

CMU Security Specialist Course

Team Project : Phase 1

Team 6 a.k.a. six senses

Seongju Moon (L)

Kyungnam Bae (E)

Jinmo Kim (A)

Jeonghwan Ahn (S)

* Byungchul Park (C)



Define security goal

Define assets to protect

Do threat modeling

Do risk assessment to prioritize items

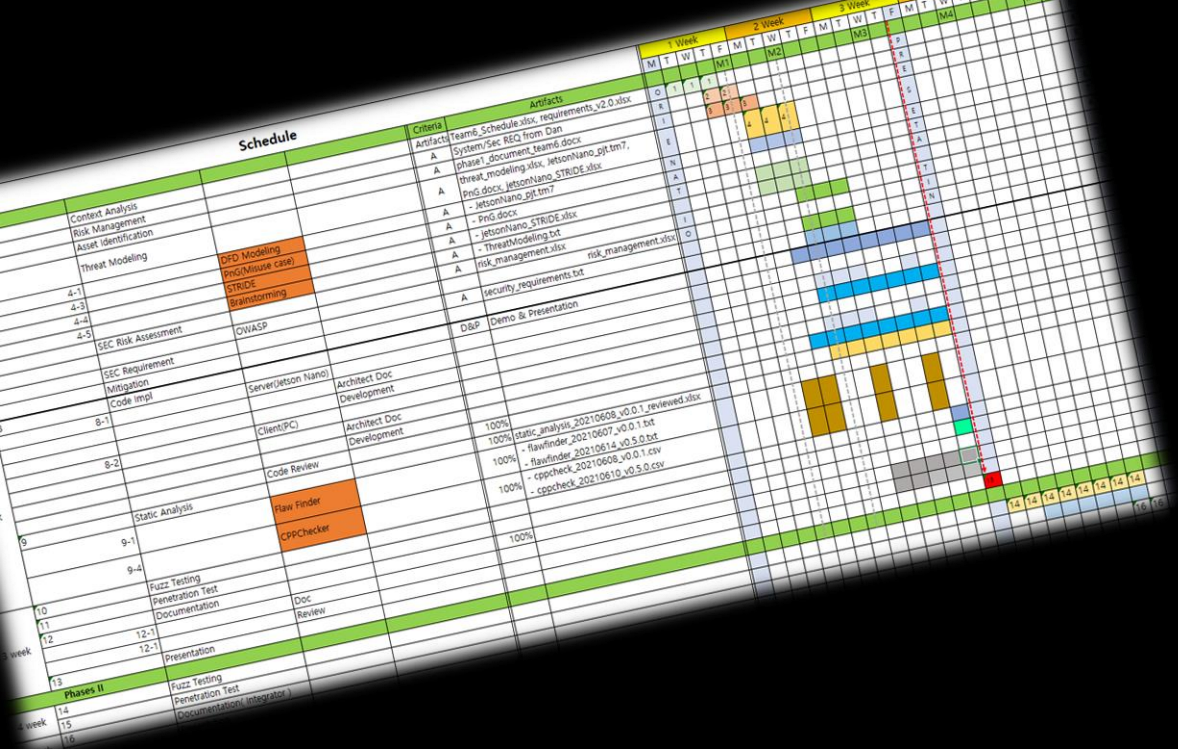
Define security requirements

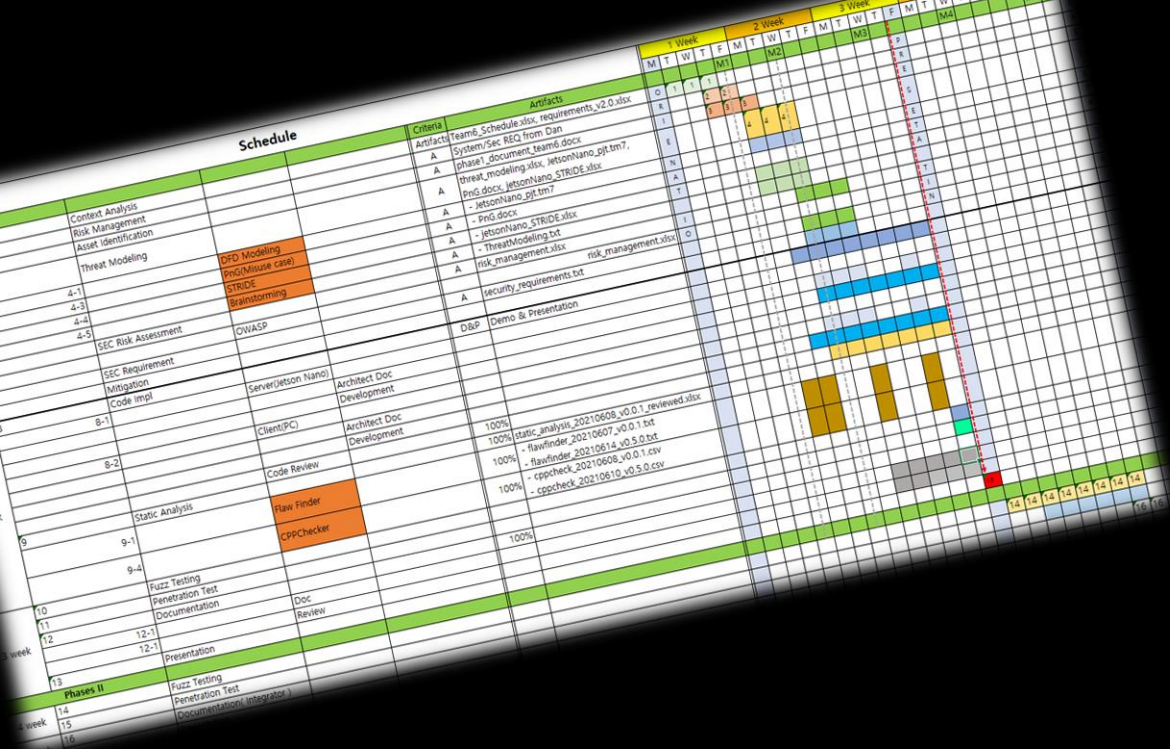
Derive mitigations

Construct architecture

Implement the mitigations

Verify the mitigations





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

- REQ-D-01** Establishing secure and authenticated communication with the camera and image analysis application and user interface when secure mode is selected or requested.
- REQ-D-02** Provides the user interface to control the system. User interface shall support the following modes of operation:
 - REQ-D-04** Secure or non secure mode of communication
 - REQ-D-05** 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-06** Run Mode - System utilizes camera to identify faces and perform facial recognition.
- REQ-D-07** Communicating with the camera and image analysis application as specified. Display image frames and any accompanying amplifying analysis information received from the camera and image analysis application in the format specified.

Project Responsibilities

- REQ-Q-01** Implementing the specified enhancements to the applications
- REQ-Q-02** Ensuring that all software in both applications are architected and coded to be secure and free of vulnerabilities.
- REQ-Q-03** 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-Q-04** Proper fault/error detection, recovery, and reporting.
- REQ-Q-05** Analyzing the provided initial implementation for vulnerabilities and developing solutions to mitigate.
- REQ-D-09** Analyze another team's implementation assigned to you for security flaws and vulnerabilities.

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

Schedule		Criteria	Artifacts	1 Week	2 Week	3 Week
Task	Phase	Criteria	Artifacts	M	T	W
Context Analysis			Team's Schedule.xlsx, requirements_v2.0.xlsx			
Risk Management			System/Sec REQ from Dan			
Asset Identification			phases, document, teams, docs			
Threat Modeling			threat_modeling.xlsx, jetsonNano_gpt.m7,			
			threat_modeling.xlsx, jetsonNano_STRIDE.xlsx			
			req.docx, jetsonNano_STRIDE.xlsx			
			jetsonNano_gpt.m7			
			- PnD docx			
			- jetsonNano_STRIDE.xlsx			
			- ThreatModeling.txt			
			risk_management.xlsx			
			security_requirements.txt			
			D&P Demo & Presentation			
4-1						
4-3						
4-4						
4-5						
SEC Risk Assessment						
SEC Requirement						
Mitigation						
Code Impl						
8-1						
8-2						
Static Analysis						
9-1						
9-4						
10						
11						
12						
12-1						
12-1						
13						
14						
15						
16						

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 user credentials must be protected. Lost or compromised credentials must be handled in a reasonable way.
- REQ-D-15 • Authentication: The system must use two factor authentication for sign on and user credentials must be protected. Lost or compromised credentials must be handled in a reasonable way.
- REQ-D-16 • Authentication: The system must use two factor authentication for sign on and user credentials must be protected. Lost or compromised credentials must be handled in a reasonable way.
- 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 should recover from networking errors as soon as possible. The goal is to maintain a secure, performant connection at all costs.
- REQ-D-21 • reliability: The system must ensure that video is reliably delivered. The system 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 quality standards.
- REQ-Q-10 3. Ensure the developed software adheres to the company coding standard and quality standards.
- REQ-Q-11 4. Ensure the developed software is adequately tested.

