Phase 1

LGE Security Specialist 2022

Team 4 (S4Best)

July, 2022

Carnegie Mellon University

LG

Agenda

01 - Introduction

02 - Analysis

03 - Threat modeling

04 - Architecture

05 - Mitigations

06 - Lessons Learned

07 - Demo / Q&A

1. Introduction

- Members & Roles

Members & Roles

- **Team 4 intro**

Team name	S4Best (Security For Best)
Motto	Do Best

- **Who we are…**

JG	(Jaegeun Lee)	{ Core engineering, Client side }
SE	(Seongeun Kim)	{ System Architecture, Server side }
JH	(Jeongho Choi)	{ System logic, Threat analysis }
NS	(Namseok Kim)	{ DevOps, Team Leading }
CR	(Choongrae Kim)	{ Secure logic, Communication }
JW	(Jiwoong Eom)	{ Authentication, Risk analysis }

- **Special thanks to**

Clifford Huff as a mentor
Jeffrey Gennari as a professor
Nancy Mead as a professor
Myongsook Jin as a manager
Jihye Yoo as a manager
and
All of the participants for 2022 LGE security specialist

2. Analysis

- Requirements
- Scenario

❑ Analyze SW requirements

App	ReqNo	Requirement	Analysis	Review
Client	REQ_CLI_01	The system shall allow an officer to login and authenticate users locally and to the backend license plate database lookup. The system must use two factor authentication for sign on and user credentials must be protected.	1. After implementing the auth function, call the auth function at the beginning of the entry point (main function) (1) Membership registration (id, pwd, name, place to born, nickname when young): After selecting 1 on the console base, have them input the ID PWD Name, check the server for duplicate IDs, and register it on the server (password is hash) (1-1) Or, after fixing one officer record, the rest of the information is updated (2) Login interaction when console 2 is selected: (3) After entering login information, two-factor authentication using Google Authenticator	Agreed User Credential: ID/Password, password initialization answer, etc. (saved in encryption or hash digest)
Client	REQ_CLI_02	Lost or compromised credentials must be handled in a reasonable way.	2. (1) Insert revocation field into member information of server DB (2) If you select 3, enter the e-mail to receive the temporary password, place to born and nickname -> After sending to the server, after mapping with the server DB, if they match, the server uses the random number generator to update the user's password and sends an email to the client -> If there is a mapping mismatch, notify the client	Server Credential : Root CA (TLS) Validating only the server in TLS (mutual authentication X/ Client is replaced with 2nd authentication)
Client	REQ_CLI_03	The system should allow a law enforcement officer to select and save retrieved information locally.	3	Need to discuss later how to save
Client	REQ_CLI_04	The system should allow a law enforcement officer to send retrieved information to a mobile device, such as a mobile phone to use in the field.	4. (1) Upload the saved content to the cloud (aws, google, etc) (2) Check the contents by accessing the cloud from the mobile phone	

Client	REQ_CLI_09	If a license plate does not generate an alert, then the user interface must display the last recognized plate image, the recognized license plate number and vehicle make, model and color so the operator can visually check if the plate matches the vehicle if desired.	It is judged that no separate modification is necessary Transfer plate information to the server through the detectandshow(&alpr, fra If there is matched information from the server through the GetResponses() f	If the current client reads the license plate information and sends it to the server, the server sends the matching plate information to the client, and the client outputs the following information on the screen. sent ->ZPV5837 Response ZPV5837 No Wants / Warrants 04/13/2023 Christopher Gordon 05/11/1937 45792 Tammy Centers Apt. 258 Davidmouth, HI 02231 2005 Aston Martin Metro time			
Client	REQ_CLI_10	The system should provide an area in the user interface that always contains the current camera /playback view.	We need to provide an area of the UI that contains the camera/playback view	already been provided			
Client	REQ_CLI_14	The system should alert officers of any communication errors or failures.	Follow-up according to requirement 13 - Display User Alert	Should the message to notify the Officer be displayed in the Log window as well? --> Take separate log --> Create separate alert processing and Auth processing windows	- Need to be displayed on the screen when timeout occurs	- Since the "text" String is already being displayed on the screen, it is necessary to insert an appropriate Alert Message into "text"	
Client	REQ_CLI_15	The system must fetch vehicle information in no more than 10 seconds as officers are often making queries in real time.	Number information must be delivered within 10 seconds and information about the vehicle must be received from the server		- Performance QA	- There are no implementations that require additional functionalities, but the Quality Attribute Scen. design alternatives should be selected according to	Quality Req Security Asset - DOS
Server	REQ_SVR_01	Support license plate queries.	License plate query function must be supported - When a license plate arrives, the user's information corresponding to the license p		Query function available. If the current match is cor DB Access / Read function implemented	Need to implement packet handling callback function	Callback Handling related Sync/Asynx ? - Implementation with Asynx seems to be necessary
Server	REQ_SVR_02	Ensure secure communication with the client applications.	It is necessary to establish a secure communicatio - Use TLS1.2 or higher - Use AES 256 bit or higher - Using mutual atheentication	Server authentication only, no mutual authentication Client authentication is replaced by secondary authentication	-	TLS1.2 enforcement (using openssl?) Apply mutual authentication	Both server/client need work How to get the certificate issuance policy?
Server	REQ_SVR_03	Authenticate remote laptop users.	User authentication is required. - ID/PW - Certificate based?	store hash value in db When passing the hash value, it is transmitted encrypted with the server's certificate	-	Apply a function to check whether a valid user's acce - ID/PW verification ? - Certificate Verification ?	When saving password, check how to keep it safely (Create a digest with SHA256 or higher and save it to a file?) How to get the certificate issuance policy?
Server	REQ_SVR_04	Support multiple users.	Must support multi-user access		bind - ANY, port - 2222 Single Thread --> Single Connection	Structural redesign and implementation required with Remote connection confirmation required Only one connection per person is maintained (in ca After confirming the capability, it is necessary to nego Stress Test Verification (Related to REQ_CLI_07/RE	Reads connection information such as port from the configuration file and configures it
Server	REQ_SVR_05	Return the best match license plate if there is not an exact match that includes a configurable minimum confidence threshold to support a partial match.	If no exact match is found, the best match license plate should be returned. For partial matching, it should include a settable reliable threshold value.		Only the data that exactly matches the PlateString (	Additional implementation of partial matching functio Need to implement additional setting function throu Rapidfuzz-cpp OSS that implements Levenshtein DI	Currently using Berkeley DB 18.1.40 Review whether the function to satisfy the requirements can be implemented through the above DB
Server	REQ_SVR_06	Track the average number of queries per second for each user and overall queries per second, for all users	We need to track the average number of queries per second. We need to track the average number of queries per second for each user.		-	Need to implement additional function to count and track queries per second	
Server	REQ_SVR_07	Track the number partial matches and no matches for each user and all users	We need to track the number of partial matches and non-matches for each user and		-	Additional implementation of partial match and unmatched tracking functions is required.	
Server	REQ_SVR_08	Support configurable values via a configuration file.	Must support configurable values through configuration files.		-	Need to implement additional setting value and setting file support function	DB file path setting?, Server port s

