Automatic License Plate Recognition (ALPR) System

Security 4 Best

About This Document

Document Information

Issuing authority	S4Best Team
Status of document	Draft / Approved / Released

Revision History

Version	Date	Comment	Author
0.5	2022-07-06	Project Phase 1 Release	S4Best Team

Conventions and Acronyms

Conventions

In this section, describe useful notes and important things audience should know as follows.

NOTE
Useful notes.

CAUTION
Important things

Acronyms

Acronym	Description
Abuse Use Case	Deliberate abuse of functional use cases in order to yield unintended results.
Accountability	The property that ensures that the actions of an entity may be traced uniquely to that entity.
Actor (Threat Agent)	Person who originates attacks, either with malice or by accident, taking advantage of vulnerabilities to create loss.
Application Programming Interface (API)	A source code interface that a computer system or program library provides to support requests for services to be made of it by a computer program [PCI HSM Security Req].
Asset	An asset is a resource of value. It varies by perspective. To a business, an asset might be the availability of information, or the information itself, such as customer data. It might be intangible, such as a company's reputation.
Attack (Exploit)	An attack is an action taken that utilizes one or more vulnerabilities to realize a threat.
Attack Surface	Logical area (browser stack, infrastructure components, etc.) or physical area (hotel kiosk) that an attack may occur or originate from.
Attack Vector	Point and channel for which attacks travel over (card reader, form fields, network proxy, client browser, etc.).
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator [NIST SP 800-137, CNSSI 4009].
Authentication	The process of determining whether someone or something is, in fact, who or what it is declared to be "http://whatis.techtarget.com"
Authorization	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls [NIST SP 800-137, CNSSI 4009].
Availability	Ensuring timely and reliable access to and use of information [NIST SP 800-137, 44 U.S.C., Sec. 3542]. Capability of a product to provide a stated function if demanded, under given conditions over its defined lifetime [ISO 26262-1].
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [NIST SP 800-137, 44 U.S.C., Sec. 3542].

Countermeasures (Control)	Countermeasures address vulnerabilities to reduce the probability of attacks or the impacts of threats. They do not directly address threats; instead they address the factors that define the threats.
Impact	Value of damage possibly sustained via an attack.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity [NIST SP 800-137, 44 U.S.C., Sec. 3542].
Multi-tenant	An architecture in which a single computing resource is shared but logically isolated to serve multiple consumers [NIST.SP.500-322].
Non-repudiation	The ability to provide proof of the integrity and origin of data.
Privacy	The ability to provide protection against personal data discovery and misuse of that information by other users [Common Criteria Part 2].
Possession and/or control	the system and associated processes shall be designed, implemented, operated and maintained so as to prevent unauthorized control, manipulation or interference
Randomness	A random bit sequence could be interpreted as the result of the flips of an unbiased “fair” coin with sides that are labeled “0” and “1,” with each flip having a probability of exactly ½ of producing a “0” or “1.” Furthermore, the flips are independent of each other: the result of any previous coin flip does not affect future coin flips. The unbiased “fair” coin is thus the perfect random bit stream generator, since the “0” and “1” values will be randomly distributed (and [0,1] uniformly distributed). All elements of the sequence are generated independently of each other, and the value of the next element in the sequence cannot be predicted, regardless of how many elements have already been produced [NIST 800-22].
Safety	The design, implementation, operation and maintenance of the system and associated processes shall not jeopardize the health and safety of individuals, the environment or any associated assets. Absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems [ISO 26262-1].
Spoof	The term is used to describe a variety of ways in which hardware and software can be fooled. IP spoofing, for example, involves trickery that makes a message appear as if it came from an authorized IP address.
Tampering	The ability to change data in transit or in a data store.
Threat	A threat is an undesired event. A potential occurrence often best described as an effect that might damage or compromise an asset or objective. It is

	relative to each site, industry, company and is more difficult to uniformly define.
Trasnport Layer Security (TLS)	Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. The protocol is widely used in applications such as email, instant messaging, and voice over IP, but its use in securing HTTPS remains the most publicly visible.
Secure Socket Layer(SSL)	Netscape's Secure Socket Layer protocol [SSL3]. TLS is based on SSL Version 3.0. [RFC5246]