* reference : LG Security Class Project Description.pdf

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

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

- Establishing secure and authenticated communication with the camera and image analysis application and user interface when secure mode is selected or requested.

Provides the user interface to control the system. User interface shall support the following modes of operation:

- Secure or non secure mode of communication.
- 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.
- Run Mode - System utilizes camera to identify faces and perform facial recognition.

Communicating with the camera and image analysis application as specified. Image frames and any accompanying amplifying analysis information received from the camera and image analysis application in the format specified.

Responsibilities

Ensuring the specified enhancements to the applications that all software in both applications are architected and coded to be secure and free of vulnerabilities.

Ensuring the implementation so the applications support two communications: 1) a secure mode with all data encrypted (including authentication) and 2) a plain text without encryption.

Ensuring proper fault/error detection, recovery, and reporting.

Ensuring the provided initial implementation for vulnerabilities and other team's implementation assigned to you for vulnerabilities.

REQ-D-09

Phase 2

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

Schedule		Artifacts		1 Week		2 Week		3 Week		4 Week	
				M	T	W	T	F	S	M	T
Context Analysis											
Risk Management											
Asset Identification											
Threat Modeling											
4-1											
4-3											
4-4											
4-5											
SEC Risk Assessment											
SEC Requirement											
Mitigation											
Code Impl											
8-1											
8-2											
Static Analysis											
9-1											
9-4											
Fuzz Testing											
Penetration Test											
Documentation											
12-1											
12-1											
12-1											
13											
14											
15											
16											

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 user credentials must be protected
- REQ-D-15** • 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 should recover from networking errors as soon as possible. The goal is to maintain a secure, performant connection at all costs.
- REQ-D-21**

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 quality standards.
- REQ-Q-10**
- REQ-Q-11** 4. Ensure the developed software is adequately tested.

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

User display and system control application is responsible for the following:

- Establishing secure and authenticated communication with the camera and image analysis application and user interface when secure mode is selected or requested.
- Provides the user interface to control the system. User interface shall support the following modes of operation:
 - Secure or non secure mode of communication
 - 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
 - Run Mode - System utilizes camera to identify faces and perform facial recognition.
 - Test Run Mode - System utilizes a video file to identify faces and perform facial recognition.
- Communicating with the camera and image analysis application as specified.
- Image frames and any accompanying amplifying analysis information received from the camera and image analysis application in the format specified.

Responsibilities

- Implementing the specified enhancements to the applications
- Ensuring that all software in both applications are architected and coded to be secure and free of vulnerabilities.
- Implementing the implementation so the applications support two communications: 1) a secure mode with all data encrypted (including authentication) and 2) a plain text
- Implementing fault/error detection, recovery, and reporting.
- Implementing the provided initial implementation for vulnerabilities and solutions to mitigate.
- Implementing other team's implementation assigned to you for vulnerabilities and vulnerabilities.

Requirements from CMU documents on left

DEVELOPMENT	
Reference	Description
D-01	REQ-D-02 REQ-D-03
D-02	Establishing connection between Client and Server
D-03	Support Secure Mode
D-04	Support Non Secure Mode
D-05	Support Learning Mode - Register new person to the Server
D-06	Support Run Mode - System identifies faces and performs facial recognition
D-07	Support Test Run Mode
D-08	Display Result - Face-recognized images
D-09	REQ-D-02
D-10	REQ-D-02
D-11	REQ-D-03
D-12	REQ-D-03
D-13	REQ-D-03
D-14	REQ-D-03
D-15	REQ-D-03
D-16	REQ-D-03
D-17	REQ-D-03
D-18	REQ-D-03
D-19	REQ-D-03
D-20	REQ-D-03
D-21	REQ-D-03
D-22	REQ-D-03
D-23	REQ-D-03
D-24	REQ-D-03
D-25	REQ-D-03
D-26	REQ-D-03
D-27	REQ-D-03
D-28	REQ-D-03
D-29	REQ-D-03
D-30	REQ-D-03
D-31	REQ-D-03
D-32	REQ-D-03
D-33	REQ-D-03
D-34	REQ-D-03
D-35	REQ-D-03
D-36	REQ-D-03
D-37	REQ-D-03
D-38	REQ-D-03
D-39	REQ-D-03
D-40	REQ-D-03
D-41	REQ-D-03
D-42	REQ-D-03
D-43	REQ-D-03
D-44	REQ-D-03
D-45	REQ-D-03
D-46	REQ-D-03
D-47	REQ-D-03
D-48	REQ-D-03
D-49	REQ-D-03
D-50	REQ-D-03
D-51	REQ-D-03
D-52	REQ-D-03
D-53	REQ-D-03
D-54	REQ-D-03
D-55	REQ-D-03
D-56	REQ-D-03
D-57	REQ-D-03
D-58	REQ-D-03
D-59	REQ-D-03
D-60	REQ-D-03
D-61	REQ-D-03
D-62	REQ-D-03
D-63	REQ-D-03
D-64	REQ-D-03
D-65	REQ-D-03
D-66	REQ-D-03
D-67	REQ-D-03
D-68	REQ-D-03
D-69	REQ-D-03
D-70	REQ-D-03
D-71	REQ-D-03
D-72	REQ-D-03
D-73	REQ-D-03
D-74	REQ-D-03
D-75	REQ-D-03
D-76	REQ-D-03
D-77	REQ-D-03
D-78	REQ-D-03
D-79	REQ-D-03
D-80	REQ-D-03
D-81	REQ-D-03
D-82	REQ-D-03
D-83	REQ-D-03
D-84	REQ-D-03
D-85	REQ-D-03
D-86	REQ-D-03
D-87	REQ-D-03
D-88	REQ-D-03
D-89	REQ-D-03
D-90	REQ-D-03
D-91	REQ-D-03
D-92	REQ-D-03
D-93	REQ-D-03
D-94	REQ-D-03
D-95	REQ-D-03
D-96	REQ-D-03
D-97	REQ-D-03
D-98	REQ-D-03
D-99	REQ-D-03
D-100	REQ-D-03


Re-define Requirement from "REQ-"
Merged the duplicated "REQ-" to "CMU-REQ-"


DEVELOPMENT	
ID	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, end a feed in Support Secure Mode
CMU-REQ-D-03	A user should be able to initiate a video feed, end 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	Nonrepudiation, 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


LG Security Class Project Description.pdf

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

Phase 2

PnG 1		Type	Internal Engineer
		Goal	Ruin the administrator's reputation
		Motivation	Revenge to the administrator
		Skill	manipulate the user credential data, find out the administrator's password from the previous one that is used 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 hacking program.
		Misuse case	(TR-59) Sniff the communication channel between server and client to get user credential data.

Requirements of Tartan Secure Camera Application

proposed system has the following basic functional requirements. Note

- 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.

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

- Performance: The system must deliver video as close to real time as possible, especially in real-time mode.
 - Authentication: The system must use two factor authentication for sign on and user credentials must be protected. Lost or compromised credentials must be handled in a reasonable way. **REQ-D-16**
 - 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.
 - Proof of identity (nonrepudiation): Users should be confident that the camera they are using is the one that they believe it is.
 - Multi-user privacy: The system must ensure that multiple video feeds remain private between the intended users.
 - Reliability: The system must ensure that video is reliably delivered. The system 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 quality standards.
- REQ-Q-10**
- REQ-Q-11** 4. Ensure the developed software is adequately tested.

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

User display and system control application is responsible for the following:

- Establishing secure and authenticated communication with the camera and image analysis application and user interface when secure mode is selected or requested.
- Provides the user interface to control the system. User interface shall support the following modes of operation:
 - Secure or non secure mode of communication. **REQ-B-03**
 - 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.
 - Run Mode - System identifies faces and performs facial recognition.
 - Test Run Mode - System utilizes a video file to identify faces and perform facial recognition.
- Communicating with the camera and image analysis application as specified.
- Image frames and any accompanying amplifying analysis information received from the camera and image analysis application in the format specified.

