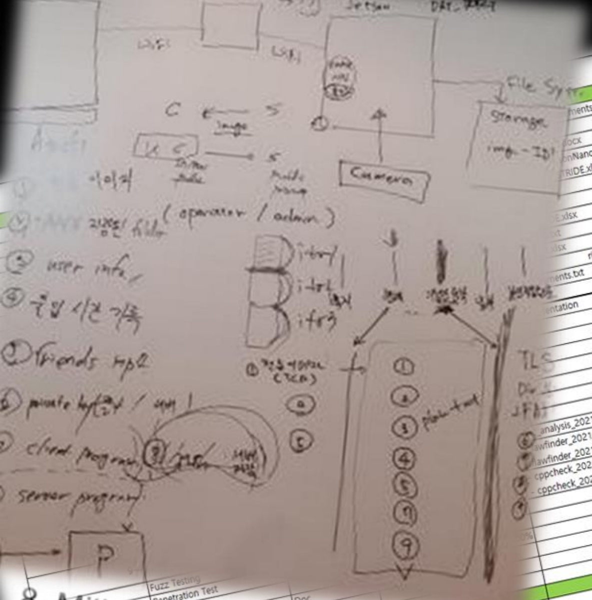
R-58) Steal the client and server => Out of S/W boundary

R-59) Sniff the communication channel between s
get user credential data.

all components of the system
petitors request
sical power and ability to use various equipment

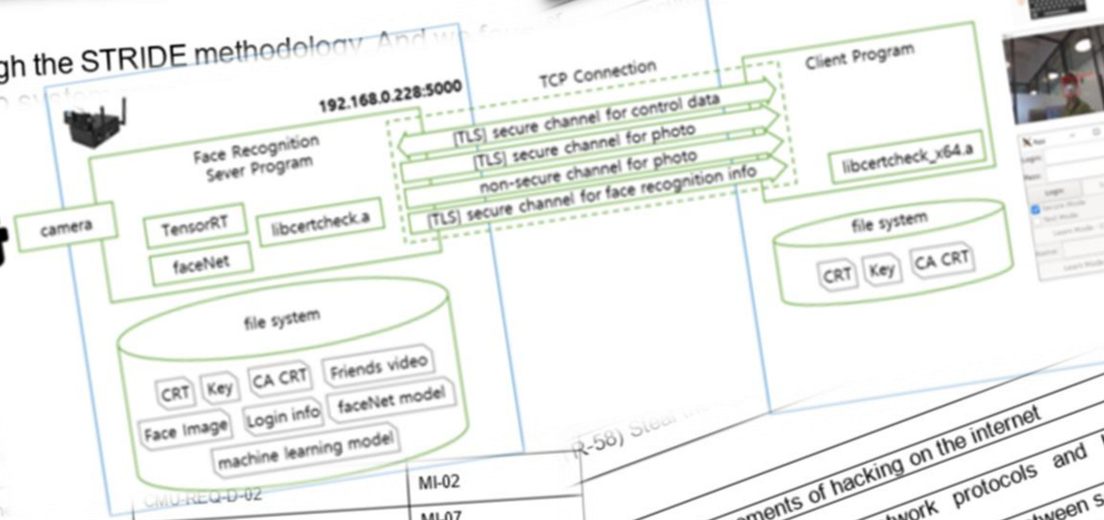
Disclose administrator's ID/Password to the
es in the company.

ange the image data not to recognize registered
's password from the previous one th
the user credential data,
administrator
e
istrator's reputa



7. Security Requirements

We've derived the security requirements through the STRIDE methodology. And we found out some of security requirements are linked to ...



SR-ID	Security Requirement		
SR-01	A strong authentication method should be used.		
SR-02	Cryptographically strong password should be used.		
SR-03	Errors, exceptions, and abnormal conditions that may occ... must be handled robustly.		
SR-04	Input validation check is required in Client side.		
SR-05	Only the verified server and client should be connected and ...		
SR-06	Protect Camera from physical damage		
SR-07	Restrictions related to files are necessary to avoid system pr...		
SR-08	Save contents of the communication as a log and use as proo... repudiation.	CMU-REQ-D-02	MI-02
SR-09	Server and client must communicate using an encrypted chann...		MI-07
SR-10	The system must perform an integrity check before using user credentials.		MI-07
SR-11	The system shall know the change of the user credential data.		MI-03, MI-07
SR-12	Use well-known cryptographic libraries and robust algorithms.		MI-03
SR-13	User Credential Data should be encrypted in the storage.	CMU-REQ-D-10	MI-02
SR-14	Video Stream over the connection should be protected.		MI-13
SR-15	A server and client program must perform an integrity check before using a certificate or key.		MI-06
SR-16	Face recognition data should be encrypted in the storage.		MI-14
SR-17	Every encryption time, newly generated random key is used for encryption to make reverse analysis difficult		MI-15
SR-18	ROOT encrypt key must be protected from binary analysis		

5.2. STRIDE

Threats that could not arise as a ... were ***grayed*** out.

Hacker
Post the achievements of hacking on the internet
Strives for recognition
Extensive knowledge of network protocols and ...
(TR-59) Sniff the communication channel between s... program ... get user credential data.