1. Analyzing and Categorizing Requirements
2. Review action Items

❑ Two primary requirements for the system

REQ_CLI_01	Two Factor Authentication

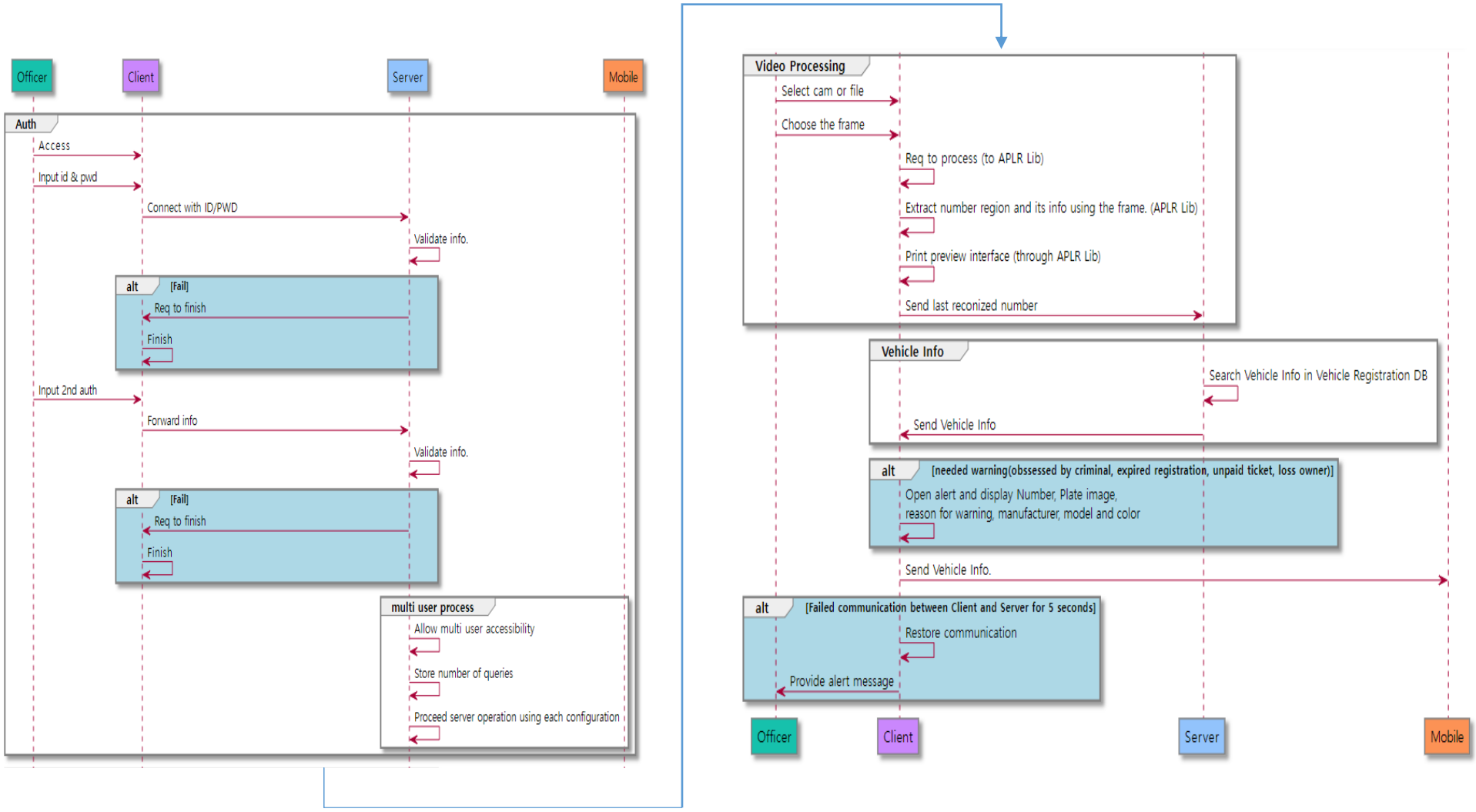
→ Officers can access highly privacy-sensitive information, such as criminal information.

Therefore, to prevent spoofing of officers, it is necessary to take a strengthened account policy.

REQ_CLI_05	Secure Communication between client and server

→ Spoofing/Sniffing of Server/Client are possible at the same time.
This can be protected through mutual authentication and message encryption between client and server.