Responsibilities

Implementing the specified enhancements to the applications

that all software in both applications are architected and coded to be secure and free of vulnerabilities.

the implementation so the applications support two communications: 1) a secure mode with all data encrypted (including authentication) and 2) a plain text

fault/error detection, recovery, and reporting

the provided initial implementation

ing solutions to mitigate

ther team's

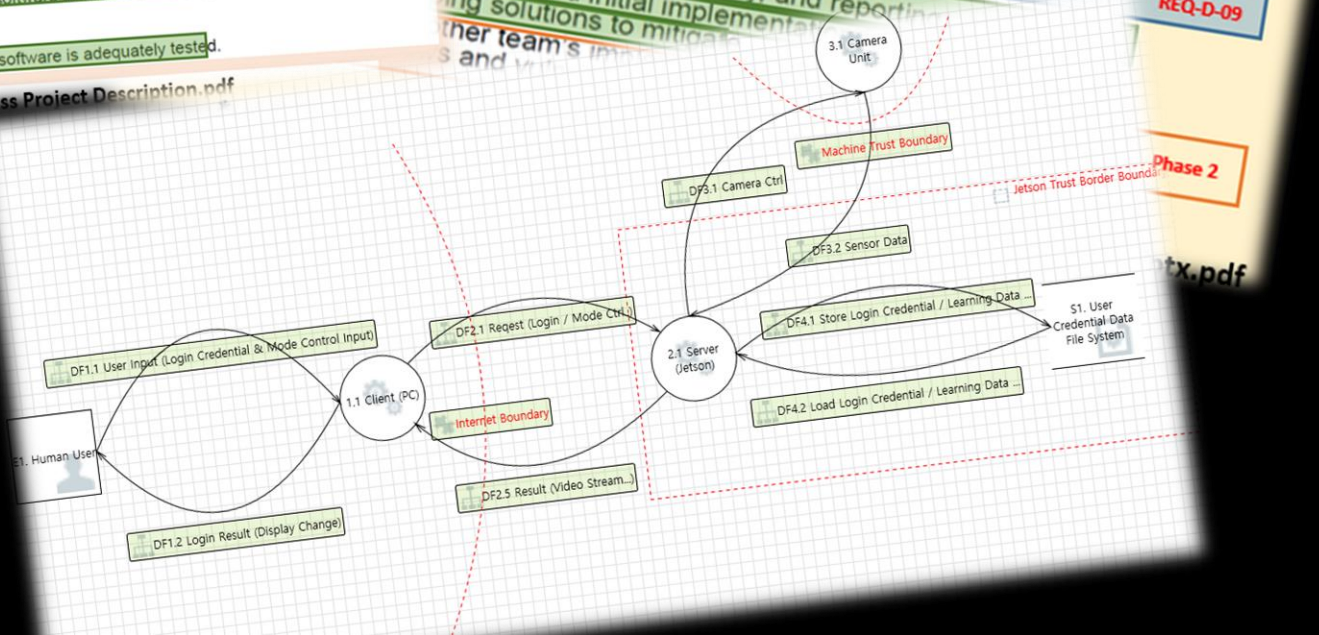
Requirements from CMU documents on left

Reference	Description
REQ-D-02	Establishing connection between Client and Server
REQ-D-03	Support Secure Mode
REQ-D-04	Support Non Secure Mode
REQ-D-05	Support Learning Mode - Register new person to the Server
REQ-D-06	Support Run Mode - System identifies faces and performs facial recognition
REQ-D-07	Support Test Run Mode
REQ-D-08	Display Result - Face-recognized images
REQ-D-09	Display Result - Face-recognized images
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
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	data sent to a user remains private while in transit. No intermediary to be snoop or spy
REQ-D-18	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: multiple video feeds remain private between the users
REQ-D-20	Reliability: the video is reliably delivered

ID	Description	Mandatory
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, end a feed in Support Secure Mode	Mandatory
CMU-REQ-D-03	A user should be able to initiate a video feed, end 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

Finalize REQs with DAN

To Do (excluding req of Tartan Architecture Doc)



PnG 1	Type	Internal Engineer
	Goal	Ruin the administrator's reputation
	Motivation	Revenge to the administrator
	Skill	manipulate the user credential data, find out the administrator's password from the previous one that is used 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 hacking program.
	Misuse case	(TR-59) Sniff the communication channel between server and client to get user credential data.

Requirements of Tartan Secure Camera Application

proposed system has the following basic functional requirements. Note

- 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

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

- Performance: The system must deliver video as close to real time as possible, especially in real-time mode.
- Authentication: The system must use two factor authentication for sign on and user credentials must be protected. Lost or compromised credentials must be handled in a reasonable way. **REQ-D-16**
- 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.
- Proof of identity (nonrepudiation): Users should be confident that the camera they are using is the one that they believe it is.
- Multi-user privacy: The system must ensure that multiple video feeds remain private between the intended users.
- reliability: The system must ensure that video is reliably delivered. The system should recover from networking errors. The goal is to maintain a secure, performant connection.

Aside from these requirements, there are 28 threats below by using STRIDE, PnG, Brainstorming.

- Ensuring that all software in both secure and free of vulnerabilities. **REQ-Q-07**
- Conduct proper fault/error detection. **REQ-Q-08**
- Ensure the developed software quality standards. **REQ-Q-09**
- Ensure the developed software. **REQ-Q-10**
- Ensure the developed software. **REQ-Q-11**

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

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

Establishing secure and authenticated communication with the camera and image analysis application and user interface when secure mode is selected or requested.

Provides the user interface to control the system. User interface shall support the following modes of operation:

Secure or non secure mode of communication

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-B-03**

Run Mode - System utilizes camera to identify faces and perform facial recognition.

Test Run Mode - System utilizes a video file to identify faces and perform facial recognition.

Communicating with the camera and image analysis application as specified.

image frames and any accompanying amplifying analysis information from the camera and image analysis application in the format specified.

Responsibilities

Implementing the specified enhancements to the applications

that all software in both applications are architected

additional consideration

Requirements from CMU documents on left

Reference	Description
REQ-D-02	Establishing connection between Client and Server
REQ-D-03	Support Secure Mode
REQ-D-04	Support Non Secure Mode
REQ-D-05	Support Learning Mode - Register new person to the Server
REQ-D-06	Support Run Mode - System identifies faces and performs facial recognition
REQ-D-07	Support Test Run Mode
REQ-D-08	Display Result - Face-recognized images
REQ-D-09	Display Result - Face-recognized images
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
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	Nonrepudiation: Users should be confident that the camera they are using is the one that they believe it is
REQ-D-18	Multi-user privacy: multiple video feeds remain private between the users
REQ-D-19	Reliability: the video is reliably delivered

ID	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	Nonrepudiation: 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

Finalize REQs with DAN

To Do (excluding req of Tartan Architecture Doc)

ID	Description	Mandatory
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	Mandatory
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	Excluded

ID	Tool	Category	Interaction	Threat	Review
TR-01	STRIDE	Information Disclosure	DF4.2 Load Login Credential / Learning Data	If the user credential data is stored as plain text, it can be disclosed	User credential should be kept securely
TR-02	STRIDE	Tampering	DF4.2 Load Login Credential / Learning Data	An attacker modify user credential data	User credential should be kept securely
TR-03	STRIDE	Spoofting	DF4.2 Load Login Credential / Learning Data	An attacker modify user credential data and non server can use it without checking	User credential should be kept securely
TR-04	STRIDE	Spoofting	DF2.1 Request (Login / Mode Ctrl.)	An attacker spoof the user (Client)	Need to more stronger authentication process
TR-05	STRIDE	Tampering	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-06	STRIDE	Reputation	DF2.1 Request (Login / Mode Ctrl.)	Client can repudiate the actions they have performed	Need to apply mutual authentication
TR-07	STRIDE	Information Disclosure	DF2.1 Request (Login / Mode Ctrl.)	An attacker can sniff the data on the connection	Need to consider encrypting the data flow
TR-08	STRIDE	Information Disclosure	DF2.1 Request (Login / Mode Ctrl.)	Weak authentication may lead to disclose information	Need to more stronger authentication process
TR-09	STRIDE	Denial Of Service	DF2.1 Request (Login / Mode Ctrl.)	Denial of service of the communication between client and server is interrupted by attackers	Need to use TLS
TR-10	STRIDE	Elevation Of Privilege	DF2.1 Request (Login / Mode Ctrl.)	An attacker sends a malicious data to server in order to change the flow of program execution	Need to apply input sanitization
TR-11	STRIDE	Denial Of Service	DF3.1 Camera Ctrl	It may be physically damaged and you may not be able to get Data from Camera	Need to protect camera unit from physical damage
TR-12	STRIDE	Denial Of Service	DF4.1 Store Login Credential / Learning Data	It is possible to be lost or destroyed	Need to send the data to secure storage