Table of Contents

1 Requirement Engineering 1

1.1 Client – Functional Requirements 1

1.2 Client – Non-Functional Requirements 2

1.3 Sever – Functional Requirements 2

1.4 Client – Non-Functional Requirements 2

2 Security Goals 3

2.1 Business Goal 3

2.2 Security Goal 3

3 Preliminary System Architecture 4

3.1 Preliminary System Architecture and Item boundary 4

3.2 System Architecture Element 4

3.3 Operation Scenario 6

3.4 Assumptions (TBD) 9

4 Threat Modeling 10

4.1 STRIDE. 10

4.2 OWASP Risk Assessment 10

4.2.1 Risk Rating 10

4.2.2 Server Threat List 11

4.2.3 Client Threat List 13

4.2.4 Network Threat List 15

4.3 PnG Risk Assessment 17

4.3.1 Identify the PnG types, goals, motivations, skills 17

4.3.2 Comparison with STRIDE 20

5 Architecture Design 21

5.1 System Architecture 21

5.1.1 System Context Diagram 21

5.1.2 State Transition 21

5.1.3 System Service Sequence 22

5.2 Client Architecture 23

5.2.1 Client State Diagram 23

5.3 2 Factor Authentication. 23

5.3.1 Basic Concept 23

5.3.2 Cross-verifies users with two different forms of identification 23

5.3.3 2FA Basic Scenario 24

5.4 TLS/SSL...25

Figures

Figure 1 Preliminary System Architecture 4

Tables

Table 1 Client – Functional Requirements 1
Table 17 Server Threat 009 13
Table 27 Network Threat 002 15

1 Requirement Engineering

1.1 Client – Functional Requirements

Table 1 Client – Functional Requirements

ID	Statement
REQ_CLI_FUNC_001	The system shall allow an officer to access the ALPR system through a secure web interface
REQ_CLI_FUNC_002	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.
REQ_CLI_FUNC_003	The system should allow a law enforcement officer to select and save retrieved information locally.
REQ_CLI_FUNC_004	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.
REQ_CLI_FUNC_005	The system should read images from the vehicle camera or a playback file and identify license plates for evaluation.
REQ_CLI_FUNC_006	The system should perform the ALPR function in real-time while maintaining a frame rate of at least 25fps.
REQ_CLI_FUNC_007	The system should query the backend license plate server for details about the vehicle. The user must be alerted for vehicles that are stolen, the owner is wanted (criminal), or if it is a vehicle of interest (expired registration, unpaid tickets, owner is missing). Alerts must contain reason and vehicle make, model and color along with the isolated plate image and the recognized license plate number for operator comparison.
REQ_CLI_FUNC_008	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.
REQ_CLI_FUNC_009	The system should provide an area in the user interface that always contains the current camera /playback view.
REQ_CLI_FUNC_010	The system should allow officers to configure computed camera / playback frames per second, average time per frame, jitter and frame number.
REQ_CLI_FUNC_011	The system should allow the officer to choose between using a live camera and playback file in the UI.
REQ_CLI_FUNC_012	The system should alert officers of any communication errors or failures.

1.2 Client – Non-Functional Requirements

Table 2 Client - Non-Functional Requirements

ID	Statement
REQ_CLI_NON_001	Lost or compromised credentials must be handled in a reasonable way.
REQ_CLI_NON_002	The system should provide secure communication between the client application and to the backend license plate database lookup system.
REQ_CLI_NON_003	The ability to detect network connectivity issues with the backend server within 5 seconds and automatically resolve the communication issue if possible.
REQ_CLI_NON_004	The system must fetch vehicle information in no more than 10 seconds as officers are often making queries in real time.