❑ APLR basic scenario

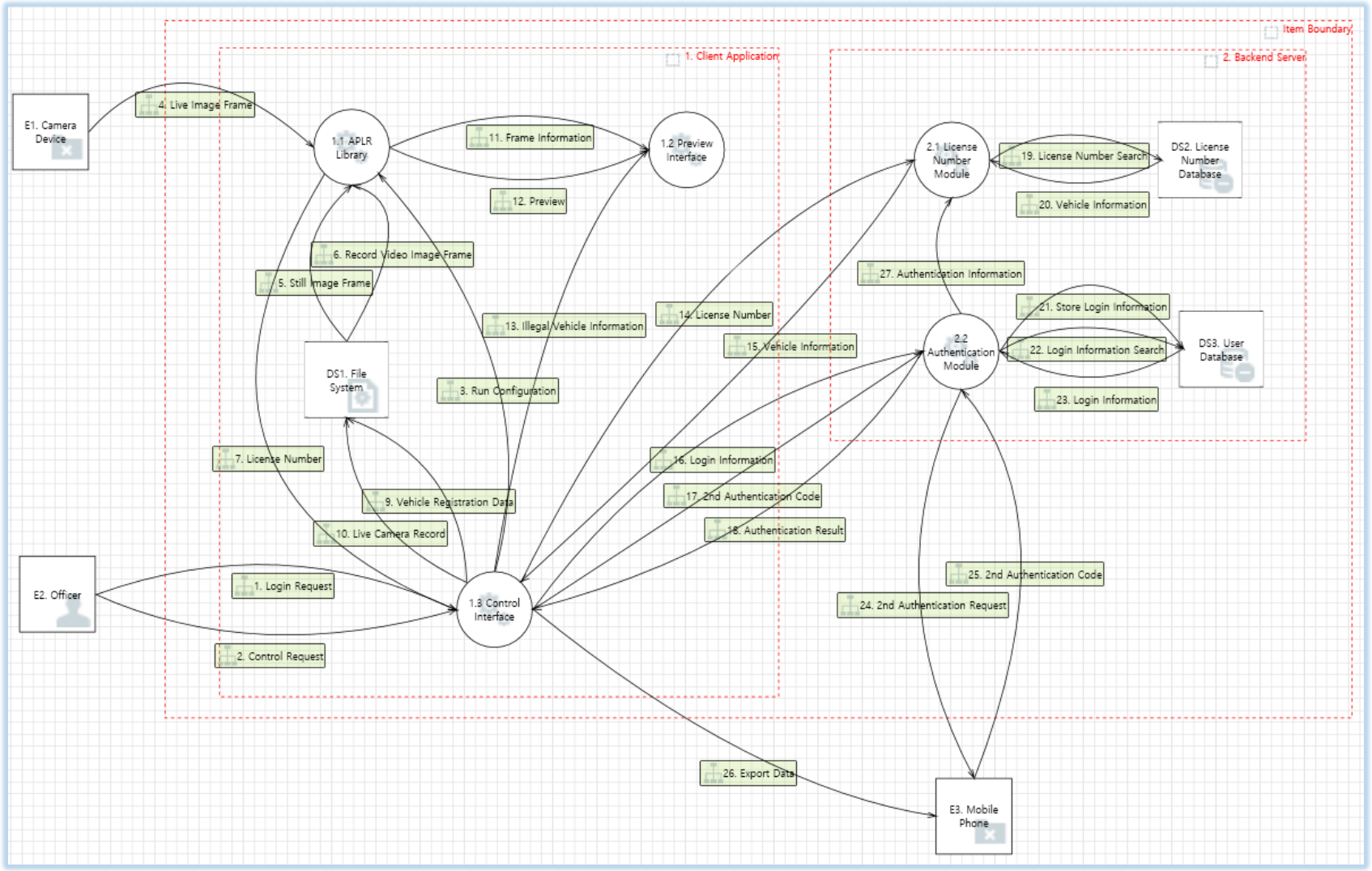


3. Threat modeling

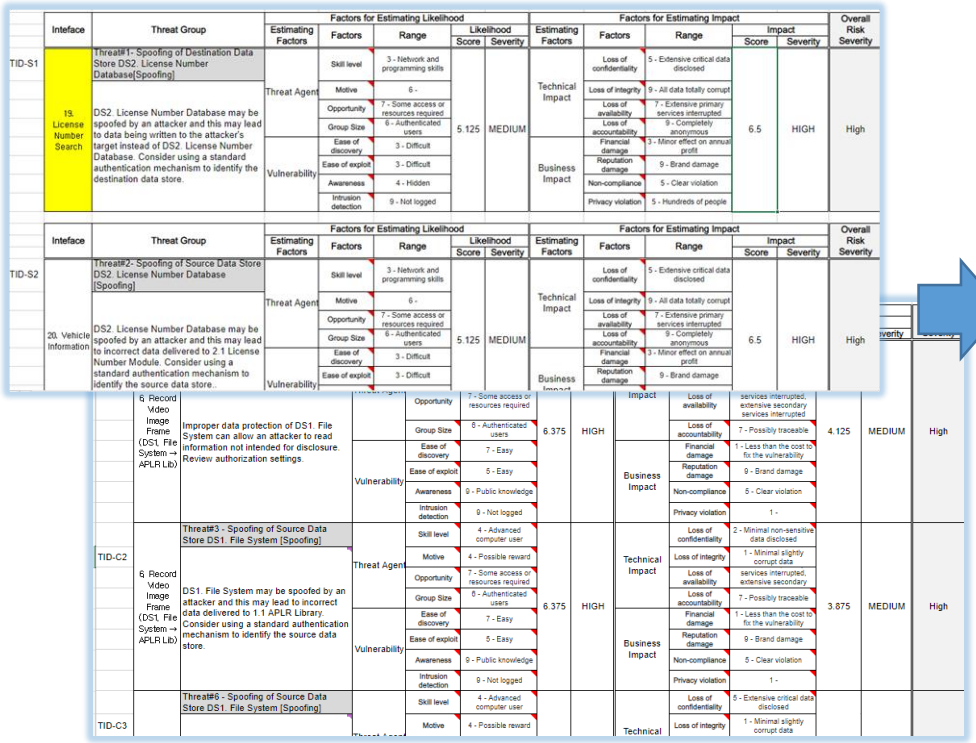
- Threat modeling #1
- Threat modeling #2

Threat Modeling #1

❑ Modeling to get a threat list



❑ Define Thread ID, Vulnerability, Mitigation and Security Requirement



Inteface	Threat Group	Estimating Factors	Factors	Range	Likelihood Score	Likelihood Severity	Estimating Factors	Factors	Range	Impact Score	Impact Severity	Overall Risk Severity
TID-S1	13. License Number Search	Threat#1: Spoofing of Destination Data Store DS2. License Number Database[Spoofing]										
		DS2. License Number Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of DS2. License Number Database. Consider using a standard authentication mechanism to identify the destination data store.	Threat Agent	Skill level	3 - Network and programming skills	5.125	MEDIUM	Technical Impact	Loss of confidentiality	5 - Extensive critical data disclosed	6.5	HIGH	High
				Motive	6 -				Loss of integrity	9 - All data totally corrupt			
				Opportunity	7 - Some access or resources required				Loss of availability	7 - Extensive primary services interrupted			
				Group Size	6 - Authenticated users				Loss of accountability	9 - Completely anonymous			
			Vulnerability	Ease of discovery	3 - Difficult			Business Impact	Financial damage	3 - Minor effect on annual profit			
				Ease of exploit	3 - Difficult				Reputation damage	9 - Brand damage			
				Awareness	4 - Hidden				Non-compliance	5 - Clear violation			
				Intrusion detection	9 - Not logged				Privacy violation	5 - Hundreds of people			
TID-S2	20. Vehicle Information	Threat#2: Spoofing of Source Data Store DS2. License Number Database [Spoofing]										
		DS2. License Number Database may be spoofed by an attacker and this may lead to incorrect data delivered to 2.1 License Number Module. Consider using a standard authentication mechanism to identify the source data store.	Threat Agent	Skill level	3 - Network and programming skills	5.125	MEDIUM	Technical Impact	Loss of confidentiality	5 - Extensive critical data disclosed	6.5	HIGH	High
				Motive	6 -				Loss of integrity	9 - All data totally corrupt			
				Opportunity	7 - Some access or resources required				Loss of availability	7 - Extensive primary services interrupted			
				Group Size	6 - Authenticated users				Loss of accountability	9 - Completely anonymous			
			Vulnerability	Ease of discovery	3 - Difficult			Business Impact	Financial damage	3 - Minor effect on annual profit			
				Ease of exploit	3 - Difficult				Reputation damage	9 - Brand damage			
TID-S5	6. Record Video Image Frame (DS1. File System → APLR Lib)	Improper data protection of DS1. File System can allow an attacker to read information not intended for disclosure. Review authorization settings.	Threat Agent	Skill level	3 - Network and programming skills	6.375	HIGH	Technical Impact	Loss of confidentiality	5 - Extensive critical data disclosed	4.125	MEDIUM	High
				Motive	6 -				Loss of integrity	9 - All data totally corrupt			
				Opportunity	7 - Some access or resources required				Loss of availability	7 - Extensive primary services interrupted, extensive secondary services interrupted			
				Group Size	6 - Authenticated users				Loss of accountability	7 - Possibly traceable			
			Vulnerability	Ease of discovery	7 - Easy			Business Impact	Financial damage	1 - Less than the cost to fix the vulnerability			
				Ease of exploit	5 - Easy				Reputation damage	9 - Brand damage			
				Awareness	9 - Public knowledge				Non-compliance	5 - Clear violation			
				Intrusion detection	9 - Not logged				Privacy violation	1 -			
TID-C2	6. Record Video Image Frame (DS1. File System → APLR Lib)	Threat#3 - Spoofing of Source Data Store DS1. File System [Spoofing]										
		DS1. File System may be spoofed by an attacker and this may lead to incorrect data delivered to 1.1 APLR Library. Consider using a standard authentication mechanism to identify the source data store.	Threat Agent	Skill level	4 - Advanced computer user	6.375	HIGH	Technical Impact	Loss of confidentiality	2 - Minimal non-sensitive data disclosed	3.875	MEDIUM	High
				Motive	4 - Possible reward				Loss of integrity	1 - Minimal slightly corrupt data			
				Opportunity	7 - Some access or resources required				Loss of availability	services interrupted, extensive secondary			
				Group Size	6 - Authenticated users				Loss of accountability	7 - Possibly traceable			
			Vulnerability	Ease of discovery	7 - Easy			Business Impact	Financial damage	1 - Less than the cost to fix the vulnerability			
				Ease of exploit	5 - Easy				Reputation damage	9 - Brand damage			
				Awareness	9 - Public knowledge				Non-compliance	5 - Clear violation			
				Intrusion detection	9 - Not logged				Privacy violation	1 -			
TID-C3		Threat#6 - Spoofing of Source Data Store DS1. File System [Spoofing]										
				Skill level	4 - Advanced computer user			Technical	Loss of confidentiality	5 - Extensive critical data disclosed			
				Motive	4 - Possible reward				Loss of integrity	1 - Minimal slightly corrupt data			