additional consideration

Same as TR-35
Same as TR-48

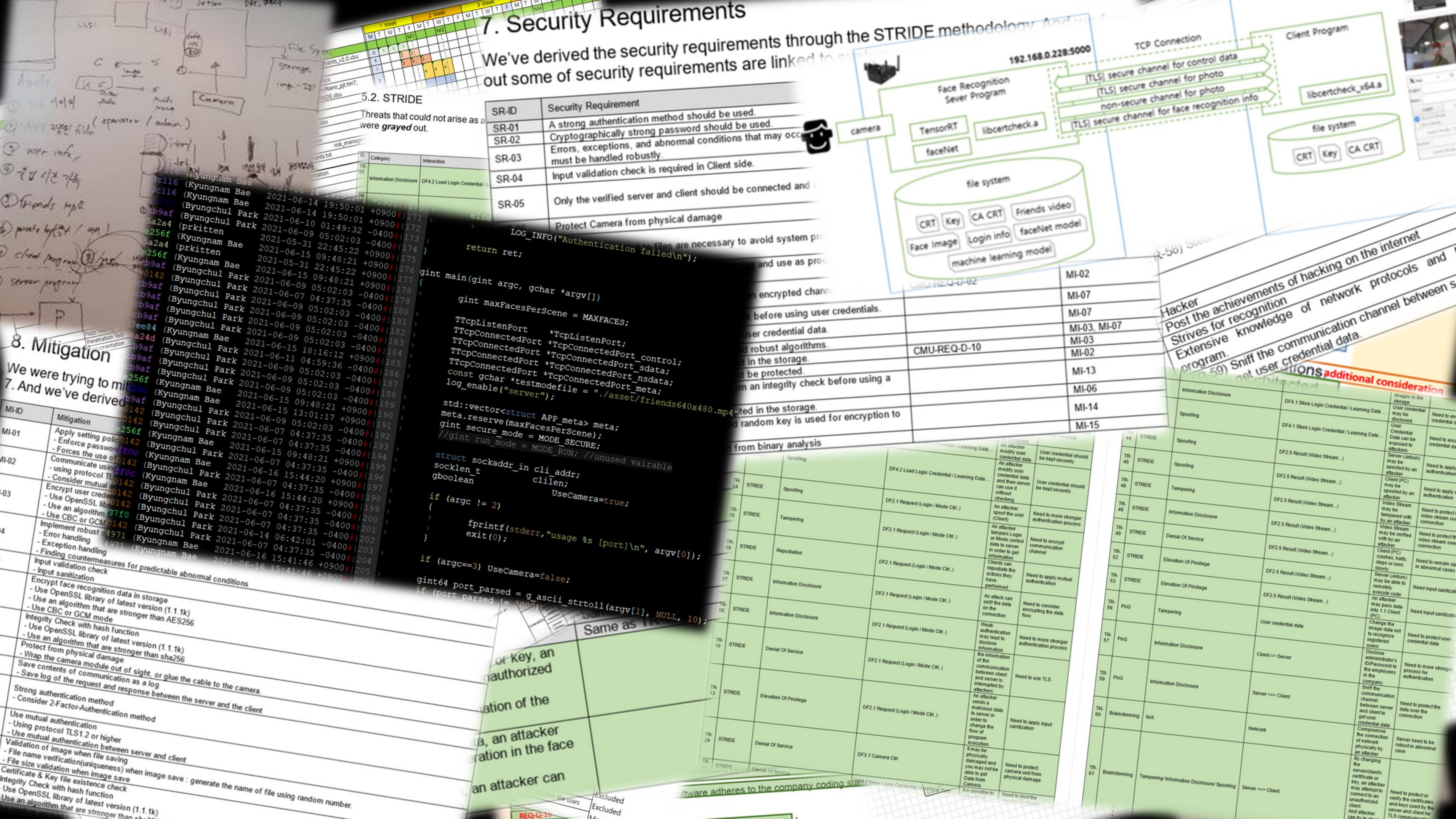
8. Mitigation

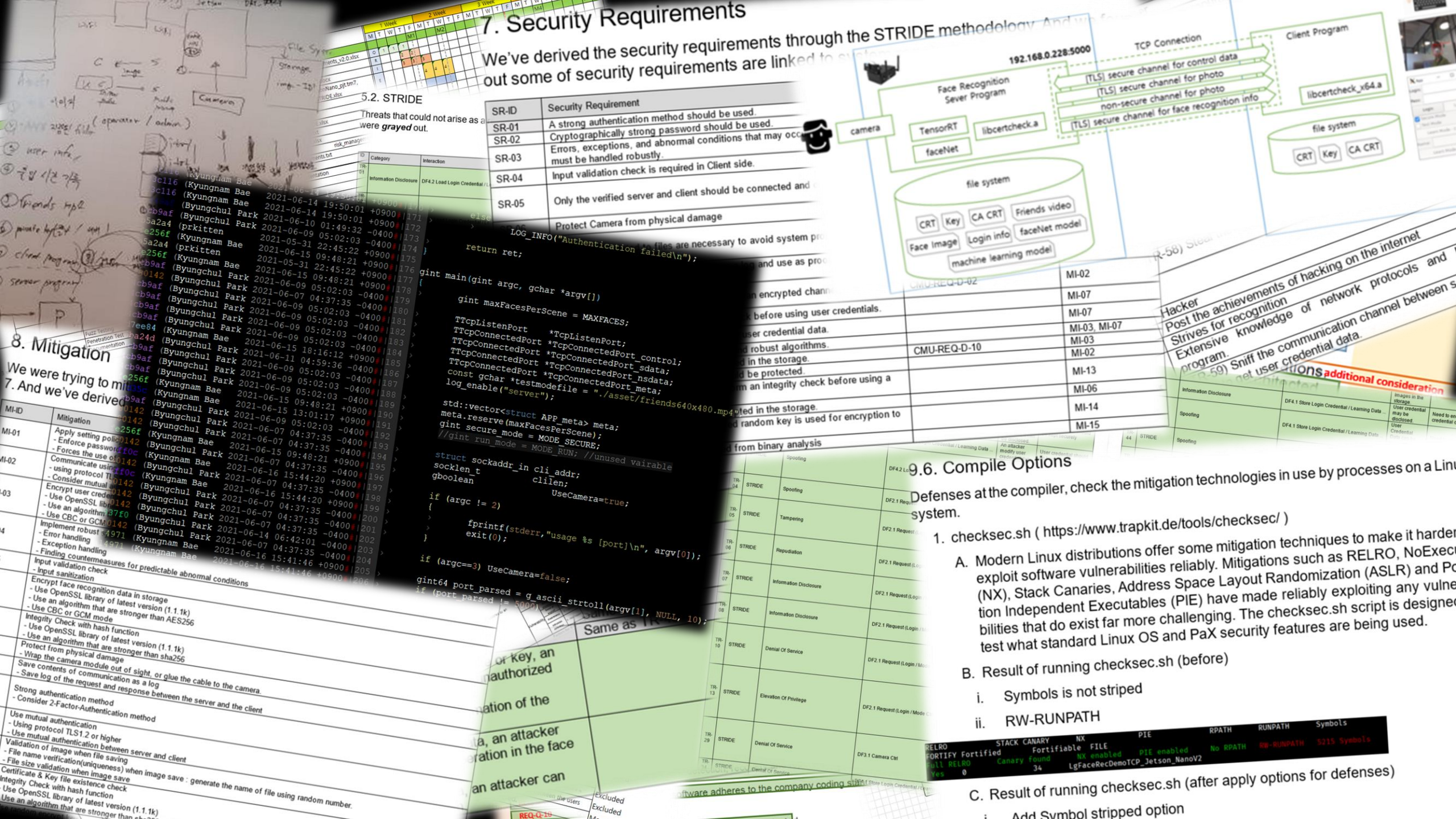
We were trying to mitigate the threat and mentioned in the Security Requirements, section 7. And we've derived the result below.

MI-ID	Mitigation
MI-01	Apply setting policy of cryptographically strong password - Enforce passwords longer than 7 characters. - Forces the use of mixed the letters of the alphabet and numbers.
MI-02	Communicate using Encrypted channel - using protocol TLS1.2 or higher - Consider mutual authentication between server and client
MI-03	Encrypt user credential data in storage - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than AES256 - Use CBC or GCM mode
MI-04	Implement robust system - Error handling - Exception handling - Finding countermeasures for predictable abnormal conditions
	Input validation check - Input sanitization
	Encrypt face recognition data in storage - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than AES256 - Use CBC or GCM mode
	Integrity Check with hash function - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than sha256
	Protect from physical damage - Wrap the camera module out of sight, or glue the cable to the camera.
	Save contents of communication as a log - Save log of the request and response between the server and the client
	Strong authentication method - Consider 2-Factor-Authentication method
	Use mutual authentication - Using protocol TLS1.2 or higher - Use mutual authentication between server and client
	Validation of image when file saving - File name verification(uniqueness) when image save : generate the name of file using random number. - File size validation when image save
	Certificate & Key file existence check
	Integrity Check with hash function - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than sha256

... or key, an unauthorized ...
... ation of the ...
... a, an attacker ... eration in the face ...
... an attacker can ...

... oftware adheres to the company coding st...


7. Security Requirements
We've derived the security requirements through the STRIDE methodology.
out some of security requirements are linked to
SR-ID
Security Requirement
SR-01
A strong authentication method should be used.
SR-02
Cryptographically strong password should be used.
SR-03
Errors, exceptions, and abnormal conditions that may occ
must be handled robustly.
SR-04
Input validation check is required in Client side.
SR-05
Only the verified server and client should be connected and
Protect Camera from physical damage
5.2. STRIDE
Threats that could not arise as a
were grayed out.
192.168.0.228:5000
TCP Connection
Client Program
Face Recognition
Sever Program
camera
TensorRT
libcertcheck.a
faceNet
[TLS] secure channel for control data
[TLS] secure channel for photo
[TLS] secure channel for photo
non-secure channel for face recognition info
[TLS] secure channel for face recognition info
libcertcheck_x64.a
file system
CRT
Key
CA CRT
Friends video
Face Image
Login info
faceNet model
machine learning model
CMU-REQ-D-02
CMU-REQ-D-10
MI-02
MI-07
MI-07
MI-03, MI-07
MI-03
MI-02
MI-13
MI-06
MI-14
MI-15
Hacker
Post the achievements of hacking on the internet
Strives for recognition
Extensive knowledge of network protocols and
program.
Sniff the communication channel between s
get user credential data.
additional consideration
8. Mitigation
We were trying to mi
7. And we've derived
MI-ID
Mitigation
MI-01
MI-02
Apply setting polic
- Enforce passwor
- Forces the use of
Communicate usin
- using protocol TL
- Consider mutual
Encrypt user crede
- Use OpenSSL libr
- Use an algorithm
- Use CBC or GCM
Implement robust
- Error handling
- Exception handling
- Finding countermeasures for predictable abnormal conditions
Input validation check
- Input sanitization
Encrypt face recognition data in storage
- Use OpenSSL library of latest version (1.1.1k)
- Use an algorithm that are stronger than AES256
- Use CBC or GCM mode
Integrity Check with hash function
- Use OpenSSL library of latest version (1.1.1k)
- Use an algorithm that are stronger than sha256
Protect from physical damage
- Wrap the camera module out of sight, or glue the cable to the camera.
Save contents of communication as a log
- Save log of the request and response between the server and the client
Strong authentication method
- Consider 2-Factor-Authentication method
Use mutual authentication
- Using protocol TLS1.2 or higher
- Use mutual authentication between server and client
Validation of image when file saving
- File name verification(uniqueness) when image save : generate the name of file using random number.
- File size validation when image save
Certificate & Key file existence check
Integrity Check with hash function
- Use OpenSSL library of latest version (1.1.1k)
- Use an algorithm that are stronger than sha256
LOG_INFO("Authentication failed\n");
return ret;
gint main(gint argc, gchar *argv[])
gint maxFacesPerScene = MAXFACES;
TTcpListenPort *TcpListenPort;
TTcpConnectedPort *TcpConnectedPort_control;
TTcpConnectedPort *TcpConnectedPort_sdata;
TTcpConnectedPort *TcpConnectedPort_nsdata;
TTcpConnectedPort *TcpConnectedPort_meta;
const gchar *testmodefile = "./asset/friends640x480.mp4
log_enable("server");
std::vector<struct APP_meta> meta;
meta.reserve(maxFacesPerScene);
gint secure_mode = MODE_SECURE;
//gint run_mode = MODE_RUN; //unused vairable
struct sockaddr_in cli_addr;
socklen_t clilen;
gboolean UseCamera=true;
if (argc != 2)
fprintf(stderr,"usage %s [port]\n", argv[0]);
exit(0);
if (argc==3) UseCamera=false;
gint64 port_parsed = g_ascii_strtoll(argv[1], NULL, 10);
Same as TR
Excluded
Excluded
Spoofing
Tampering
Repudiation
Information Disclosure
Denial Of Service
Elevation Of Privilege
Network
Client => Server
Server <=> Client



7. Security Requirements

We've derived the security requirements through the STRIDE methodology. And we

SR-ID	Security Requirement
SR-01	A strong authentication method should be used.
SR-02	Cryptographically strong password should be used.
SR-03	Errors, exceptions, and abnormal conditions that may occ must be handled robustly.
SR-04	Input validation check is required in Client side.
SR-05	Only the verified server and client should be connected and
	Protect Camera from physical damage

5.2. STRIDE

Threats that could not arise as a
were ***grayed*** out.

ID	Category	Interaction
TR-01	Information Disclosure	DF4.2 Load Login Credential / L

```
        LOG_INFO("Authentication failed\n");
    return ret;

gint main(gint argc, gchar *argv[])
{
    gint maxFacesPerScene = MAXFACES;

    TTcpListenPort    *TcpListenPort;
    TTcpConnectedPort *TcpConnectedPort_control;
    TTcpConnectedPort *TcpConnectedPort_sdata;
    TTcpConnectedPort *TcpConnectedPort_nsdata;
    TTcpConnectedPort *TcpConnectedPort_meta;
    const gchar *testmodefile = "./asset/friends640x480.mp4";
    log_enable("server");

    std::vector<struct APP_meta> meta;
    meta.reserve(maxFacesPerScene);
    gint secure_mode = MODE_SECURE;
    //gint run_mode = MODE_RUN; //unused vairable

    struct sockaddr_in cli_addr;
    socklen_t          clilen;
    gboolean           UseCamera=true;

    if (argc != 2)
    {
        fprintf(stderr,"usage %s [port]\n", argv[0]);
        exit(0);
    }

    if (argc==3) UseCamera=false;

    gint64 port_parsed = g_ascii_strtoll(argv[1], NULL, 10);
    if (port_parsed != 5002)
```


	MI-02
	MI-07
	MI-07
	MI-03, MI-07
CMU-REQ-D-10	MI-03
	MI-02
	MI-13
	MI-06
	MI-14
	MI-15

Hacker
Post the achievements of hacking on the internet
Strives for recognition
Extensive knowledge of network protocols and
program.
-59) Sniff the communication channel between s
et user credential data.