ID	Tool	Category	Interaction	Threat	Review
TR-35	STRIDE	Information Disclosure	DF4.1 Store Login Credential / Learning Data	User credential may be disclosed	Need to encrypt credential data
TR-41	STRIDE	Spoofting	DF4.1 Store Login Credential / Learning Data	User Credential Data can be exposed to attackers	Need to encrypt credential data
TR-44	STRIDE	Spoofting	DF2.5 Result (Video Stream...)	Server (Jelton) may be spoofed by an attacker	Need to apply authentication
TR-45	STRIDE	Spoofting	DF2.5 Result (Video Stream...)	Client (PC) may be spoofed by an attacker	Need to apply authentication
TR-46	STRIDE	Tampering	DF2.5 Result (Video Stream...)	Video Stream may be tampered with by an attacker	Need to protect video stream over connection
TR-48	STRIDE	Information Disclosure	DF2.5 Result (Video Stream...)	Video Stream may be sniffed with by an attacker	Need to protect video stream over connection
TR-49	STRIDE	Denial Of Service	DF2.5 Result (Video Stream...)	Client (PC) crashes, halts, stops or runs slowly	Need to remain stable in abnormal cases
TR-52	STRIDE	Elevation Of Privilege	DF2.5 Result (Video Stream...)	Server (Jelton) may be able to remotely execute code	Need input sanitization
TR-53	STRIDE	Elevation Of Privilege	DF2.5 Result (Video Stream...)	An attacker may pass data into 1 Client (PC)	Need to protect user credential data
TR-56	PnG	Tampering	User credential data	Change the image data not to recognize registered	Need to protect user credential data
TR-57	PnG	Information Disclosure	Client <=> Server	Disclose administrator's ID/Password to the employees in the company	Need to more stronger process for authentication
TR-59	PnG	Information Disclosure	Server <=> Client	Sniff the communication channel between server and client to get user credential data	Need to protect the data over the connection
TR-60	Brainstorming	N/A	Network	Compromise the connection of network physically by an attacker	Server need to be robust in abnormal case
TR-61	Brainstorming	Tampering/ Information Disclosure/ Spoofting	Server <=> Client	The service/certificate or key, an attacker may attempt to connect to an unauthorized client. And attacker can try to hijack the TLS communication	Need to protect or verify the certificates and keys used by the server and client for the TLS communication

PnG 1	Type	Internal Engineer
	Goal	Ruin the administrator's reputation
	Motivation	Revenge to the administrator
	Skill	manipulate the user credential data, find out the administrator's password from the previous one that is used to other system
	Misuse case	(TR-56) Change the image data not to recognize users. (TR-57) Disclose administrator's ID to employees in the company.

PnG 2	Type	Spy
	Goal	Steal all components
	Motivation	Competitors
	Skill	Physical
	Misuse case	(TR-58) ...

PnG 3	Type	...
	Goal	...
	Motivation	...
	Skill	...
	Misuse case	...

ID	Tool	Category	Interaction	Threat	Review
TR-01	STRIDE	Information Disclosure	DF4.2 Load Login Credential / Learning Data	If the user credential data is stored as plain text it can be disclosed	User credential should be kept securely
TR-02	STRIDE	Tampering	DF4.2 Load Login Credential / Learning Data	An attacker modify user credential data	User credential should be kept securely
TR-03	STRIDE	Spoofting	DF4.2 Load Login Credential / Learning Data	An attacker modify user credential data and use it without checking	User credential should be kept securely
TR-04	STRIDE	Spoofting	DF2.1 Request (Login / Mode Ctrl.)	An attacker spoof the user (Client)	Need to more stronger authentication process
TR-05	STRIDE	Tampering	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-06	STRIDE	Reputation	DF2.1 Request (Login / Mode Ctrl.)	Client can reproduce the actions they have performed	Need to apply mutual authentication
TR-07	STRIDE	Information Disclosure	DF2.1 Request (Login / Mode Ctrl.)	An attacker can sniff the data on the connection	Need to consider encrypting the data flow
TR-08	STRIDE	Information Disclosure	DF2.1 Request (Login / Mode Ctrl.)	Weak authentication may lead to disclose information	Need to more stronger authentication process
TR-09	STRIDE	Denial Of Service	DF2.1 Request (Login / Mode Ctrl.)	The authentication of the communication between client and server is interrupted by attackers	Need to use TLS
TR-10	STRIDE	Elevation Of Privilege	DF2.1 Request (Login / Mode Ctrl.)	An attacker sends a malicious data to server in order to change the flow of program execution	Need to apply input sanitization
TR-11	STRIDE	Denial Of Service	DF3.1 Camera Ctrl	It may be physically damaged and you may not be able to get Data from Camera	Need to protect camera unit from physical damage
TR-12	STRIDE	Denial Of Service	DF4.1 Store Login Credential / Learning Data	It is possible to ...	Need to send the ...

Requirements of Tartan Secure Camera Application

proposed system has the following basic functional requirements. Note

- 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

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

Performance: The system must deliver video as close to real time as possible, specially in real-time mode.

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

Information privacy: When in the desired mode the system must ensure that a user remains private while in transit. No intermediary should be able to spy on an ongoing video feed.

(nonrepudiation): Users should be confident that the camera is the one that they believe it is.

The system must ensure that multiple video feeds remain intended users.

The system must ensure that video is reliably delivered. The goal is to avoid working errors.

5. Result of Threat Modeling

lements, there are 28 threats below by using STRIDE, PnG, Brainstorming.

ID	Tool	Category	Interaction	Threat	Review
TR-01	STRIDE	Information Disclosure	DF4.2 Load Login Credential / Learning Data	If the user credential data is stored as plain text it can be disclosed	User credential should be kept securely
TR-02	STRIDE	Tampering	DF4.2 Load Login Credential / Learning Data	An attacker modify user credential data	User credential should be kept securely
TR-03	STRIDE	Spoofting	DF4.2 Load Login Credential / Learning Data	An attacker modify user credential data and use it without checking	User credential should be kept securely
TR-04	STRIDE	Spoofting	DF2.1 Request (Login / Mode Ctrl.)	An attacker spoof the user (Client)	Need to more stronger authentication process
TR-05	STRIDE	Tampering	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-06	STRIDE	Reputation	DF2.1 Request (Login / Mode Ctrl.)	Client can reproduce the actions they have performed	Need to apply mutual authentication
TR-07	STRIDE	Information Disclosure	DF2.1 Request (Login / Mode Ctrl.)	An attacker can sniff the data on the connection	Need to consider encrypting the data flow
TR-08	STRIDE	Information Disclosure	DF2.1 Request (Login / Mode Ctrl.)	Weak authentication may lead to disclose information	Need to more stronger authentication process
TR-09	STRIDE	Denial Of Service	DF2.1 Request (Login / Mode Ctrl.)	The authentication of the communication between client and server is interrupted by attackers	Need to use TLS
TR-10	STRIDE	Elevation Of Privilege	DF2.1 Request (Login / Mode Ctrl.)	An attacker sends a malicious data to server in order to change the flow of program execution	Need to apply input sanitization
TR-11	STRIDE	Denial Of Service	DF3.1 Camera Ctrl	It may be physically damaged and you may not be able to get Data from Camera	Need to protect camera unit from physical damage
TR-12	STRIDE	Denial Of Service	DF4.1 Store Login Credential / Learning Data	It is possible to ...	Need to send the ...

ID	Tool	Category	Interaction	Threat	Review
TR-13	STRIDE	Elevation Of Privilege	DF2.1 Request (Login / Mode Ctrl.)	An attacker sends a malicious data to server in order to change the flow of program execution	Need to apply input sanitization
TR-14	STRIDE	Denial Of Service	DF3.1 Camera Ctrl	It may be physically damaged and you may not be able to get Data from Camera	Need to protect camera unit from physical damage
TR-15	STRIDE	Denial Of Service	DF4.1 Store Login Credential / Learning Data	It is possible to ...	Need to send the ...