1.3 Sever – Functional Requirements

Table 3 Server - Functional Requirements

ID	Statement
REQ_SVR_FUNC_001	Support license plate queries.
REQ_SVR_FUNC_002	Authenticate remote laptop users.
REQ_SVR_FUNC_003	Support multiple users.
REQ_SVR_FUNC_004	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.
REQ_SVR_FUNC_005	Track the average number of queries per second for each user and overall queries per second, for all users.
REQ_SVR_FUNC_006	Track the number partial matches and no matches for each user and all users
REQ_SVR_FUNC_007	Support configurable values via a configuration file.

1.4 Client – Non-Functional Requirements

Table 4 Client - Functional Requirements

ID	Statement
REQ_SVR_NON_001	Ensure secure communication with the client applications.

2 Security Goals

2.1 Business Goal

The system allows authorized users to make decisions based on the information provided by the image recognition system.
Earn our customer’s trust.

2.2 Security Goal

G-01 : Encrypts Sensitive Information
G-02 : Provides Authentication
G-03 : Provides integrity of sensitive data

3 Preliminary System Architecture

This section provide overall system description and strategy for ALPR system.

3.1 Preliminary System Architecture and Item boundary

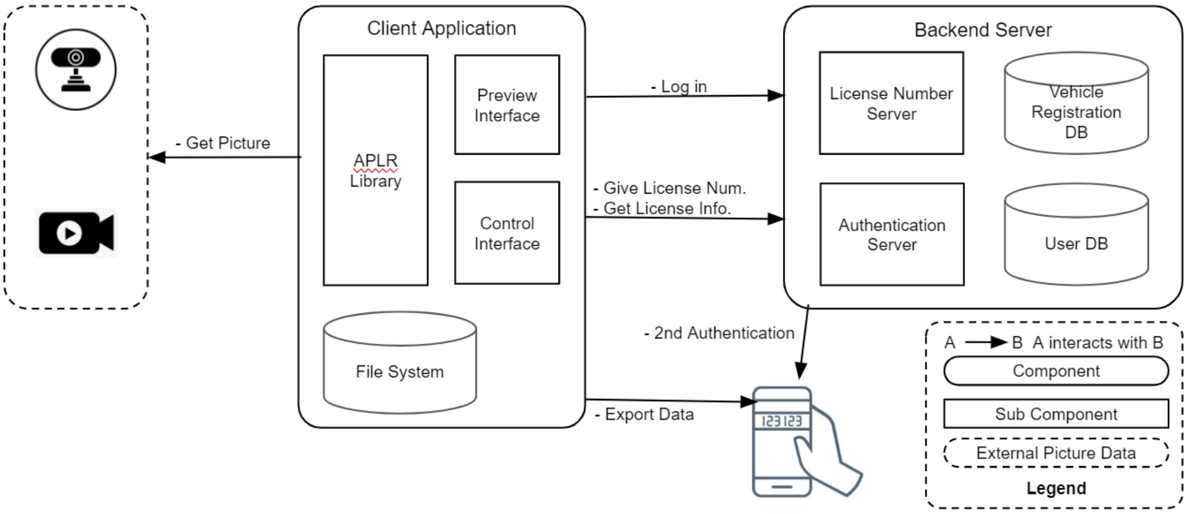


Figure 1 Preliminary System Architecture

3.2 System Architecture Element

Table 5 ALPR System Definition

	Client Application	Backend Server	Mobile Phone	External Picture Data
HW	x86 Base PC	x86 Base PC	NA	NA
Interface	WiFi, Cloud	WiFi, Cloud	WiFi, Cloud	USB, Block IO
OS	Windows 10	Windows 10	Android	NA
SW Module	APLR Lib., Frame Image Interface, Control Interface, File System	License Number Server, Vehicle Registration DB, Authentication Server, User DB	2nd Authentication Application, Vehicle Information Viewer	Live Camera, Playback
Data	User ID, PW Officer authentication result Image of vehicles on the road Image Frame Information	User ID, PW Two Factor Authentication Information Officer authentication result Vehicle license number	Two Factor Authentication Information Vehicle information corresponding to license number	Image of vehicles on the road

	(FPS, Average Time per Frame, Frame Number, Jitter) Vehicle license number Vehicle information corresponding to license number	Vehicle information corresponding to license number		