Information Disclosure	DF4.1 Store Login Credential / Learning Data	Images in the storage	
Spoofing	DF4.1 Store Login Credential / Learning Data	User credential may be disclosed	Need to en credential d
Spoofing		User Credential	

additional consideration

8. Mitigation

We were trying to mi
7. And we've derived

MI-ID	Mitigation
MI-01	Apply setting polic - Enforce password - Forces the use o
MI-02	Communicate using - using protocol T - Consider mutual a
MI-03	Encrypt user crede - Use OpenSSL libr - Use an algorithm - Use CBC or GCM
MI-04	Implement robust - Error handling - Exception handling - Finding countermeasures for predictable abnormal conditions
	Input validation check - Input sanitization
	Encrypt face recognition data in storage - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than AES256 - Use CBC or GCM mode
	Integrity Check with hash function - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than sha256
	Protect from physical damage - Wrap the camera module out of sight, or glue the cable to the camera.
	Save contents of communication as a log - Save log of the request and response between the server and the client
	Strong authentication method - Consider 2-Factor-Authentication method
	Use mutual authentication - Using protocol TLS1.2 or higher - Use mutual authentication between server and client
	Validation of image when file saving - File name verification(uniqueness) when image save : generate the name of file using random number. - File size validation when image save
	Certificate & Key file existence check
	Integrity Check with hash function Use OpenSSL library of latest version (1.1.1k) Use an algorithm that are stronger than sh

TR-04	STRIDE	Spoofing	DF2.1 Request
TR-05	STRIDE	Tampering	DF2.1 Request
TR-06	STRIDE	Repudiation	DF2.1 Request (Lo
TR-07	STRIDE	Information Disclosure	DF2.1 Request (Login
TR-08	STRIDE	Information Disclosure	DF2.1 Request (Login /
TR-10	STRIDE	Denial Of Service	DF2.1 Request (Login / Mo
TR-13	STRIDE	Elevation Of Privilege	DF2.1 Request (Login / Mode C
TR-29	STRIDE	Denial Of Service	DF3.1 Camera Ctrl
TR-	STRIDE	Denial Of Service	

Same as

or key, an
nauthorized
ation of the
a, an attacker
ration in the face
an attacker can

oftware adheres to the company coding st

Excluded
Excluded
REQ-C-10

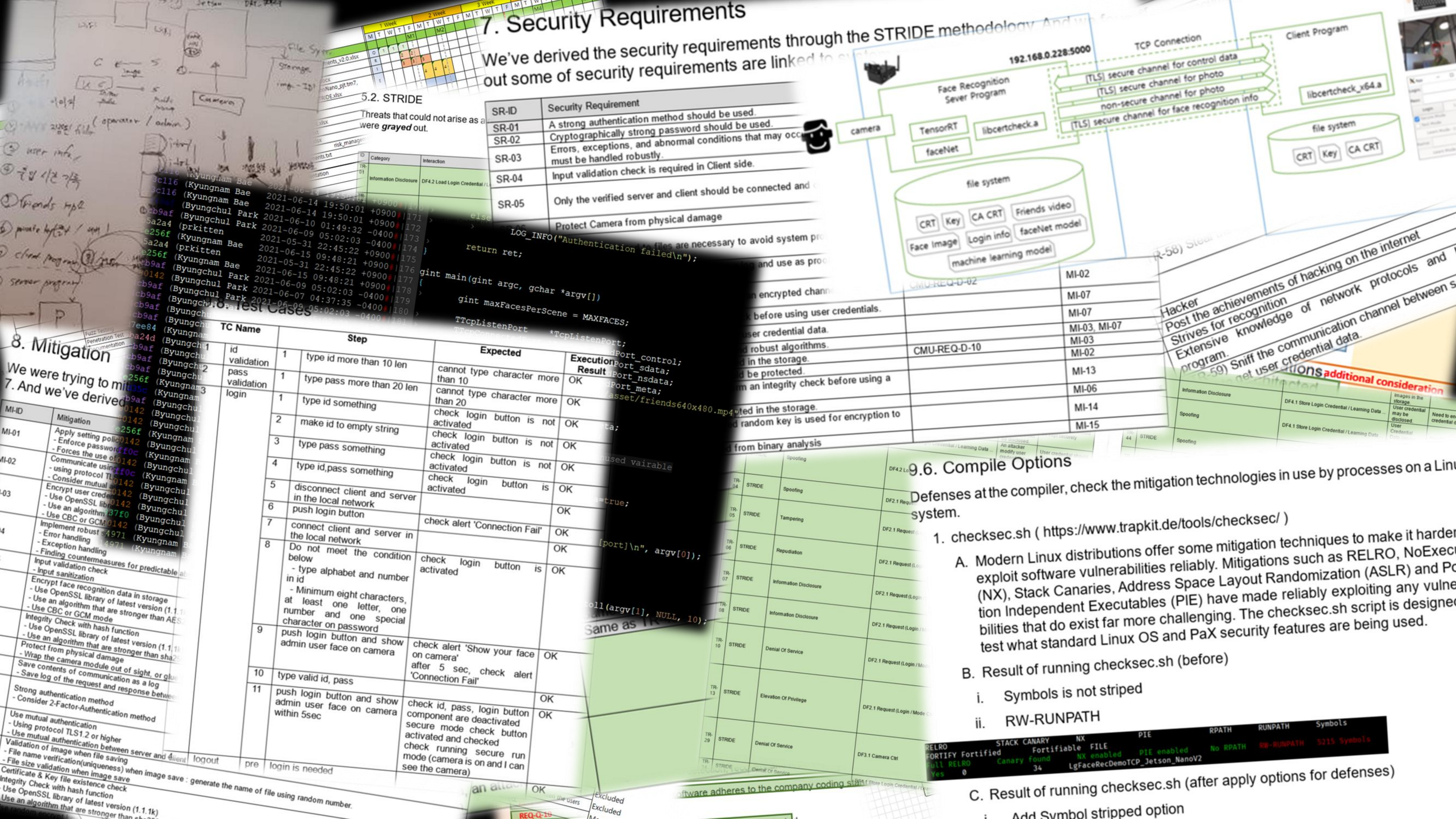
9.6. Compile Options

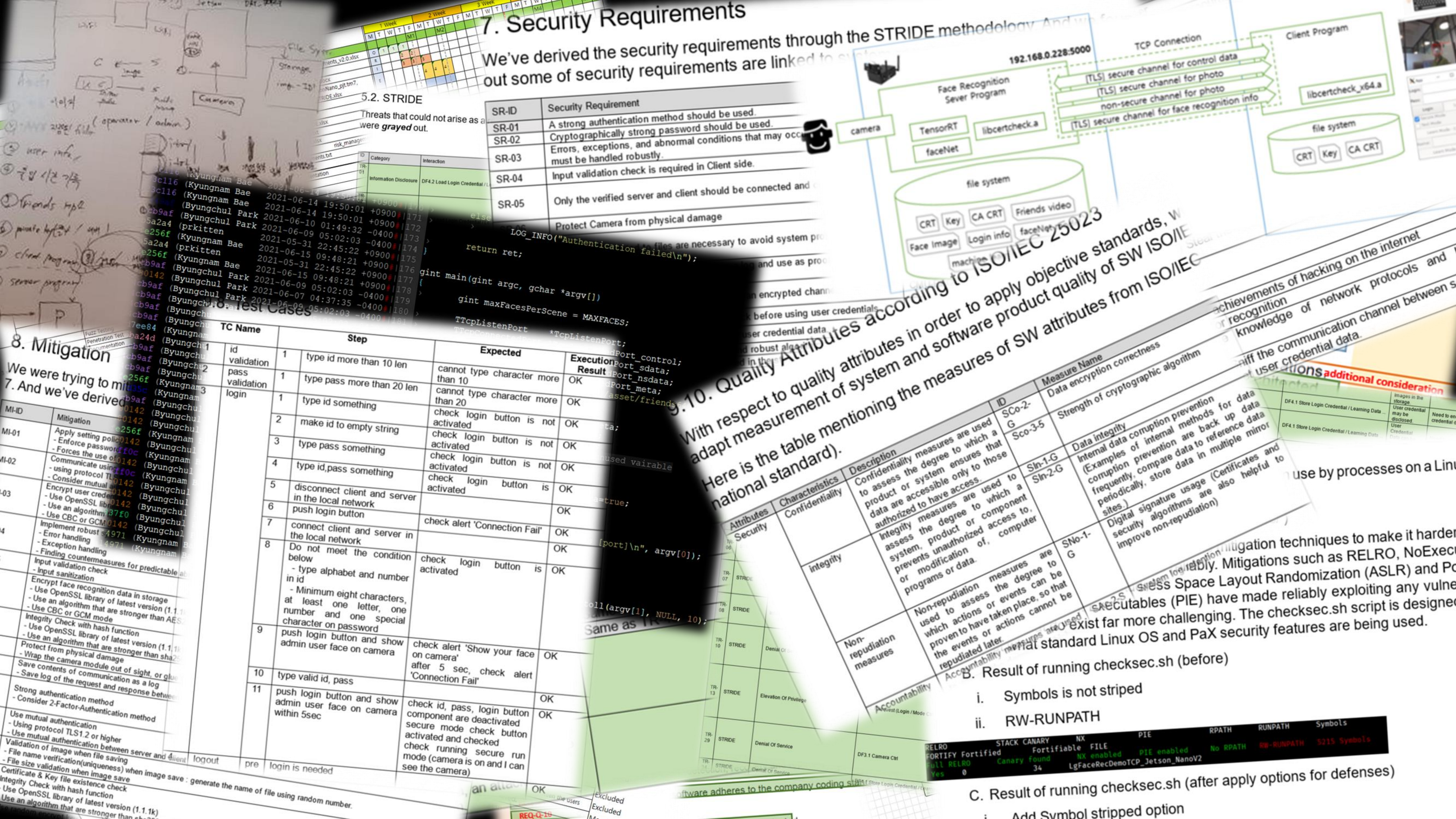
Defenses at the compiler, check the mitigation technologies in use by processes on a Linu
system.