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

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

Establishing secure and authenticated communication with the camera and image analysis application and user interface when secure mode is selected or requested.

Provides the user interface to control the system. User interface shall support the following modes of operation:

Secure or non secure mode of communication

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-B-03**

Run Mode - System utilizes camera to identify faces and perform facial recognition.

Communicating with the camera and image analysis application as specified.

image frames and any accompanying amplifying analysis information received from the camera and image analysis application in the format specified.

Responsibilities

Implementing the specified enhancements to the applications

that all software in both applications are architected

additional consideration

ID	Tool	Category	Interaction	Threat	Review
TR-16	STRIDE	Information Disclosure	DF4.1 Store Login Credential / Learning Data	User credential may be disclosed	Need to encrypt credential data
TR-17	STRIDE	Spoofting	DF4.1 Store Login Credential / Learning Data	User Credential Data can be exposed to attackers	Need to apply authentication
TR-18	STRIDE	Spoofting	DF2.5 Result (Video Stream...)	Server (Jelton) may be spoofed by an attacker	Need to apply authentication
TR-19	STRIDE	Spoofting	DF2.5 Result (Video Stream...)	Client (PC) may be spoofed by an attacker	Need to apply authentication
TR-20	STRIDE	Tampering	DF2.5 Result (Video Stream...)	Video Stream may be tampered with by an attacker	Need to protect video stream over connection
TR-21	STRIDE	Information Disclosure	DF2.5 Result (Video Stream...)	Video Stream may be sniffed with by an attacker	Need to protect video stream over connection
TR-22	STRIDE	Denial Of Service	DF2.5 Result (Video Stream...)	Client (PC) crashes, halts, sleep or runs slowly	Need to remain stable in abnormal cases
TR-23	STRIDE	Elevation Of Privilege	DF2.5 Result (Video Stream...)	Server (Jelton) may be able to remotely execute code	Need input sanitization
TR-24	STRIDE	Elevation Of Privilege	DF2.5 Result (Video Stream...)	An attacker may pass data into 1 Client (PC)	Need input sanitization
TR-25	PnG	Tampering	User credential data	Change the image data not to recognize registered	Need to protect user credential data
TR-26	PnG	Information Disclosure	Client <=> Server	Disclose administrator's ID/password to the employees in the company	Need to more stronger process for authentication
TR-27	PnG	Information Disclosure	Server <=> Client	Sniff the communication channel between server and client to get user credential data	Need to protect the data over the connection
TR-28	Brainstorming	N/A	Network	Compromise the connection of network physically by an attacker	Server need to be robust in abnormal case
TR-29	Brainstorming	Tampering/Information Disclosure/Spoofting	Server <=> Client	The service/certificate or key, an attacker may attempt to connect to an unauthorized client. And attacker can try to ...	Need to protect or verify the certificates and keys used by the server and client for the TLS communication

PnG 1	Type	Internal Engineer
	Goal	Ruin the administrator's reputation
	Motivation	Revenge to the administrator
	Skill	manipulate the user credential data, find out the administrator's password from the previous one that is used to other system
	Misuse case	(TR-56) Change the image data not to recognize users. (TR-57) Disclose administrator's ID to employees in the company.

PnG 2	Type	Spy
	Goal	Steal all components
	Motivation	Competitors
	Skill	Physical
	Misuse case	(TR-58) Steal all components

PnG 3	Type	Physical
	Goal	Steal all components
	Motivation	Competitors
	Skill	Physical
	Misuse case	(TR-59) Steal all components

Requirements of Tartan Secure Camera Application

proposed system has the following basic functional requirements. Note

- 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

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

Performance: The system must deliver video as close to real time as possible, specially in real-time mode.

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

Privacy: When in the desired mode the system must ensure that a user remains private while in transit. No intermediary should be able to spy on an ongoing video feed.

(nonrepudiation): Users should be confident that the camera is the one that they believe it is.

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.	CMU-REQ-D-15	MI-01
SR-03	Errors, exceptions, and abnormal conditions that may occur in the software must be handled robustly.		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

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

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

Establishing secure and authenticated communication with the camera and image analysis application and user interface when secure mode is selected or requested.

Provides the user interface to control the system. User interface shall support the following modes of operation:

- Secure or non secure mode of communication
- 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-B-03
- Run Mode - System utilizes camera to identify faces and perform facial recognition.
- Test Run Mode - System utilizes a video file to identify faces and perform facial recognition.

Communicating with the camera and image analysis application as specified.


Image frames and any accompanying analysis information in the format specified.

the applications are architected

additional consideration

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.	CMU-REQ-D-15	MI-01
SR-03	Errors, exceptions, and abnormal conditions that may occur in the software must be handled robustly.		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

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.	CMU-REQ-D-15	MI-01
SR-03	Errors, exceptions, and abnormal conditions that may occur in the software must be handled robustly.		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

PnG 1	Type	Internal Engineer
	Goal	Ruin the administrator's reputation
	Motivation	Revenge to the administrator
	Skill	manipulate the user credential data, find out the administrator's password from the previous one that is used to other system
	Misuse case	(TR-56) Change the image data not to recognize users. (TR-57) Disclose administrator's ID to employees in the company.

PnG 2	Type	Spy
	Goal	Steal all components
	Motivation	Competitors
	Skill	Physical
	Misuse case	(TR-58) ...

PnG 3	Type	Spy
	Goal	Steal all components
	Motivation	Competitors
	Skill	Physical
	Misuse case	(TR-58) ...

REQ-NO	REQ-DESCRIPTION	REQ-STATUS	REQ-DATE	REQ-OWNER	REQ-ASSIGNED	REQ-START	REQ-END	REQ-PROGRESS	REQ-COMMENTS
REQ-D-01	Establishing connection between Client and Server	Completed	2023-01-01	John Doe	John Doe	2023-01-01	2023-01-01	100%	
REQ-D-02	A user should be able to initiate a video feed, and a feed in Support Secure Mode	In Progress	2023-01-02	John Doe	John Doe	2023-01-02	2023-01-05	50%	
REQ-D-03	A user should be able to end a video feed	In Progress	2023-01-03	John Doe	John Doe	2023-01-03	2023-01-05	50%	
REQ-D-04	A user should be able to save a video feed for offline review	In Progress	2023-01-04	John Doe	John Doe	2023-01-04	2023-01-05	50%	
REQ-D-05	A user should be able to tune image analysis	In Progress	2023-01-05	John Doe	John Doe	2023-01-05	2023-01-05	50%	
REQ-D-06	The system must use 2FA	In Progress	2023-01-06	John Doe	John Doe	2023-01-06	2023-01-05	50%	
REQ-D-07	User credentials must be protected	In Progress	2023-01-07	John Doe	John Doe	2023-01-07	2023-01-05	50%	
REQ-D-08	Lost or compromised credentials must be handled in a reasonable way	In Progress	2023-01-08	John Doe	John Doe	2023-01-08	2023-01-05	50%	
REQ-D-09	Nonrepudiation: Users should be confident that the camera they are using is the one that they believe it is	In Progress	2023-01-09	John Doe	John Doe	2023-01-09	2023-01-05	50%	
REQ-D-10	Multi-user Privacy: multiple video feeds remain private between the users	In Progress	2023-01-10	John Doe	John Doe	2023-01-10	2023-01-05	50%	
REQ-D-11	Reliability: the video feeds remain	In Progress	2023-01-11	John Doe	John Doe	2023-01-11	2023-01-05	50%	
REQ-D-12	Nonrepudiation: Users should be confident that the camera they are using is the one that they believe it is	In Progress	2023-01-12	John Doe	John Doe	2023-01-12	2023-01-05	50%	

Requirements of Tartan Secure Camera Application

proposed system has the following basic functional requirements. Note

- A user should be able to initiate a video feed, and 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

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

Performance: The system must deliver video as close to real time as possible, specially in real-time mode.

Authentication: The system must use two factor authentication for sign on and credentials must be protected. Lost or compromised credentials must be handled in a reasonable way.

Privacy: When in the desired mode the system must ensure a user remains private while in transit. No intermediary should be able to spy on an ongoing video feed.

Nonrepudiation: Users should be confident that the camera they are using is the one that they believe it is.

9.6. Compile Options

Defenses at the compiler, check the mitigation technologies in the system.