Threat ID	Vulnerability	Mitigation	Security Requirement	SR ID
TID-S1	Spoofing with abnormal DB file (Vehicle Registration DB)	Vehicle Regstration DB File ACL Management	DB File should be protected and managed using ACL. The management policy for DB file should be applicable to Windows 10, Access, read, and write rights for DB files are limited to the backend server.	SR-S1
		Vehicle Regstration DB File Authentication	It is necessary to apply an appropriate authentication technique and go through the authentication process in order to guarantee the integrity and validity of the DB file. This can be done by MAC appended to file contents.	SR-S2
		Vehicle Registration DB User/Password	The user authentication should be applied with user ID and PW to check the validtiy of access rights to DB file.	SR-S3
TID-S2	Spoofing with abnormal DB file (User DB)	User DB File ACL Management	DB File should be protected and managed using ACL. The management policy for DB file should be applicable to Windows 10, Access, read, and write rights for DB files are limited to the backend server.	SR-S1
		User DB File Athentication	It is necessary to apply an appropriate authentication technique and go through the authentication process in order to guarantee the integrity and validity of the DB file. This can be done by MAC appended to file contents.	SR-S2
		User DB User/Password	The user authentication should be applied with user ID and PW to check the validtiy of access rights to DB file.	SR-S3
TID-S5	DoS Excessive access to user DB	Limit the number of simultaneous client connections	Limit the number of simultaneous client connections to mitigate excessive access to the user DB. The maximum number of client connected concurrently is defined as < N.	SR-S4
		Rate Limit : number of log-in errors	Rate limit should be applied to the log-in process to limit the maximum number of errors in order to mitigate excessive access to the user DB.	SR-S5
TID-C1	Information Disclosure Sniffing for play-back file	ACL management regarding to play-back file	Playback files should be protected by managing ACL. Management policies for stored files should be applicable to Windows 10, Access and modification rights for saved files are limited to client application.	SR-C1
TID-C2	Spoofing with abnormal file (Playback file)	ACL management regarding to play-back file	Playback files should be protected by managing ACL. Management policies for stored files should be applicable to Windows 10, Access and modification rights for saved files are limited to client application.	SR-C1
TID-C3	Spoofing with abnormal file (Vehicle Registration Data File)	Vehicle Registration Data File Encryption	Vehicle registration data file should be saved after being encrypted. This is to prevent information leakage due to data sniffing by attackers.	SR-C2

❑ Most concerns

TID-C5	User Spoofing - Weak passwords, password exposure

→ Officers can access highly privacy-sensitive information, such as criminal information.

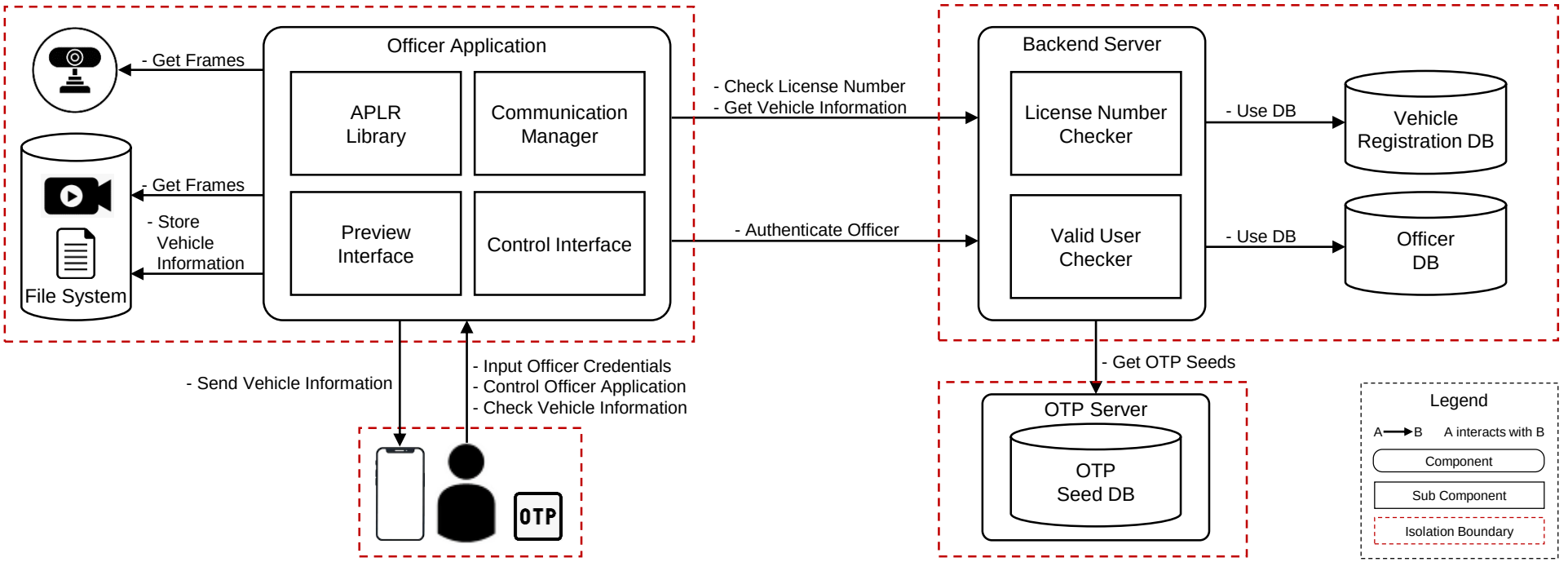
TID-N7	Information Disclosure - Client-Server User ID/PW

→ Officer's ID/PW can be sniffed by monitoring network communication.