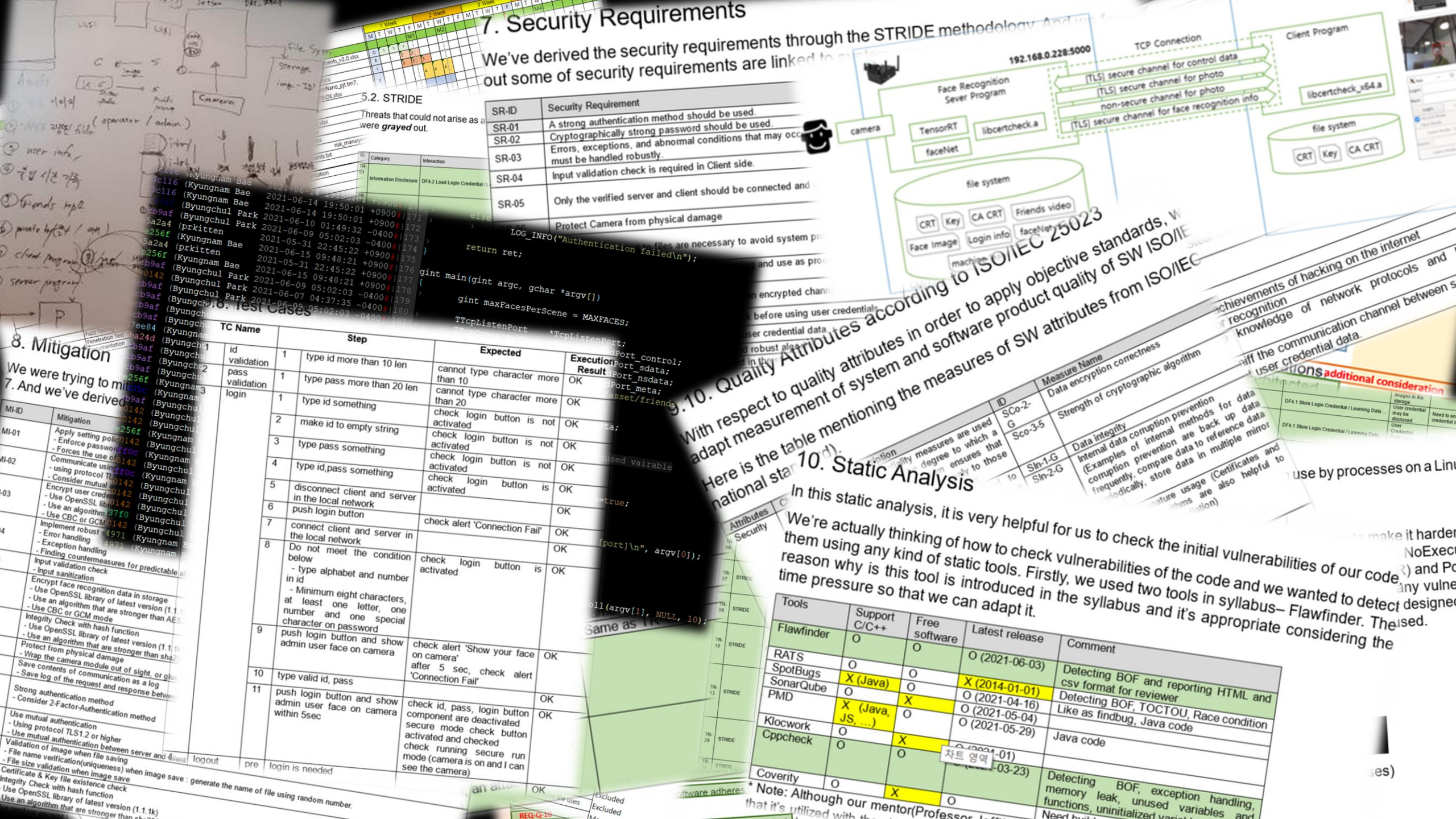
1. checksec.sh (https://www.trapkit.de/tools/checksec/)
   A. Modern Linux distributions offer some mitigation techniques to make it harder
   exploit software vulnerabilities reliably. Mitigations such as RELRO, NoExecu
   (NX), Stack Canaries, Address Space Layout Randomization (ASLR) and Po
   tion Independent Executables (PIE) have made reliably exploiting any vulne
   bilities that do exist far more challenging. The checksec.sh script is designe
   test what standard Linux OS and PaX security features are being used.
   B. Result of running checksec.sh (before)
      i. Symbols is not striped
      ii. RW-RUNPATH

```
RELRO           STACK CANARY      NX            PIE             RPATH      RUNPATH      Symbols
FORTIFY Fortified      Fortifiable  FILE
Full RELRO      Canary found      NX enabled    PIE enabled     No RPATH   RW-RUNPATH   5215 Symbols
Yes  0          34                LgFaceRecDemoTCP_Jetson_NanoV2
```

   C. Result of running checksec.sh (after apply options for defenses)
      i. Add Symbol stripped option


7. Security Requirements
We've derived the security requirements through the STRIDE methodology.
5.2. STRIDE
8. Mitigation
8. Test Cases
9.6. Compile Options
Face Recognition Sever Program
Client Program
TCP Connection
192.168.0.228:5000
file system
checksec.sh (https://www.trapkit.de/tools/checksec/)
B. Result of running checksec.sh (before)
C. Result of running checksec.sh (after apply options for defenses)


7. Security Requirements
We've derived the security requirements through the STRIDE methodology.
5.2. STRIDE
8. Mitigation
8. Test Cases
9.10. Quality Attributes according to ISO/IEC 25023
With respect to quality attributes in order to apply objective standards,
adapt measurement of system and software product quality of SW ISO/IEC
Here is the table mentioning the measures of SW attributes from ISO/IEC
national standard).
B. Result of running checksec.sh (before)
i. Symbols is not striped
ii. RW-RUNPATH
C. Result of running checksec.sh (after apply options for defenses)
Add Symbol stripped option



7. Security Requirements

We've derived the security requirements through the STRIDE methodology. And we f
out some of security requirements are linked to s

SR-ID	Security Requirement
SR-01	A strong authentication method should be used.
SR-02	Cryptographically strong password should be used.
SR-03	Errors, exceptions, and abnormal conditions that may occ must be handled robustly.
SR-04	Input validation check is required in Client side.
SR-05	Only the verified server and client should be connected and
	Protect Camera from physical damage

5.2. STRIDE

Threats that could not arise as a
were ***grayed*** out.

ID	Category	Interaction
TR-01	Information Disclosure	DF4.2 Load Login Credential / L

```
    LOG_INFO("Authentication failed\n");
  return ret;

gint main(gint argc, gchar *argv[])
{
  gint maxFacesPerScene = MAXFACES;

  TTcpListenPort    *TcpListenPort;
                                    Port_control;
                                    Port_sdata;
                                    Port_nsdata;
                                    Port_meta;
                                    asset/friends
                                    ta;
                                    used vairable
                                    =true;
                                    [port]\n", argv[0]);
                                    ll(argv[1], NULL, 10);
```

8. Test Cases

TC	TC Name	Step	Expected	Execution Result
1	id validation	1 type id more than 10 len	cannot type character more than 10	OK
2	pass validation	1 type pass more than 20 len	cannot type character more than 20	OK
3	login	1 type id something	check login button is not activated	OK
		2 make id to empty string	check login button is not activated	OK
		3 type pass something	check login button is not activated	OK
		4 type id,pass something	check login button is activated	OK
		5 disconnect client and server in the local network		OK
		6 push login button	check alert 'Connection Fail'	OK
		7 connect client and server in the local network		OK
		8 Do not meet the condition below - type alphabet and number in id - Minimum eight characters, at least one letter, one number and one special character on password	check login button is activated	OK
		9 push login button and show admin user face on camera	check alert 'Show your face on camera' after 5 sec, check alert 'Connection Fail'	OK
		10 type valid id, pass		OK
		11 push login button and show admin user face on camera within 5sec	check id, pass, login button component are deactivated secure mode check button activated and checked check running secure run mode (camera is on and I can see the camera)	OK
	logout	pre login is needed		OK

8. Mitigation

We were trying to mi
7. And we've derived

MI-ID	Mitigation
MI-01	Apply setting poli - Enforce password - Forces the use o
MI-02	Communicate using - using protocol T - Consider mutual a
-03	Encrypt user crede - Use OpenSSL libr - Use an algorithm - Use CBC or GCM
4	Implement robust - Error handling - Exception handling - Finding countermeasures for predictable
	Input validation check - Input sanitization
	Encrypt face recognition data in storage - Use OpenSSL library of latest version (1.1.1 - Use an algorithm that are stronger than AES - Use CBC or GCM mode
	Integrity Check with hash function - Use OpenSSL library of latest version (1.1.1 - Use an algorithm that are stronger than sha2
	Protect from physical damage - Wrap the camera module out of sight, or glu
	Save contents of communication as a log - Save log of the request and response betwe
	Strong authentication method - Consider 2-Factor-Authentication method
	Use mutual authentication - Using protocol TLS1.2 or higher - Use mutual authentication between server and client
	Validation of image when file saving - File name verification(uniqueness) when image save : generate the name of file using random number. - File size validation when image save
	Certificate & Key file existence check
	Integrity Check with hash function - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than sha2

9.10. Quality Attributes according to ISO/IEC 25023

With respect to quality attributes in order to apply objective standards, w
adapt measurement of system and software product quality of SW ISO/IE
Here is the table mentioning the measures of SW attributes from ISO/IEC
national star

ID	Measure Name
SCo-2-G	Data encryption correctness
Sco-3-5	Strength of cryptographic algorithm
Sln-1-G	Data integrity
Sln-2-G	Internal data corruption prevention (Examples of internal methods for data corruption prevention are back up data frequently, compare data to reference data periodically, store data in multiple mirror
	nature usage (Certificates and rithms are also helpful to

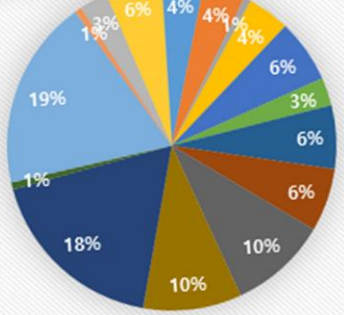
10. Static Analysis

In this static analysis, it is very helpful for us to check the initial vulnerabilities of our code
them using any kind of static tools. Firstly, we used two tools in syllabus– Flawfinder. The
reason why is this tool is introduced in the syllabus and it's appropriate considering the
time pressure so that we can adapt it.