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

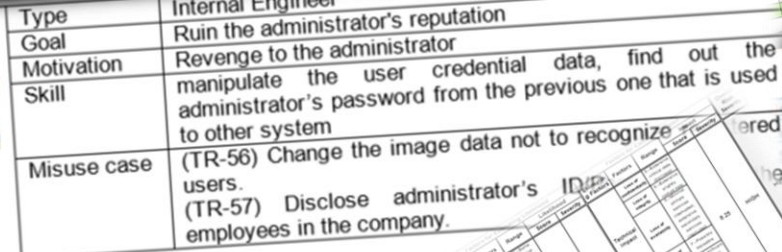
7. Security Requirements

We've derived the security requirements through the following process. Some of security requirements are linked to system requirements.

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 occur in the software 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 communicated.
SR-06	Protect Camera from physical damage
SR-07	Restrictions related to files are necessary to avoid system problems.
SR-08	Save contents of the communication as a log and use as proof of non-repudiation.
SR-09	Server and client must communicate using an encrypted channel.
SR-10	The system must perform an integrity check before using user credentials.
SR-11	The system shall know the change of the user credential data.
SR-12	Use well-known cryptographic libraries and robust algorithms.
SR-13	User Credential Data should be encrypted in the storage.
SR-14	Video Stream over the connection should be protected.
SR-15	A server and client program must perform an integrity check before using a certificate or key.
SR-16	Face recognition data should be encrypted in the storage.
SR-17	Every encryption time, newly generated random key is used for encryption to make reverse analysis difficult
SR-18	ROOT encrypt key must be protected from binary analysis

CMU-REQ-D-02	A user should be able to initiate a video feed, and a feed in Support Secure Mode	In Progress
CMU-REQ-D-03	A user should be able to end a video feed	In Progress
CMU-REQ-D-04	A user should be able to save a video feed for offline review	In Progress
CMU-REQ-D-05	A user should be able to tune image analysis	In Progress
CMU-REQ-D-06	The system must use 2FA	In Progress
CMU-REQ-D-07	User credentials must be protected	In Progress
CMU-REQ-D-08	Lost or compromised credentials must be handled in a reasonable way	In Progress
CMU-REQ-D-09	Nonrepudiation: Users should be confident that the camera they are using is the one that they believe it is	In Progress
CMU-REQ-D-10	Multi-user Privacy: multiple video feeds remain private between the users	In Progress
CMU-REQ-D-11	Reliability: the video feeds remain	In Progress
CMU-REQ-D-12	Nonrepudiation: Users should be confident that the camera they are using is the one that they believe it is	In Progress

REQ-NO	REQ-DESCRIPTION	REQ-STATUS	REQ-DATE	REQ-OWNER	REQ-ASSIGNED	REQ-START	REQ-END	REQ-PROGRESS	REQ-COMMENTS
REQ-D-01	Establishing connection between Client and Server	Completed	2023-01-01	John Doe	John Doe	2023-01-01	2023-01-01	100%	
REQ-D-02	A user should be able to initiate a video feed, and a feed in Support Secure Mode	In Progress	2023-01-02	John Doe	John Doe	2023-01-02	2023-01-05	50%	
REQ-D-03	A user should be able to end a video feed	In Progress	2023-01-03	John Doe	John Doe	2023-01-03	2023-01-05	50%	
REQ-D-04	A user should be able to save a video feed for offline review	In Progress	2023-01-04	John Doe	John Doe	2023-01-04	2023-01-05	50%	
REQ-D-05	A user should be able to tune image analysis	In Progress	2023-01-05	John Doe	John Doe	2023-01-05	2023-01-05	50%	
REQ-D-06	The system must use 2FA	In Progress	2023-01-06	John Doe	John Doe	2023-01-06	2023-01-05	50%	
REQ-D-07	User credentials must be protected	In Progress	2023-01-07	John Doe	John Doe	2023-01-07	2023-01-05	50%	
REQ-D-08	Lost or compromised credentials must be handled in a reasonable way	In Progress	2023-01-08	John Doe	John Doe	2023-01-08	2023-01-05	50%	
REQ-D-09	Nonrepudiation: Users should be confident that the camera they are using is the one that they believe it is	In Progress	2023-01-09	John Doe	John Doe	2023-01-09	2023-01-05	50%	
REQ-D-10	Multi-user Privacy: multiple video feeds remain private between the users	In Progress	2023-01-10	John Doe	John Doe	2023-01-10	2023-01-05	50%	
REQ-D-11	Reliability: the video feeds remain	In Progress	2023-01-11	John Doe	John Doe	2023-01-11	2023-01-05	50%	
REQ-D-12	Nonrepudiation: Users should be confident that the camera they are using is the one that they believe it is	In Progress	2023-01-12	John Doe	John Doe	2023-01-12	2023-01-05	50%	



Requirements of Tartan Secure Camera Application

proposed system has the following basic functional requirements. Note

- A user should be able to initiate a video feed and 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.

system also has the following architectural concerns (i.e. quality attribute

7. Security Requirements

We've derived the security requirements through out some of security requirements are linked to sys

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 occur in the software 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 communicated.

10. Static Analysis

Tools	Support C/C++	Free software	Latest release	Comment
Flawfinder	O	O	O (2021.06.01)	
RATS	O	O	O (2021.06.01)	

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

* Note: Although our mentor (Professor Jeff) suggested to use the SonarQube, it's utilized with the Github system we're using. We can't use it because it's not supported by the Github system.

CMU-REQ-D-10 User credentials must be handled in a responsible manner.

CMU-REQ-D-11 Lost or compromised credentials must be handled in a responsible manner.

CMU-REQ-D-12 Nonoperational systems must be handled in a responsible manner.

9.6. Compile Options

9.6. Compile Options

Defenses at the compiler, check the mitigation technologies in each system.

```
$ gcc -fstack-protector-strong -fcf-protection=full -D_FORTIFY_SOURCE=3
```

For some mitigation techniques to make it harder to exploit, such as RELRO, NoExecute, and Position Independent Executable (PIE) and Position Independent Code (PIC).

1. checksec.sh (<https://www.trapkit.de/tools/checksec/>)
 - A. Modern Linux distributions offer some mitigation techniques to make it harder to exploit software vulnerabilities reliably. Mitigations such as RELRO, NoExecute (NX), Stack Canaries, Address Space Layout Randomization (ASLR) and Position Independent Executables (PIE) have made reliably exploiting any vulnerabilities that do exist far more challenging. The checksec.sh script is designed to 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

C. Result of running checksec.sh (after apply options for defenses)

- i. Add Symbol stripped option
- ii. Apply option for "No RUNPATH"

ii. Apply option 1		Mitigation ID		Disclosure		Consideration	
CMU-REQ-D-15		MI-10			DF4.1 Store Login Credential / Learning Data	Images in the storage	
		MI-01				User credential may be disclosed	Need to protect credential
		MI-04			DF4.1 Store Login Credential / Learning Data	User Credential Data can be exposed to attackers	Need to protect credential
		MI-05			DF2.5 Result (Video Stream...)	Server (Jelton) may be spoofed by an attacker	Need to apply authentication
		MI-11			DF2.5 Result (Video Stream...)	Client (PC) may be spoofed by an attacker	Need to apply authentication
		MI-08			DF2.5 Result (Video Stream...)	Video Stream may be tampered with by an attacker	Need to protect video stream connection
		MI-12			DF2.5 Result (Video Stream...)	Video Stream may be sniffed with by an attacker	Need to protect video stream connection
		MI-09			DF2.5 Result (Video Stream...)	Client (PC) crashes, halts, stops or runs slowly	Need to remain in abnormal case
CMU-REQ-D-02		MI-02			DF2.5 Result (Video Stream...)	Server (Jelton) may be able to remotely execute code	Need input sanitization
		MI-07			DF2.5 Result (Video Stream...)	An attacker may pass data into 1.1 Client (PC)	Need input sanitization
		MI-07			User credential data	Change the image data not to recognize registered users	Need to protect user credential data
		MI-03, MI-07			Client <=> Server	Disclose administrator's ID/Password to the employees in the company	Need to more strongly process for authentication
CMU-REQ-D-10		MI-03			Server <=> Client	Sniff the communication channel between server and client to get user credential data	Need to protect the data over the connection
		MI-02			Network	Compromise the connection of network physically by an attacker	Server need to be robust in abnormal case
		MI-13				By changing the server's certificate or key, an attacker may attempt to connect to an unauthorized client	Need to protect or verify the certificates and keys used by the server and client
		MI-06			Server <=> Client	And attacker	
		MI-14					
		MI-15					

PnG 1	Type	Internal Engineer
	Goal	Ruin the administrator's reputation
	Motivation	Revenge to the administrator
	Skill	manipulate the user credential data, find out the administrator's password from the previous one that is used to other system
	Misuse case	(TR-56) Change the image data not to recognize users. (TR-57) Disclose administrator's ID/employees in the company.