4. Architecture

- System context
- Service sequence
- Source tree

❑ System Context Diagram

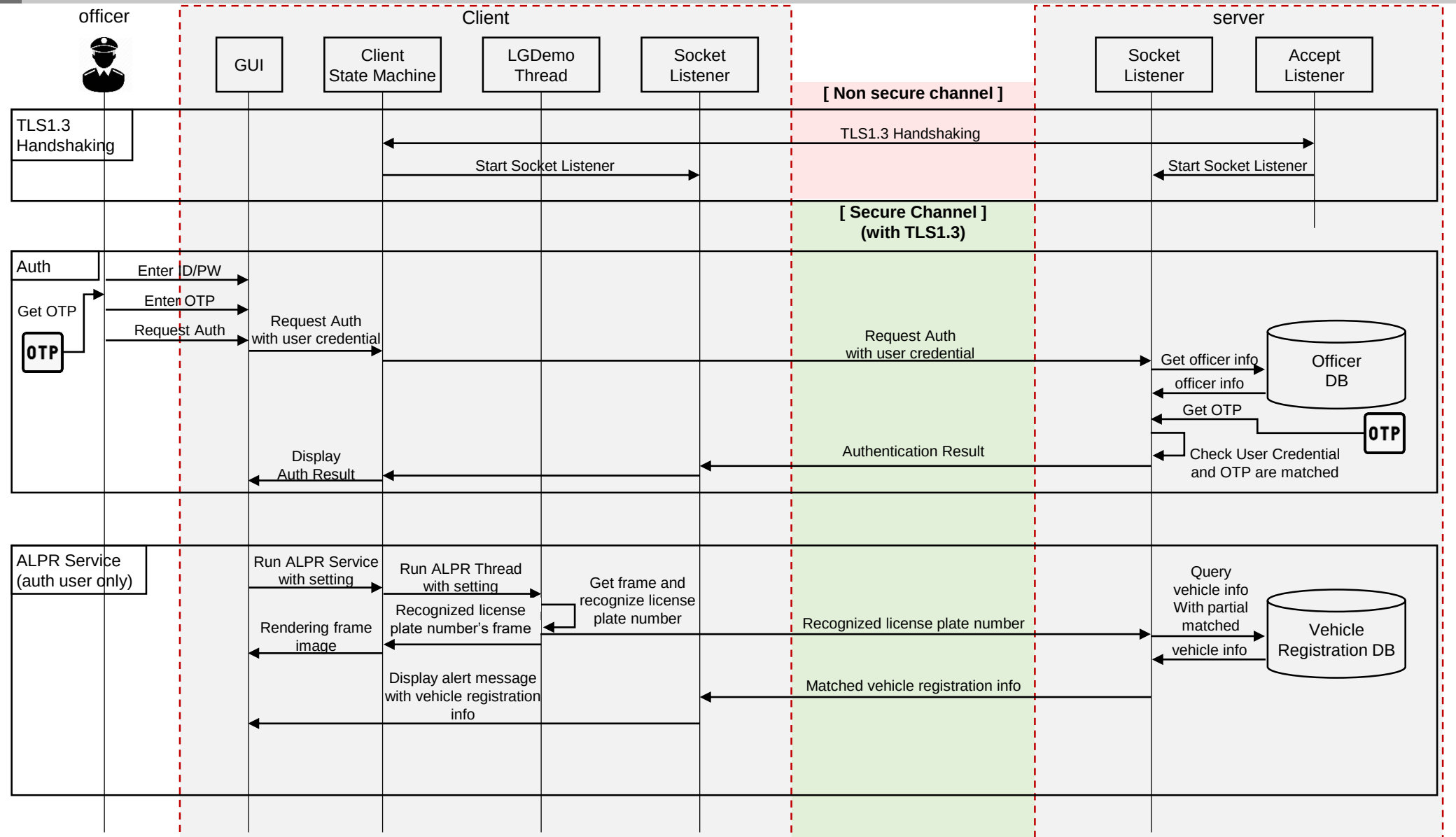


❑ Entity Description

1st Level	2nd Level	Description
Officer Application	APLR Library	Recognizes the license plate area from a specific frame image and extracts the license number
	Preview Interface	Outputs frame images and corresponding frame information
	Control Interface	Proceeds with officer's certification process for client application Sets operation mode of application(frame input selection) Outputs license information of cars
	Comm. Manager	Connect to backend server
User	Officer	Controls officer application
	OTP Device	Used for 2-factor authentication
	Mobile Phone	Officer checks vehicle information sent from officer app.