Tools	Support C/C++	Free software	Latest release	Comment
Flawfinder	O	O	O (2021-06-03)	Detecting BOF and reporting HTML and csv format for reviewer
RATS	O	O	X (2014-01-01)	Detecting BOF, TOCTOU, Race condition
SpotBugs	X (Java)	O	O (2021-04-16)	Like as findbug, Java code
SonarQube	O	X	O (2021-05-04)	
PMD	X (Java, JS, ...)	O	O (2021-05-29)	Java code
Klocwork	O	X	O (2021-01)	
Cppcheck	O	O	(2021-03-23)	Detecting BOF, exception handling, memory leak, unused variables and functions, uninitialized variable
Coverity	O	X	O	Need b

* Note: Although our mentor(Professor
that it's utilized with

차트 영역



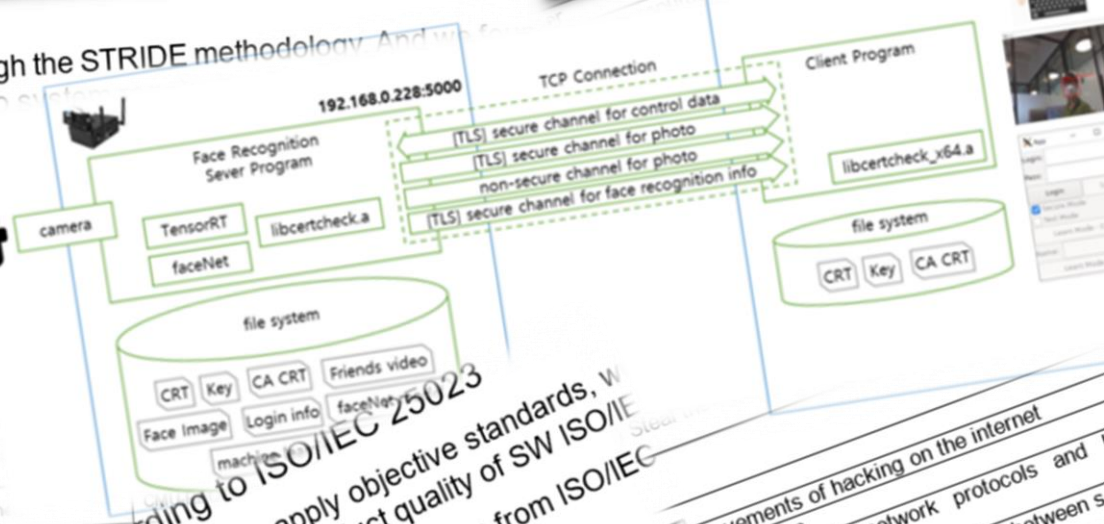
ctuOneDefinitionRuleViolation
noCopyConstructor
passedByValue
unreadVariable
unusedLabel
invalidPointerCast
noExplicitConstructor
postfixOperator
unsignedLessThanZero
useInitializationList

Parameter
ngOverride
eratorEq
tMemberVar
edFunction
bleScope

7. Security Requirements

We've derived the security requirements through the STRIDE methodology. And we
out some of security requirements are linked to

SR-ID	Security Requirement
SR-01	A strong authentication method should be used.
SR-02	Cryptographically strong password should be used.
SR-03	Errors, exceptions, and abnormal conditions that may occ must be handled robustly.
SR-04	Input validation check is required in Client side.
SR-05	Only the verified server and client should be connected and
	Protect Camera from physical damage




```
LOG_INFO("Authentication failed\n");
return ret;

gint main(gint argc, gchar *argv[])
{
    gint maxFacesPerScene = MAXFACES;

    TTcpListenPort    *TcpListenPort;
                                    Port_control;
                                    Port_sdata;
                                    Port_nsdata;
                                    Port_meta;
                                    asset/friends
                                                    ta;
                                                    used vairable
                                                    =true;
                                                    [port]\n", argv[0]);
                                                    oll(argv[1], NULL, 10);
```

8. Mitigation

We were trying to mi
7. And we've derived

MI-ID	Mitigation
MI-01	Apply setting poli - Enforce password - Forces the use of
MI-02	Communicate using - using protocol TL - Consider mutual a
-03	Encrypt user crede - Use OpenSSL libr - Use an algorithm - Use CBC or GCM
4	Implement robust - Error handling - Exception handling - Finding countermeasures for predictable
	Input validation check - Input sanitization
	Encrypt face recognition data in storage - Use OpenSSL library of latest version (1.1. - Use an algorithm that are stronger than AES - Use CBC or GCM mode
	Integrity Check with hash function - Use OpenSSL library of latest version (1.1.1 - Use an algorithm that are stronger than sha2
	Protect from physical damage - Wrap the camera module out of sight, or glu
	Save contents of communication as a log - Save log of the request and response betwe
	Strong authentication method - Consider 2-Factor-Authentication method
	Use mutual authentication - Using protocol TLS1.2 or higher - Use mutual authentication between server and client
	Validation of image when file saving - File name verification(uniqueness) when image save : generate the name of file using random number. - File size validation when image save
	Certificate & Key file existence check
	Integrity Check with hash function - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than sha2

9. Test Cases

TC Name	Step		Expected	Execution Result
id validation	1	type id more than 10 len	cannot type character more than 10	OK
pass validation	1	type pass more than 20 len	cannot type character more than 20	OK
login	1	type id something	check login button is not activated	OK
	2	make id to empty string	check login button is not activated	OK
	3	type pass something	check login button is not activated	OK
	4	type id,pass something	check login button is activated	OK
	5	disconnect client and server in the local network		OK
	6	push login button	check alert 'Connection Fail'	OK
	7	connect client and server in the local network		OK
	8	Do not meet the condition below - type alphabet and number in id - Minimum eight characters, at least one letter, one number and one special character on password	check login button is activated	OK
	9	push login button and show admin user face on camera	check alert 'Show your face on camera' after 5 sec, check alert 'Connection Fail'	OK
	10	type valid id, pass		OK
	11	push login button and show admin user face on camera within 5sec	check id, pass, login button component are deactivated secure mode check button activated and checked check running secure run mode (camera is on and I can see the camera)	OK
logout	pre	login is needed		OK

9.10. Quality Attributes according to ISO/IEC 25023

With respect to quality attributes in order to apply objective standards, w
adapt measurement of system and software product quality of SW ISO/IE
Here is the table mentioning the measures of SW attributes from ISO/IEC
national star

ID	Measure Name
SCo-2-G	Data encryption correctness
Sco-3-5	Strength of cryptographic algorithm
Sln-1-G	Data integrity
Sln-2-G	Internal data corruption prevention (Examples of internal methods for data corruption prevention are back up data frequently, compare data to reference data periodically, store data in multiple mirror

ature usage (Certificates and
rithms are also helpful to
ation)

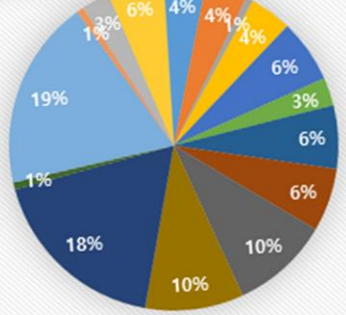
10. Static Analysis

In this static analysis, it is very helpful for us to check the initial vulnerabilities of our code
them using any kind of static tools. Firstly, we used two tools in syllabus– Flawfinder. The
reason why is this tool is introduced in the syllabus and it's appropriate considering the
time pressure so that we can adapt it.

Tools	Support C/C++	Free software	Latest release	Comment
Flawfinder	O	O	O (2021-06-03)	Detecting BOF and reporting HTML and csv format for reviewer
RATS	O	O	X (2014-01-01)	Detecting BOF, TOCTOU, Race condition
SpotBugs	X (Java)	O	O (2021-04-16)	Like as findbug, Java code
SonarQube	O	X	O (2021-05-04)	
PMD	X (Java, JS, ...)	O	O (2021-05-29)	Java code
Klocwork	O	X	O (2021-01)	
Cppcheck	O	O	(2021-03-23)	Detecting BOF, exception handling, memory leak, unused variables and functions, uninitialized variable
Coverity	O	X	O	Need build

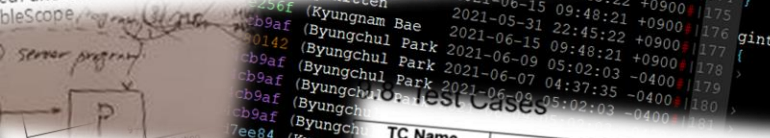
* Note: Although our mentor(Professor
that it's utilized with

차트 영역



ctuOneDefinitionRuleViolation
noCopyConstructor
passedByValue
unreadVariable
unusedLabel
invalidPointerCast
noExplicitConstructor
postfixOperator
unsignedLessThanZero
useInitializationList

Parameter
ngOverride
eratorEq
tMemberVar
edFunction
bleScope



7. Security Requirements

We've derived the security requirements through the STRIDE methodology. And we f
out some of security requirements are linked to s

SR-ID	Security Requirement
SR-01	A strong authentication method should be used.
SR-02	Cryptographically strong password should be used.
SR-03	Errors, exceptions, and abnormal conditions that may occ must be handled robustly.
SR-04	Input validation check is required in Client side.
SR-05	Only the verified server and client should be connected and
	Protect Camera from physical damage


```
    LOG_INFO("Authentication failed\n");
  return ret;

gint main(gint argc, gchar *argv[])
{
  gint maxFacesPerScene = MAXFACES;

  TTcpListenPort  *TcpListenPort;
                                    Port_control;
                                    Port_sdata;
                                    Port_nsdata;
                                    Port_meta;
                                    sset/friends
                                    ta;
                                    used vairable
                                    =true;
                                    [port]\n", argv[0]);
                                    oll(argv[1], NULL, 10);
```