PnG 2	Type	Spy
	Goal	Steal all components
	Motivation	Competitors
	Skill	Physical
	Misuse case	(TR-56) Change the image data not to recognize users. (TR-57) Disclose administrator's ID/employees in the company.

PnG 3	Type	Spy
	Goal	Steal all components
	Motivation	Competitors
	Skill	Physical
	Misuse case	(TR-56) Change the image data not to recognize users. (TR-57) Disclose administrator's ID/employees in the company.

Requirements of Tartan Security Camera Application

proposed system has the following basic functional requirements. Note

- 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

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

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

Authentication: The system must use two factor authentication for sign on and credentials must be protected. Lost or compromised credentials must be handled in a reasonable way.

Privacy: When in the desired mode the system must ensure that a user remains private while in transit. No intermediary should be able to spy on an ongoing video feed.

(nonrepudiation): Users should be confident that the camera feeds remain the one that they believe it is.

6.6. Compile Options

Defenses at the compiler, check the mitigation technologies in the system.

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

7. Security Requirements

We've derived the security requirements through out some of security requirements are linked to sys

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 occur in the software must be handled robustly.
SR-04	Input validation check is required in Client side.

Only the verified server and client should be connected and communicated.

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 occur in the software must be handled robustly.
SR-04	Input validation check is required in Client side.

10. Static Analysis

In this static analysis, it is very helpful for us to check the initial vulnerabilities of our code. We're actually thinking of how to check vulnerabilities of the code and we wanted to detect 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)	Java code
PMD	X (Java, JS, ...)	O	O (2021-05-29)	Detecting BOF, exception handling, memory leak, unused variables and functions, uninitialized variable
Klocwork	O	X	O (2021-03-23)	Need build environment
Cppcheck	O	O	O (2021-03-23)	Detecting BOF, exception handling, memory leak, unused variables and functions, uninitialized variable
Coverity	O	O	O (2021-03-23)	Need build environment

* Note: Although our mentor(Professor Jeff)'s suggested to use the SonarQube, it's not possible to use it in this system. We're using the Flawfinder.

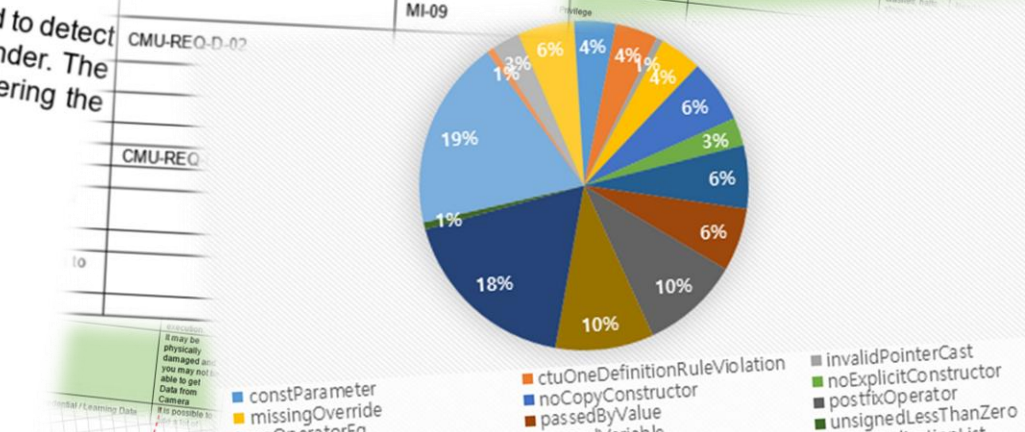
6.6. Compile Options

Defenses at the compiler, check the mitigation technologies in the system.

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

C. Result of running checksec.sh (after apply options for defenses)

- Add Symbol stripped option
- Apply option for "No RUNPATH"



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

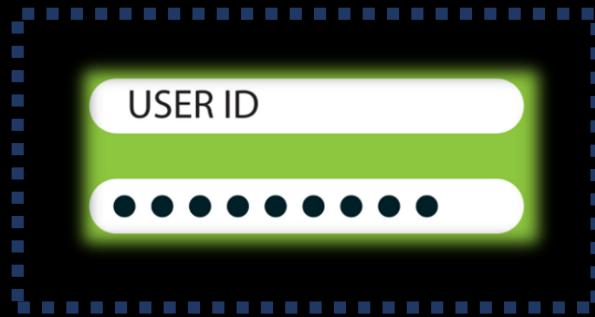


+ name



#authentication #2FA
#face #recognition

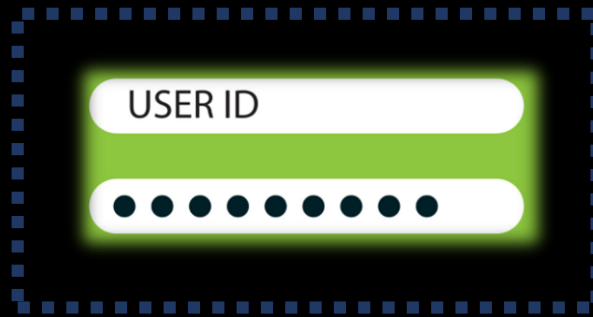
Define assets to protect + Do threat modeling



Define assets to protect + Do threat modeling



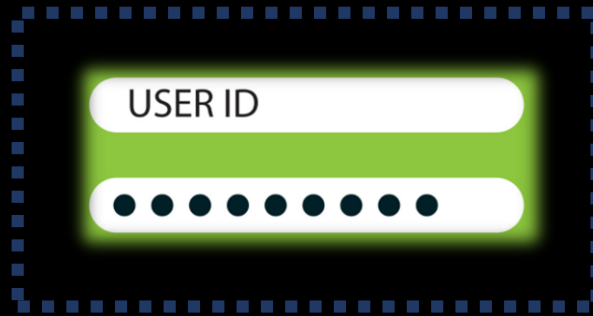
#authentication
#login #password



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



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

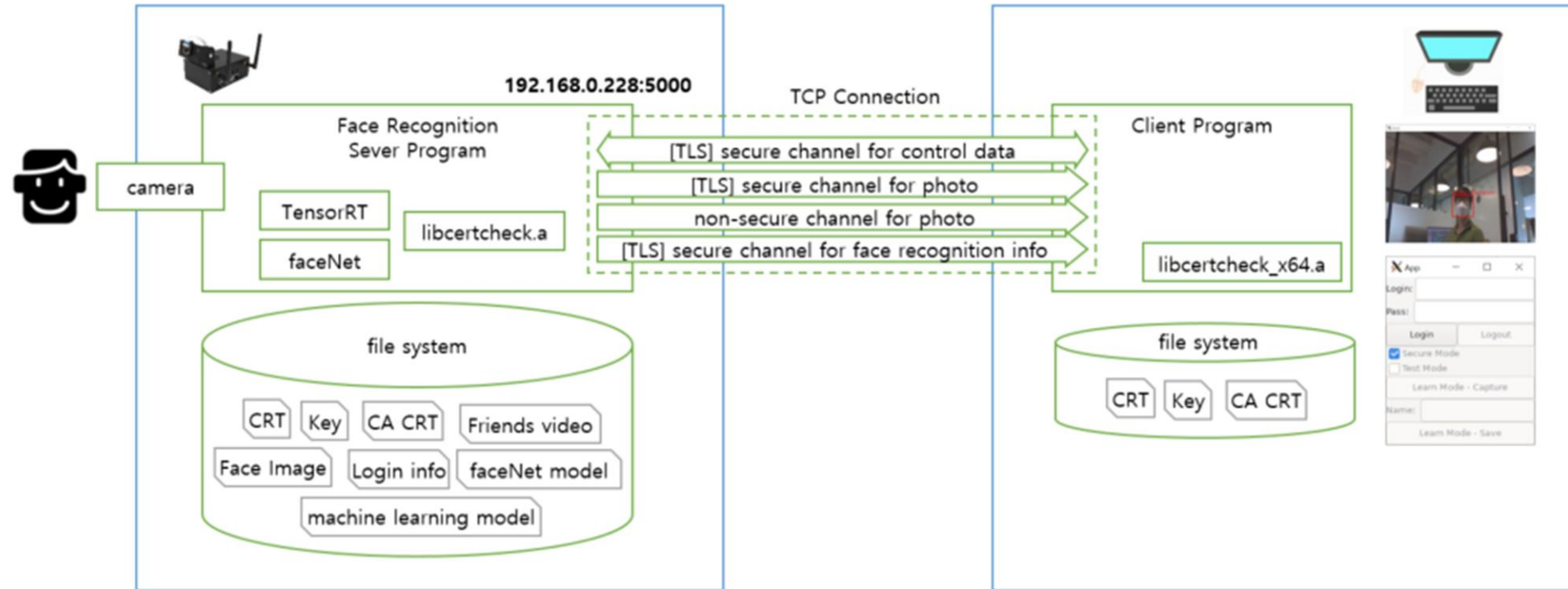
Use verified crypto algorithm (AES256-CBC)