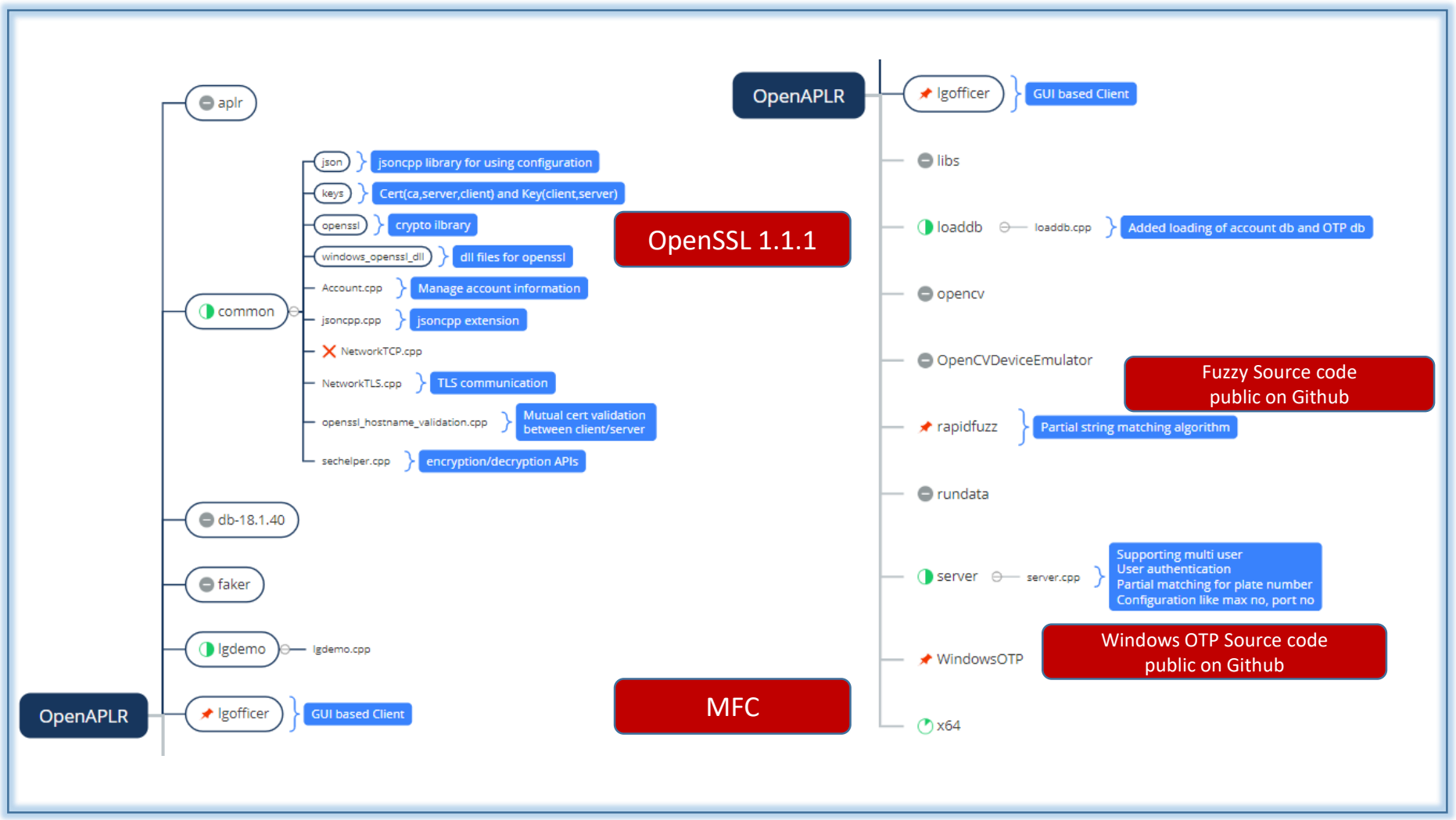
1st Level	2nd Level	Description
Backend Server	License Number Checker	Search and retrieve the vehicle information corresponding to license number delivered from client application from DB, and send those to client application again.
	Valid User Checker	Proceed with user authentication using the two factor authentication with the user ID/PW delivered from client application.
	Vehicle Registration DB	Stores various vehicle information for each vehicle license number.
	Officer DB	Stores officer's user credential, such as ID, PW, account recovery hint, etc.
OTP Server	OTP Seeds DB	Stores seed information of each physical OTP device.

System Service Sequence



Source Tree

❑ Source tree and Libraries / Open source / Framework used



5. Mitigation

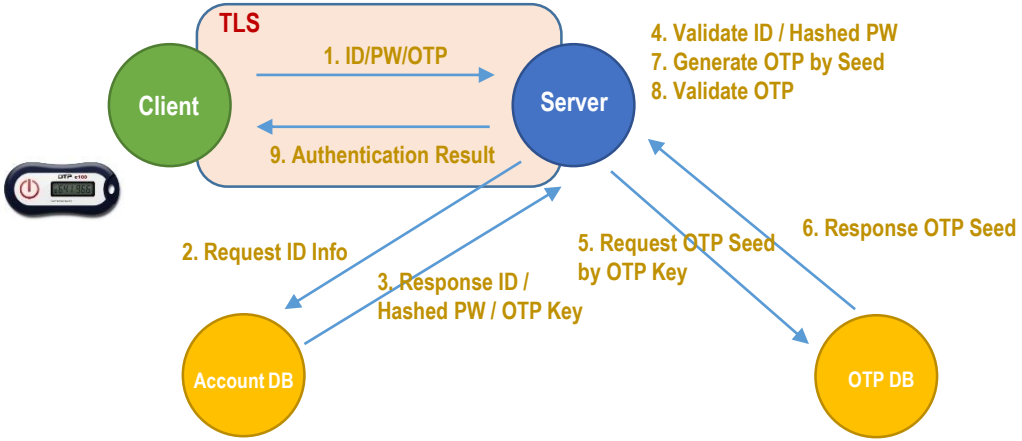
- Multi factor authentication
- TLS
- Input validation

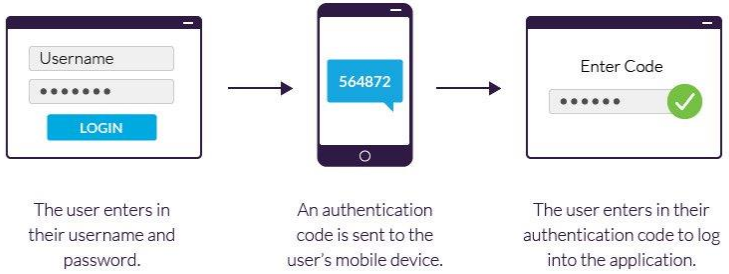
❑ Two factor authentication

1. Basic concept

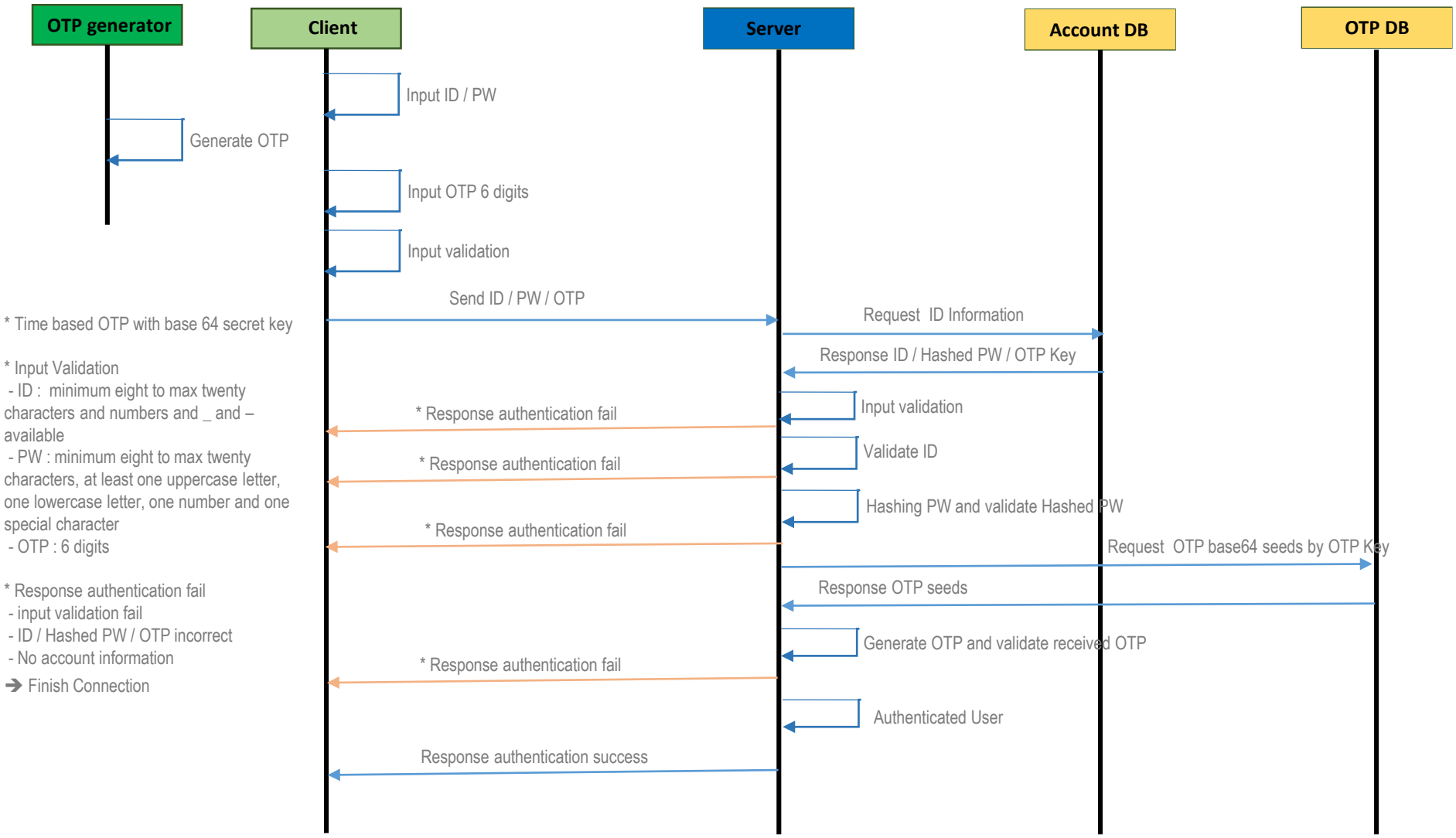
And How?