Table 6 ALPR System Definition

Component	Sub Component	Description
External Picture Data	Live Camera	Video frame image transmitted in real time through the camera
	Play-Back	Video frame image obtained from saved video file
Client 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 (FPS, Average Time per Frame, Frame Number, Jitter)
	Control Interface	Proceeds with officer's certification process for client application Sets operation mode of application(frame input selection) Outputs license information of cars
	File System	Saves license information obtained from backend server
Backend Server	License Number Server	Search and retrieve the vehicle information corresponding to license number delivered from client application from DB, and send those to client application again.
	Authentication Server	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. The field of the saved record follows the predefined form in the assignment introduction.
	User DB	Stores officer's user credential, such as ID, PW, account recovery hint, etc. which are corresponding to each officer.
Mobile Phone	2nd Authentication App.	Mobile application for two factor authentication
	Vehicle Information Viewer	Mobile application for saving and checking vehicle information delivered from client application.

3.3 Operation Scenario

APLR Scenario

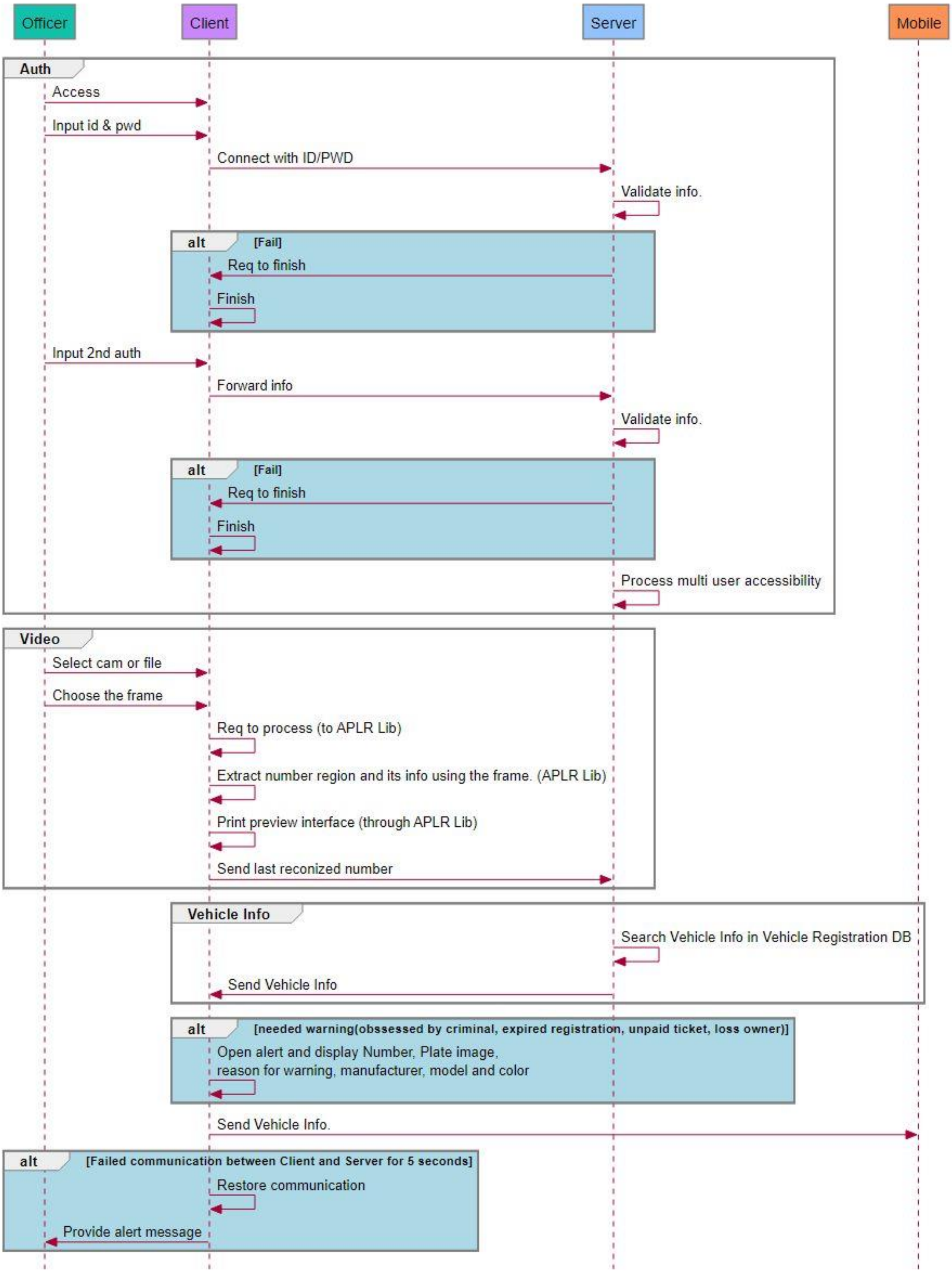

Officer
Client
Server
Mobile
Auth
Access
Input id & pwd
Connect with ID/PWD
Validate info.
alt
[Fail]
Req to finish
Finish
Input 2nd auth
Forward info
Validate info.
alt
[Fail]
Req to finish
Finish
Process multi user accessibility
Video
Select cam or file
Choose the frame
Req to process (to APLR Lib)
Extract number region and its info using the frame. (APLR Lib)
Print preview interface (through APLR Lib)
Send last reconized number
Vehicle Info
Search Vehicle Info in Vehicle Registration DB
Send Vehicle Info
alt
[needed warning(obssessed by criminal, expired registration, unpaid ticket, loss owner)]
Open alert and display Number, Plate image,
reason for warning, manufacturer, model and color
Send Vehicle Info.
alt
[Failed communication between Client and Server for 5 seconds]
Restore communication
Provide alert message

Figure 2 APLR Operation Scenario

1. Client Application Execution and Connection to Server

1.1 The officer runs the client application and connects to the backend server by entering the user ID and password.

1.2 Backend server performs additional verification using two factor authentication infrastructure after validating user ID and password delivered from client application.