Embed the root key into code obfuscated

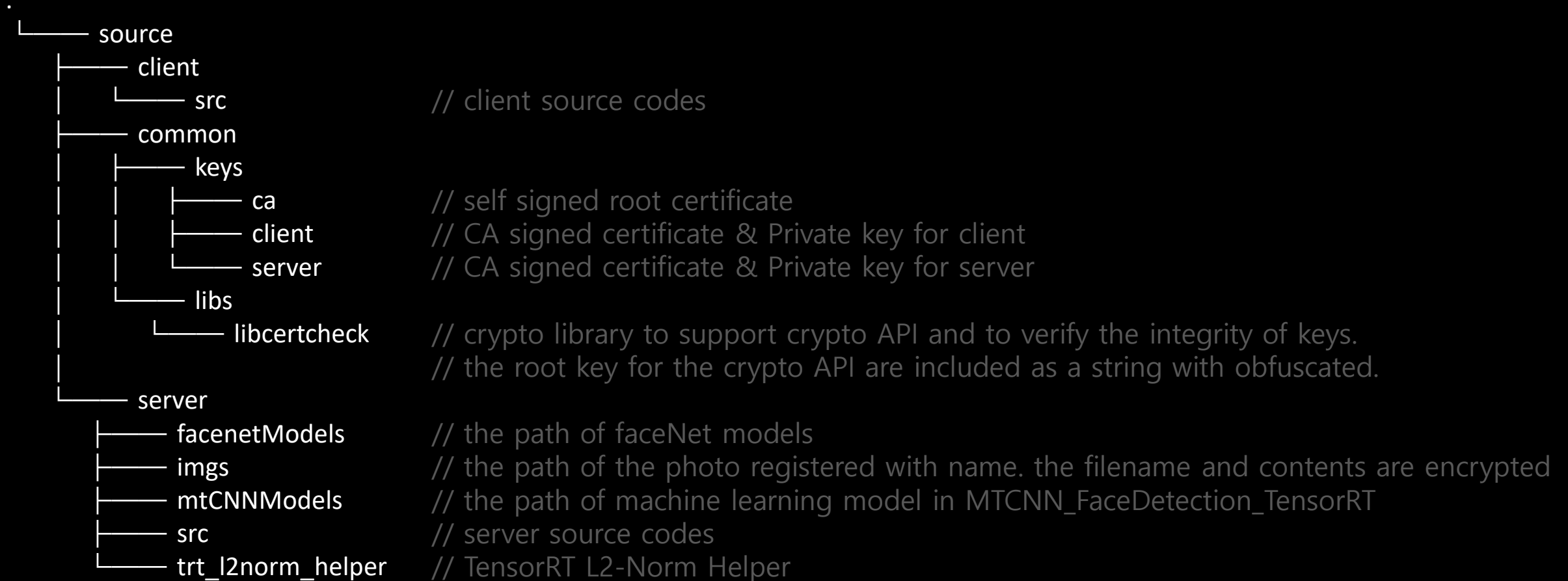
Use a random file name in the storage

Use TLS in network communication

Construct architecture

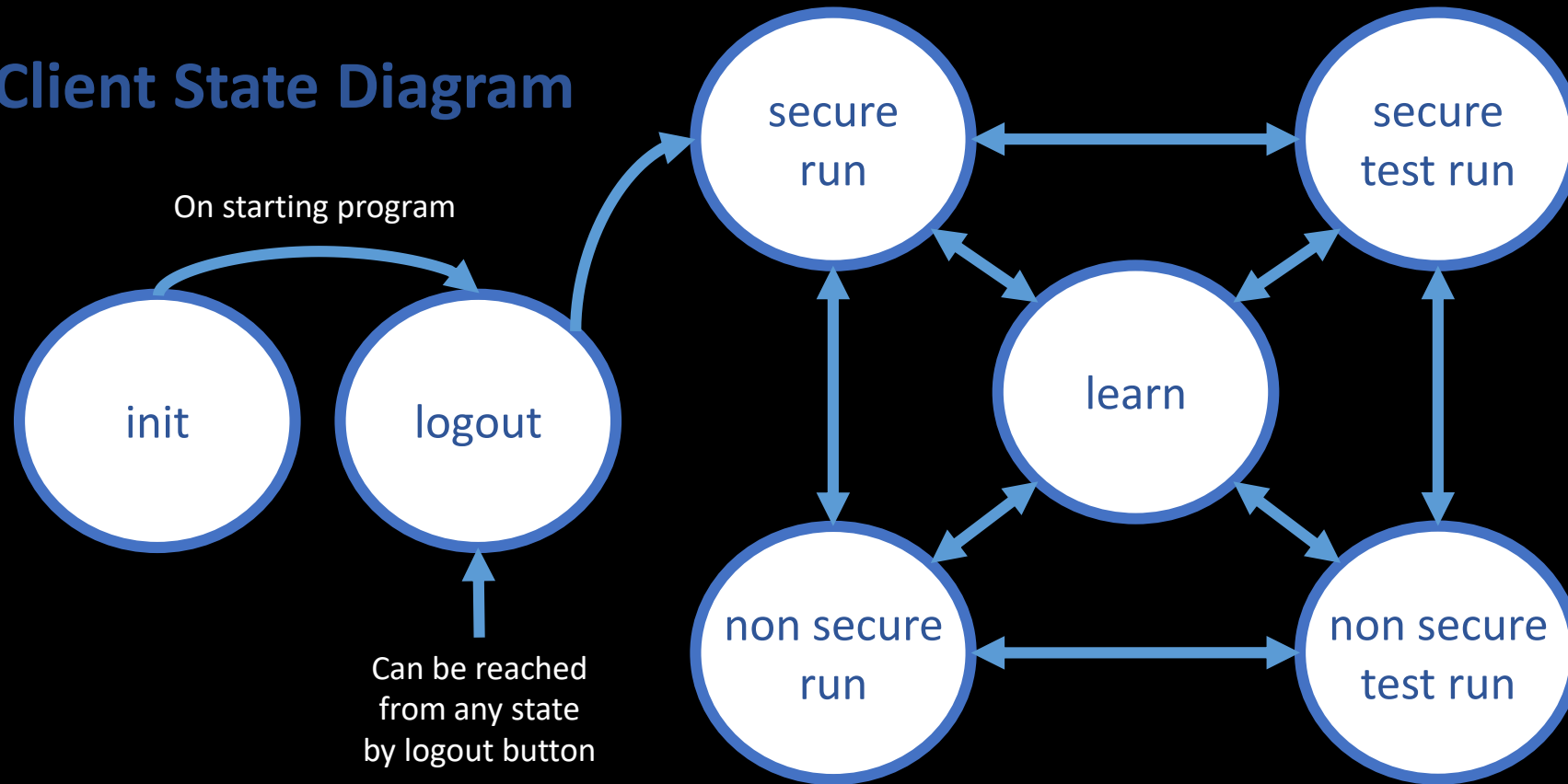


Construct architecture



Construct architecture

Client State Diagram



Construct architecture

Team6 Client App

D:

Pass:

LoginLogout

☒ Secure Mode

☐ Test Mode

Pause

Name:

Learn Mode - Save

Team6 Client App

D: admin

Pass:

LoginLogout


☒ Secure Mode

☐ Test Mode

Pause

Name:

Learn Mode - Save



Construct architecture

Let me show you demo clip..