8. Mitigation

We were trying to mi
7. And we've derived

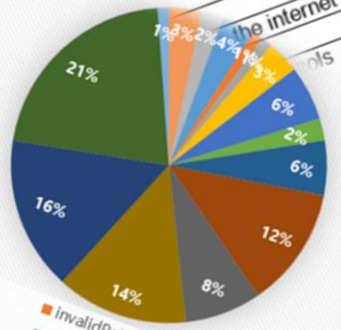
MI-ID	Mitigation
MI-01	Apply setting polic - Enforce password - Forces the use of
MI-02	Communicate using - using protocol TL - Consider mutual a Encrypt user crede - Use OpenSSL libr - Use an algorithm - Use CBC or GCM
03	Implement robust - Error handling - Exception handling - Finding countermeasures for predictable
4	Input validation check - Input sanitization Encrypt face recognition data in storage - Use OpenSSL library of latest version (1.1.1 - Use an algorithm that are stronger than AES - Use CBC or GCM mode Integrity Check with hash function - Use OpenSSL library of latest version (1.1.1 - Use an algorithm that are stronger than sha2 Protect from physical damage - Wrap the camera module out of sight, or glu Save contents of communication as a log - Save log of the request and response betwe Strong authentication method - Consider 2-Factor-Authentication method Use mutual authentication - Using protocol TLS1.2 or higher - Use mutual authentication between server and client Validation of image when file saving - File name verification(uniqueness) when image save : generate the name of file using random number. - File size validation when image save Certificate & Key file existence check Integrity Check with hash function Use OpenSSL library of latest version (1.1.1k) Use an algorithm that are stronger than sha2

o. Test Cases

TC Name	Step		Expected	Execution Result
id validation	1	type id more than 10 len	cannot type character more than 10	OK
pass validation	1	type pass more than 20 len	cannot type character more than 20	OK
login	1	type id something	check login button is not activated	OK
	2	make id to empty string	check login button is not activated	OK
	3	type pass something	check login button is not activated	OK
	4	type id,pass something	check login button is activated	OK
	5	disconnect client and server in the local network		OK
	6	push login button	check alert 'Connection Fail'	OK
	7	connect client and server in the local network		OK
	8	Do not meet the condition below - type alphabet and number in id - Minimum eight characters, at least one letter, one number and one special character on password	check login button is activated	OK
	9	push login button and show admin user face on camera	check alert 'Show your face on camera' after 5 sec, check alert 'Connection Fail'	OK
	10	type valid id, pass		OK
	11	push login button and show admin user face on camera within 5sec	check id, pass, login button component are deactivated secure mode check button activated and checked check running secure run mode (camera is on and I can see the camera)	OK
logout	pre	login is needed		OK

9.10. Quality Attributes according to ISO/IEC 25023

With respect to quality attributes in order to apply objective standar
adapt measurement of system and software product quality of SW
Here is the table mentioning the measures of SW attributes fr
national star d).



constParameter
missingOverride
noOperatorEq
uninitMemberVar
invalidPointerCast
noCopyConstructor
passedByValue
unreadVariable

ID	Measure Name
SCo-2-G	Data encry
Sco-3-5	Strengt
	Data integrity
Sln-1-G	Internal data co
Sln-2-G	(Examples of inte corruption prevention frequently, compare data periodically, store data in

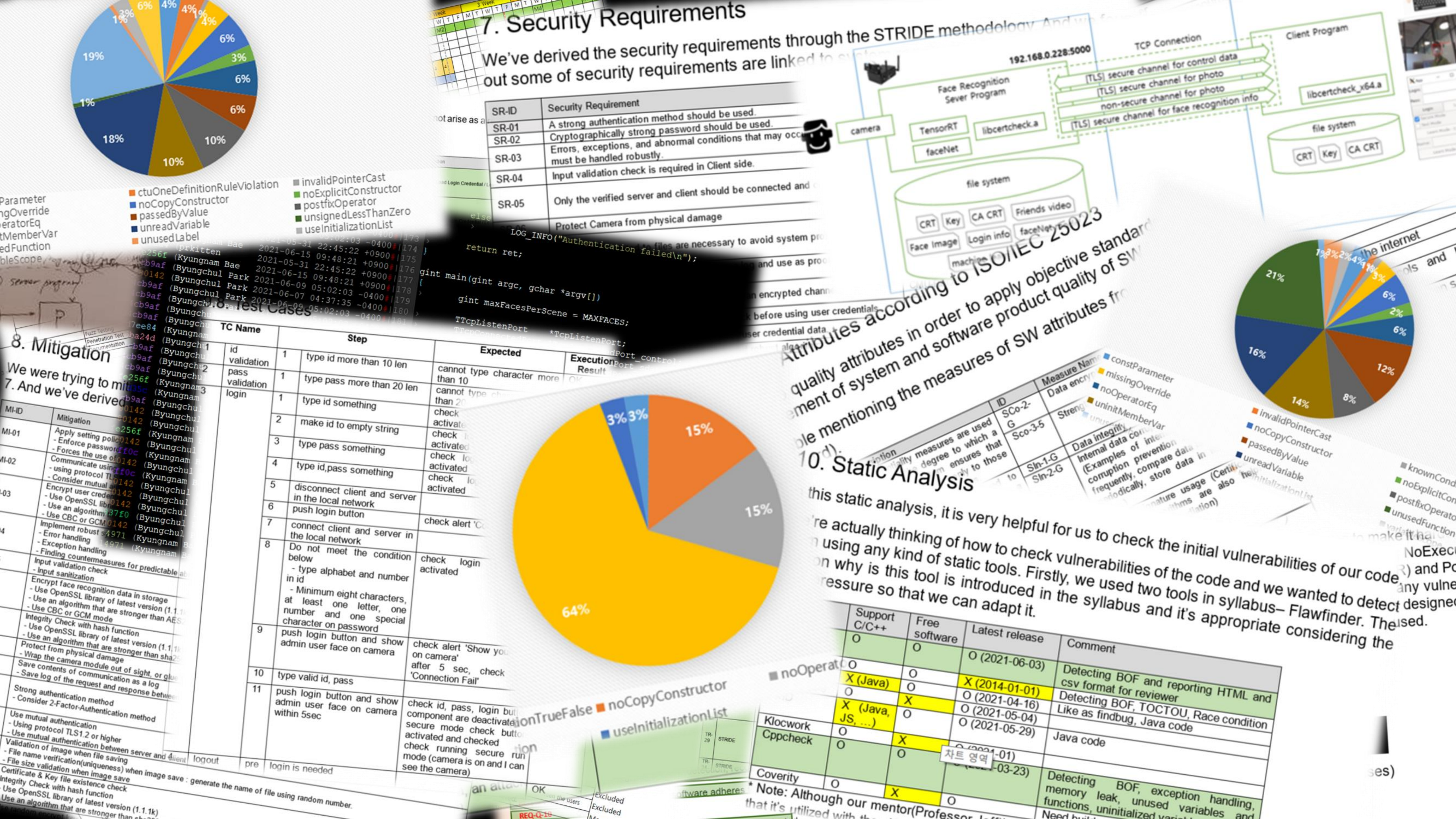
10. Static Analysis

In this static analysis, it is very helpful for us to check the initial vulnerabilities of our code
them using any kind of static tools. Firstly, we used two tools in syllabus– Flawfinder. The
reason why is this tool is introduced in the syllabus and it's appropriate considering the
time pressure so that we can adapt it.

Tools	Support C/C++	Free software	Latest release	Comment
Flawfinder	O	O	O (2021-06-03)	Detecting BOF and reporting HTML and csv format for reviewer
RATS	O	O	X (2014-01-01)	Detecting BOF, TOCTOU, Race condition
SpotBugs	X (Java)	O	O (2021-04-16)	Like as findbug, Java code
SonarQube	O	X	O (2021-05-04)	
PMD	X (Java, JS, ...)	O	O (2021-05-29)	Java code
Klocwork	O	X	O (2021-01)	
Cppcheck	O	O	(2021-03-23)	Detecting BOF, exception handling, memory leak, unused variables and functions, uninitialized variable
Coverity	O	X	O	Need build

차트 영역

* Note: Although our mentor(Professor
that it's utilized with the


7. Security Requirements
We've derived the security requirements through the STRIDE methodology.
out some of security requirements are linked to
SR-ID
Security Requirement
SR-01
A strong authentication method should be used.
SR-02
Cryptographically strong password should be used.
SR-03
Errors, exceptions, and abnormal conditions that may occ
must be handled robustly.
SR-04
Input validation check is required in Client side.
SR-05
Only the verified server and client should be connected and
Protect Camera from physical damage
192.168.0.228:5000
TCP Connection
Client Program
Face Recognition
Sever Program
camera
TensorRT
libcertcheck.a
faceNet
file system
CRT
Key
CA CRT
Friends video
Face Image
Login info
[TLS] secure channel for control data
[TLS] secure channel for photo
non-secure channel for photo
[TLS] secure channel for face recognition info
libcertcheck_x64.a
ctuOneDefinitionRuleViolation
noCopyConstructor
passedByValue
unreadVariable
unusedLabel
invalidPointerCast
noExplicitConstructor
postfixOperator
unsignedLessThanZero
useInitializationList
LOG_INFO("Authentication failed\n");
return ret;
gint main(gint argc, gchar *argv[])
gint maxFacesPerScene = MAXFACES;
8. Test Cases
TC Name
Step
Expected
Execution Result
id validation
type id more than 10 len
cannot type character more than 10
pass validation
type pass more than 20 len
login
type id something
make id to empty string
type pass something
type id,pass something
disconnect client and server in the local network
push login button
connect client and server in the local network
Do not meet the condition below
- type alphabet and number in id
- Minimum eight characters, at least one letter, one number and one special character on password
push login button and show admin user face on camera
type valid id, pass
push login button and show admin user face on camera within 5sec
logout
login is needed
8. Mitigation
We were trying to mi
7. And we've derived
Mitigation
Strong authentication method
- Consider 2-Factor-Authentication method
Use mutual authentication
- Using protocol TLS1.2 or higher
Attributes according to ISO/IEC 25023
quality attributes in order to apply objective standard
ment of system and software product quality of SW
le mentioning the measures of SW attributes fr
10. Static Analysis
this static analysis, it is very helpful for us to check the initial vulnerabilities of our code
re actually thinking of how to check vulnerabilities of the code and we wanted to detect
using any kind of static tools. Firstly, we used two tools in syllabus– Flawfinder. The
n why is this tool is introduced in the syllabus and it's appropriate considering the
ressure so that we can adapt it.
Support C/C++
Free software
Latest release
Comment
O (2021-06-03)
Detecting BOF and reporting HTML and csv format for reviewer
X (2014-01-01)
Detecting BOF, TOCTOU, Race condition
Like as findbug, Java code
Java code
Klocwork
Cppcheck
Coverity
Detecting BOF, exception handling, memory leak, unused variables, and functions, uninitialized variable
Note: Although our mentor(Professor
64%
15%
15%
3%
3%
21%
16%
14%
12%
8%
19%
18%
10%
10%