2. Cross-verifies users with two different forms of identification

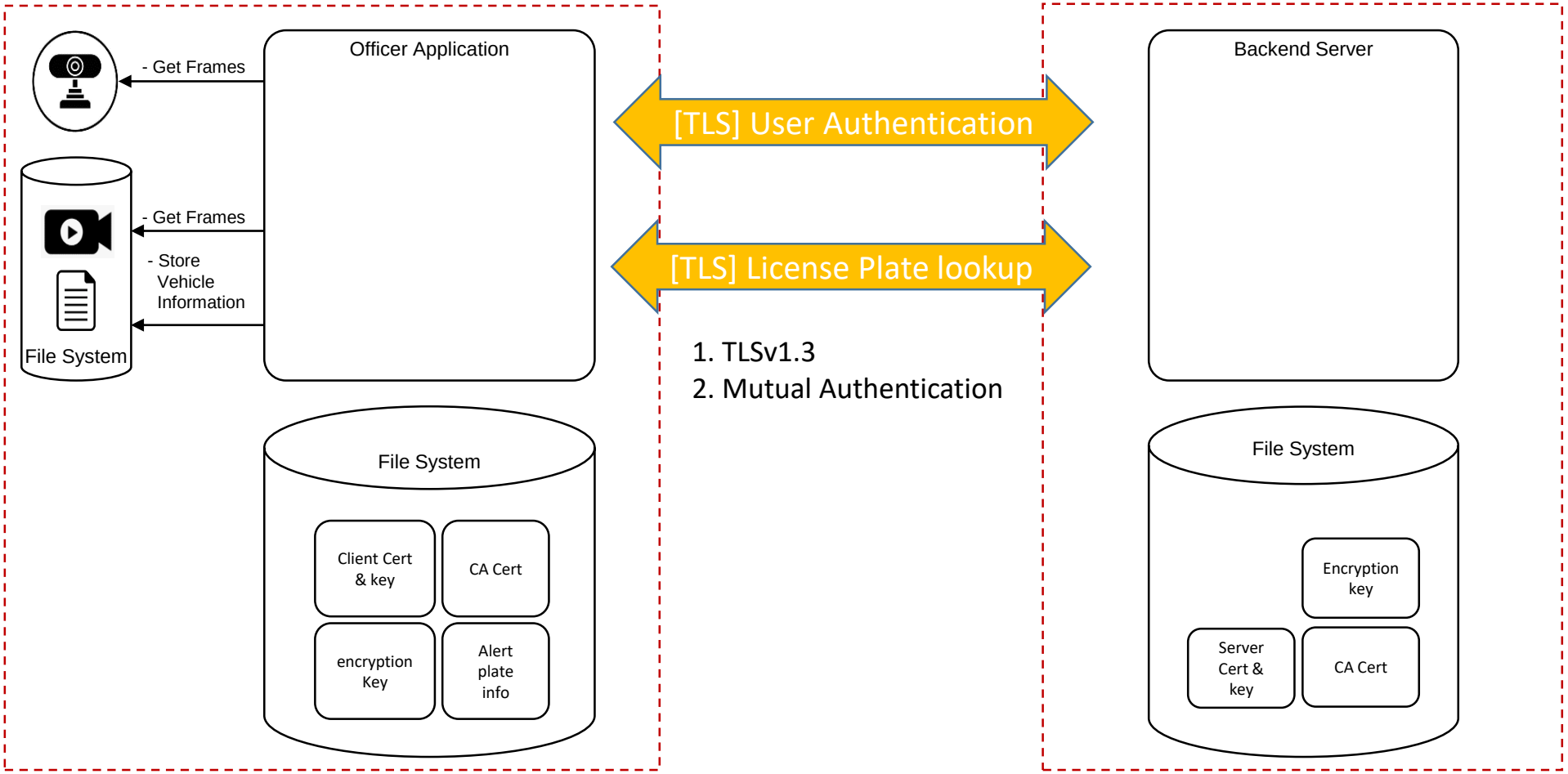




❑ 2FA basic scenario

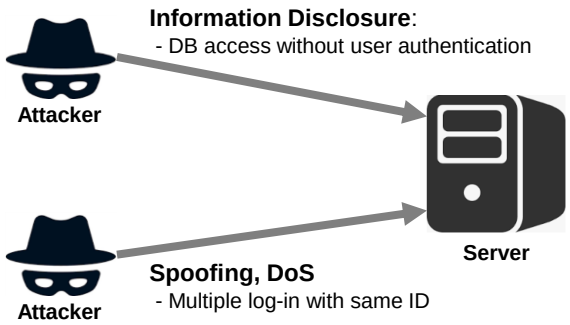


TLS/SSL


Officer Application
- Get Frames
- Get Frames
- Store Vehicle Information
File System
File System
Client Cert & key
CA Cert
encryption Key
Alert plate info
[TLS] User Authentication
[TLS] License Plate lookup
1. TLSv1.3
2. Mutual Authentication
Backend Server
File System
Encryption key
Server Cert & key
CA Cert

Input Validation : Check Packet Validity

❑ Possible Attack Cases

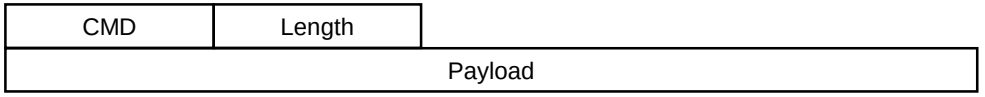


❑ Mitigation

- Keep state consistency between server and client
- Prevent multiple log-in with same ID
- Limit the number of concurrent connected client