Define security goal

Define assets to protect

Do threat modeling

Do risk assessment to prioritize items

Define security requirements

Derive mitigations

Construct architecture

Implement the mitigations

Verify the mitigations

Define security goal

“ Protect the user privacy information in our system. ”

Define assets to protect + Do threat modeling

+ name

Define assets to protect + Do threat modeling

#privacy #stalker
#name

+ name

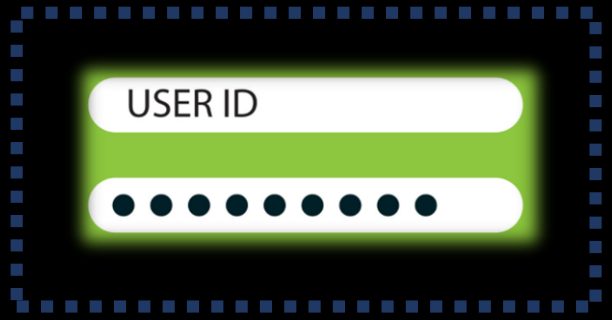
Define assets to protect + Do threat modeling

#privacy #stalker
#name

+ name

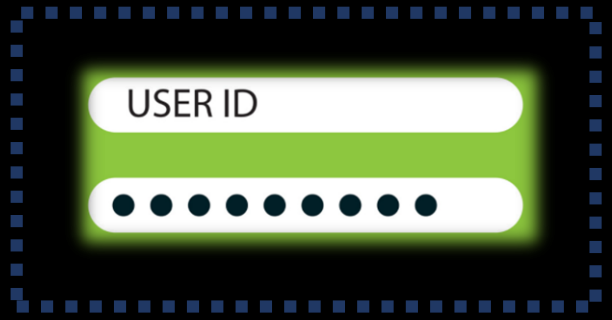
#authentication #2FA
#face #recognition

Define assets to protect + Do threat modeling



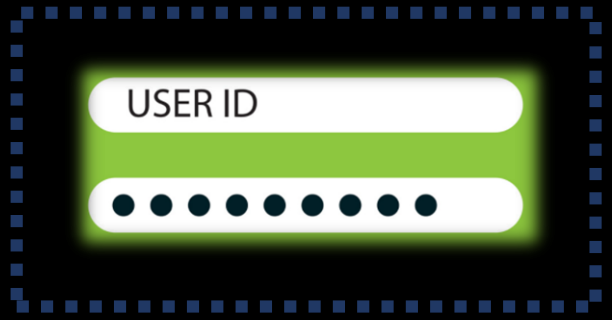
Define assets to protect + Do threat modeling

#authentication
#login #password



Define assets to protect + Do threat modeling

#authentication
#login #password



#privacy

Define assets to protect + Do threat modeling

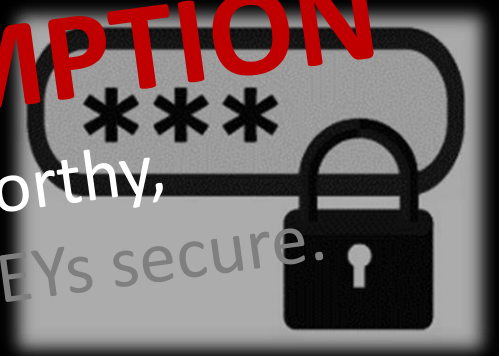
Define assets to protect + Do threat modeling

#privacy

#authentication

Define assets to protect + Do threat modeling

#privacy



#authentication

IMPORTANT ASSUMPTION

The root of trust is trustworthy,

which is the way to keep the KEYs secure.

Derive mitigations

+ name

Introduce login system

Force users to use strong password

Apply 2FA (what you know + what you are)

Separate meta data from image on network

Encrypt the image + name in the storage

Use verified crypto algorithm (AES256-CBC)

Use a random file name in the storage

Use TLS in network communication

Derive mitigations

+ name

Introduce login system

Force users to use strong password

Apply 2FA (what you know + what you are)

Separate meta data from image on network

Encrypt the image + name in the storage

Use verified crypto algorithm (AES256-CBC)

Use a random file name in the storage

Use TLS in network communication

Derive mitigations

\+ name

Introduce login system

Force users to use strong password

Apply 2FA (what you know + what you are)

Separate meta data from image on network

Encrypt the image + name in the storage

Use verified crypto algorithm (AES256-CBC)

Use a random file name in the storage

Use TLS in network communication

Derive mitigations

+ name

Introduce login system

Force users to use strong password

Apply 2FA (what you know + what you are)

Separate meta data from image on network

Encrypt the image + name in the storage

Use verified crypto algorithm (AES256-CBC)

Use a random file name in the storage

Use TLS in network communication

Derive mitigations

+ name

Introduce login system

Force users to use strong password

Apply 2FA (what you know + what you are)

Separate meta data from image on network

Encrypt the image + name in the storage

Use verified crypto algorithm (AES256-CBC)

Use a random file name in the storage

Use TLS in network communication

Derive mitigations

\+ name

Introduce login system

Force users to use strong password

Apply 2FA (what you know + what you are)

Separate meta data from image on network

Encrypt the image + name in the storage

Use verified crypto algorithm (AES256-CBC)

Use a random file name in the storage

Use TLS in network communication

Derive mitigations

+ name

Introduce login system

Force users to use strong password

Apply 2FA (what you know + what you are)

Separate meta data from image on network

Encrypt the image + name in the storage

Use verified crypto algorithm (AES256-CBC)

Use a random file name in the storage

Use TLS in network communication

Derive mitigations

+ name

Introduce login system

Force users to use strong password

Apply 2FA (what you know + what you are)

Separate meta data from image on network

Encrypt the image + name in the storage

Use verified crypto algorithm (AES256-CBC)

Use a random file name in the storage

Use TLS in network communication

Derive mitigations

+ name

Introduce login system

Force users to use strong password

Apply 2FA (what you know + what you are)

Separate meta data from image on network

Encrypt the image + name in the storage

Use verified crypto algorithm (AES256-CBC)

Use a random file name in the storage

Use TLS in network communication

Derive mitigations

Encrypt the hashed credential in the storage

Use TLS in network communication

Derive mitigations

Encrypt the hashed credential in the storage

Use TLS in network communication

Derive mitigations

Encrypt the hashed credential in the storage

Use TLS in network communication

Derive mitigations

Embed the root key into code obfuscated

Use TLS in network communication

Derive mitigations

Embed the root key into code obfuscated

Use TLS in network communication

Derive mitigations

Embed the root key into code obfuscated

Use TLS in network communication

Derive mitigations

Introduce login system

Force users to use strong password

Encrypt the hashed credential in the storage

Apply 2FA (what you know + what you are)

Separate meta data from image on network

Encrypt the image + name in the storage

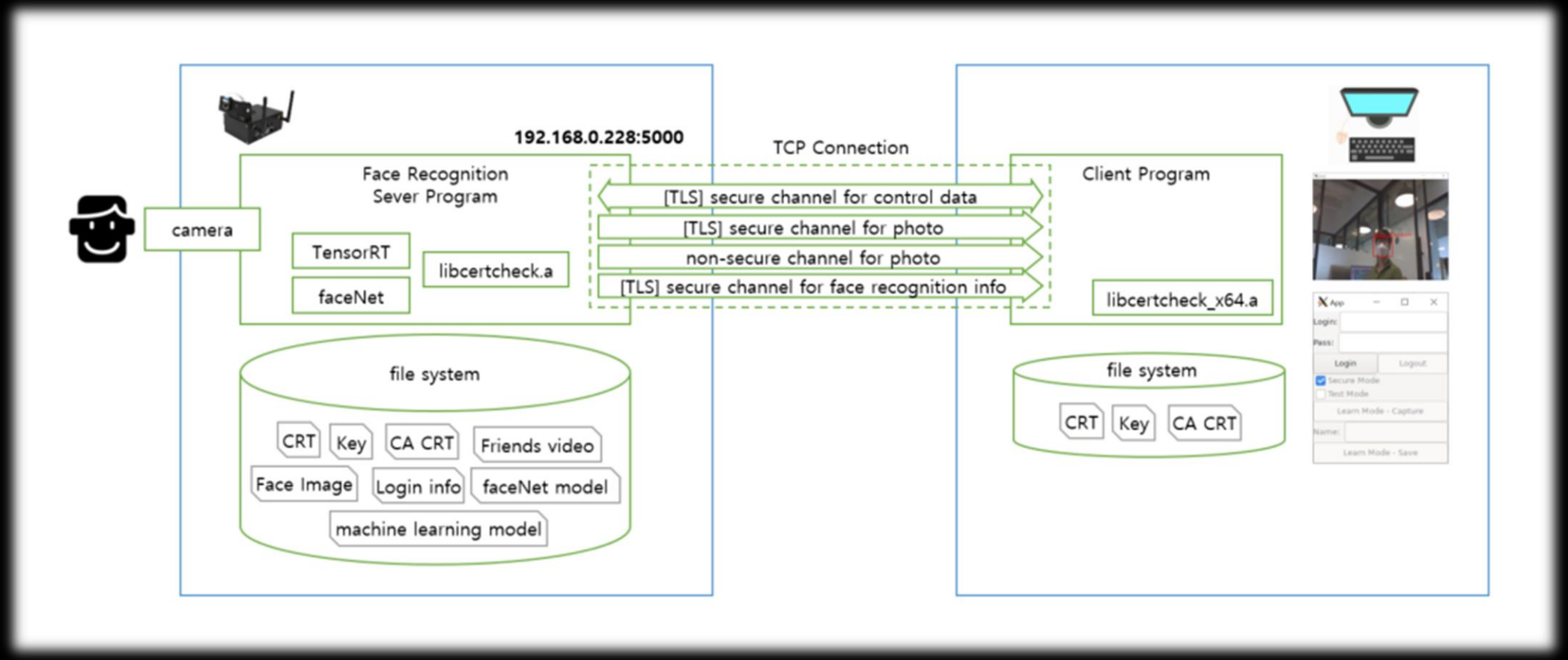
Use verified crypto algorithm (AES256-CBC)