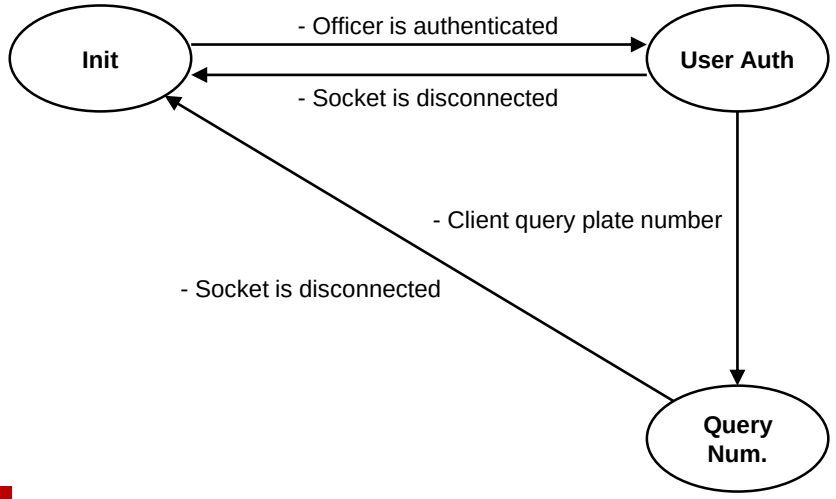
❑ Communication Packet

- Two packets are delivered sequentially : Header + Payload



- CMD is used to check whether client packet corresponds with server state
- Payload consists of contents corresponding to CMD.

❑ State Transition



State	Operation Description
Init	- Server rejects all packets except for user authentication commands. - Once finishing the user authentication, state is switched to “User Auth” state. - If the number of currently connected client exceeds maximum number configured, server rejects all attempts to log in.
User Authentication	- Server accepts only plate number query command. - If user authentication commands arrives, server considers multiple log-in attempts with the same ID and closes the connection.
Query Number	- Server responds every query of client. - If connection is closed, state is switched to “Init” state

6. Lessons learned

- Lessons learned

Lessons learned

- **Lesson #1 -** *Consider it in the early phases*
  - ✓ Importance of abstracting security requirement from initial phase.
  - ✓ In the process of converting a program based on traditional TCP communication to TLS-based communication, many difficulties were encountered.
  - ✓ This is an obvious technical debt, and it is a cost that would not have been incurred if TLS was considered from the initial requirements analysis stage.

- **Lesson #2 -** *Opportunity to learn and experience the secure development methodology*
  - ✓ Opportunity to learn the secure development methodology, such as extracting requirements from asset, threat, risk analysis and applying secure coding.

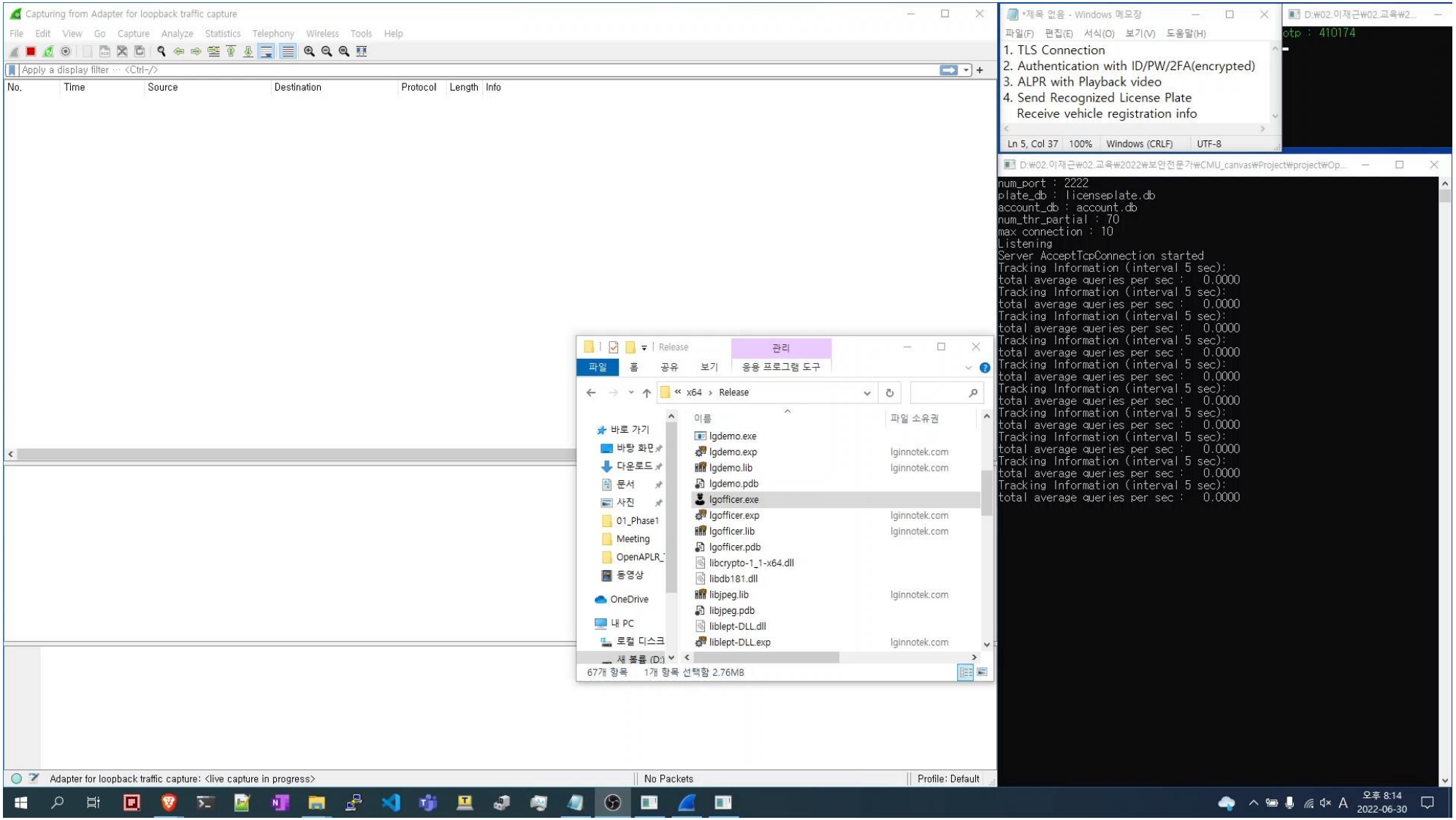
- **Lesson #3 -** *Having secondary security measures*
  - ✓ 2FA offer better protection than passwords alone.

- **Lesson #4 -** *Consider security development process*
  - ✓ Organizations that do not implement a vulnerability management process are at significantly increased risk of experiencing a security incident.

7. Demo / Q&A

- Demo
- Q&A

❑ Clip video for demo



Thank You