Embed the root key into code obfuscated

Use a random file name in the storage

Use TLS in network communication

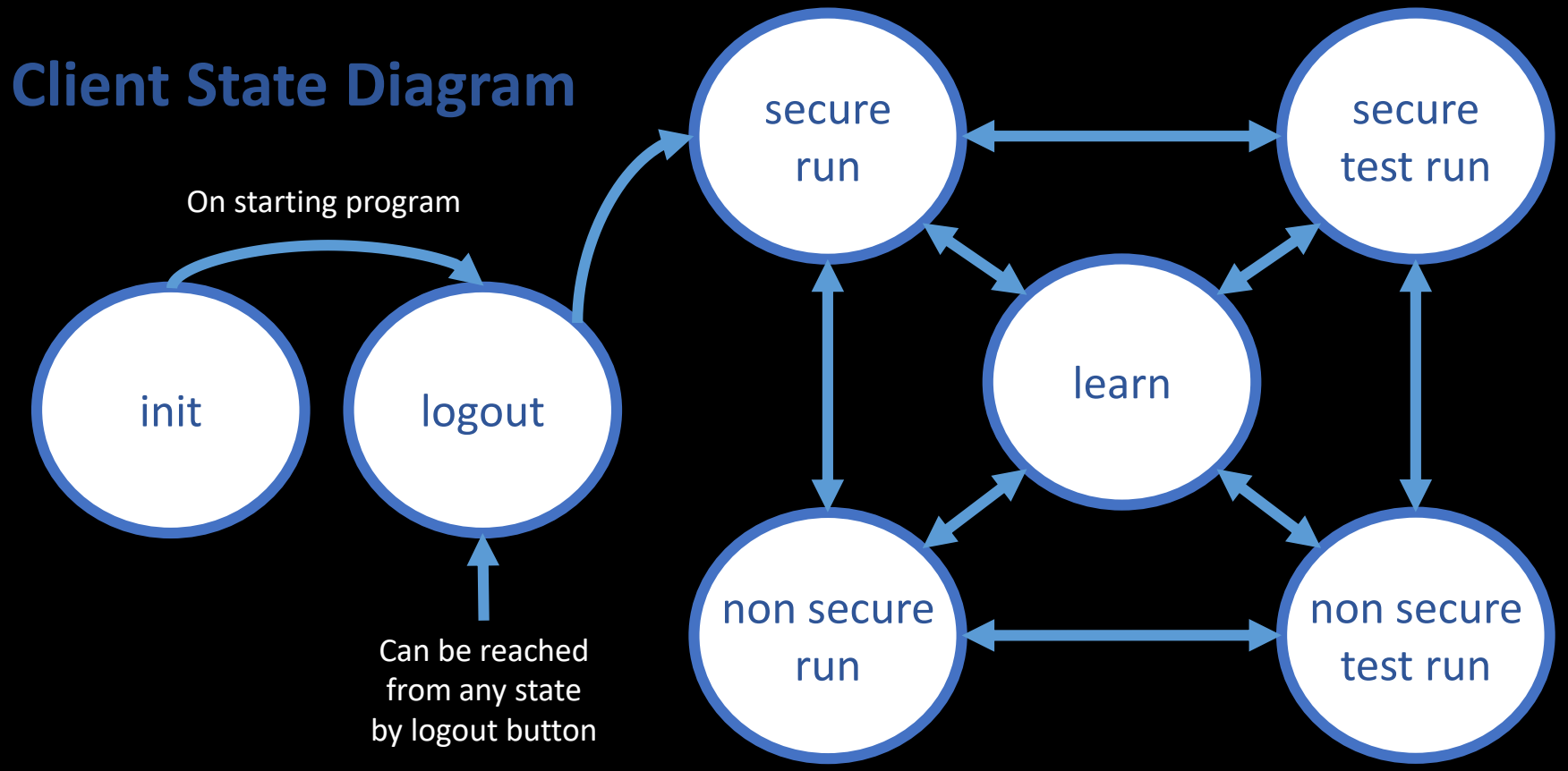
Construct architecture



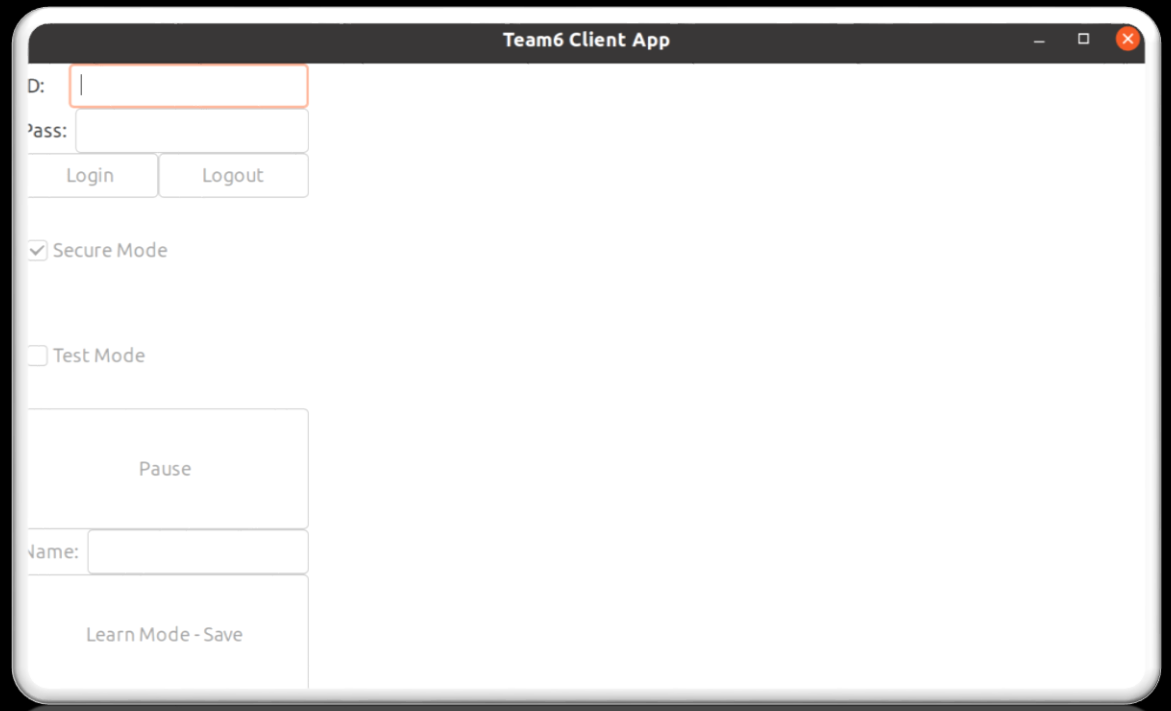
Construct architecture

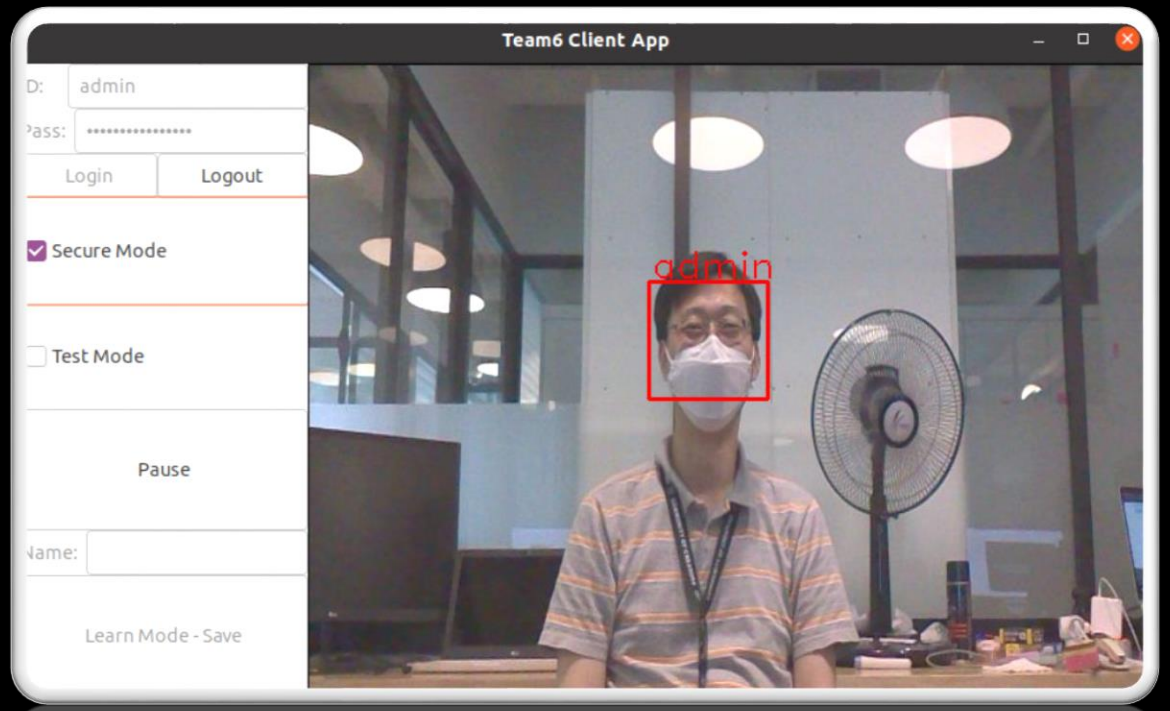
```
.
└── source
    ├── client
    │   └── src                    // client source codes
    ├── common
    │   ├── keys
    │   │   ├── ca                 // self signed root certificate
    │   │   ├── client             // CA signed certificate & Private key for client
    │   │   └── server             // CA signed certificate & Private key for server
    │   └── libs
    │       └── libcertcheck       // crypto library to support crypto API and to verify the integrity of keys.
    │                              // the root key for the crypto API are included as a string with obfuscated.
    └── server
        ├── facenetModels          // the path of faceNet models
        ├── imgs                   // the path of the photo registered with name. the filename and contents are encrypted
        ├── mtCNNModels            // the path of machine learning model in MTCNN_FaceDetection_TensorRT
        ├── src                    // server source codes
        └── trt_l2norm_helper      // TensorRT L2-Norm Helper
```

Construct architecture



Construct architecture





Construct architecture

Let me show you demo clip..