1.3 When the validation of step 1.1 and 1.2 is completed, the validation result is delivered to the client application.

1.4 If the result of user verification in step 1.3 is valid, proceed to step 2.1. If it is not valid, the application is terminated.

2. Selection of image of vehicles on the road in client application

2.1 The officer selects one of live camera and playback file as input of image of vehicles on the road.

2.2 Select the frame in the mode selected in step 2.1 as the input of the ALPR Library and proceed with the image recognition process.

3. License number recognition using APLR library

3.1 Extracts the area of the license plate and the license number inside area by using the frame selected in step 2.1 as input.

3.2 Extracts the frame information being processed and outputs it at the bottom of the preview interface.

3.3 Send the last recognized number to backend server

4. Search vehicle information in backend server

4.1 Backend server retrieves the vehicle information corresponding to the number delivered in step 3.3 from vehicle registration DB and delivers it to the client application.

4.2 Step 3.3 and 4.1 should be done within 10 seconds.

5. Alert output of client application

5.1 Alert is displayed when a warning is found in the vehicle information delivered in step 4.1.

Alert displays the vehicle number and license plate image, as well as the reason for the warning, make, model, and vehicle color.

5.2 The reasons for the warning in step 5.1 include theft and criminal possession, deregistration, unpaid tickets, and missing owner.

6. Storing vehicle information and forwarding to mobile phone in client application

6.1 The vehicle information delivered in step 4.1 is collected by the client application and delivered to the mobile phone if necessary.

7. Exception handling when communication fails

7.1 Client application should recover communication problem if communication with backend server fails for 5 seconds.

7.2 The proper alert should be provided to user if a communication problem occurs.

8. Backend server facilities

8.1 Multiple officers physically separated can be connected to backend server.

8.2 The average and total number of queries per second are stored for individual officers and all users, respectively.

8.3 Use the configuration file to set the server operation.

3.4 Assumptions (TBD)

Table 7 Assumption list

Assumptions No.	Description

4 Threat Modeling

4.1 STRIDE.

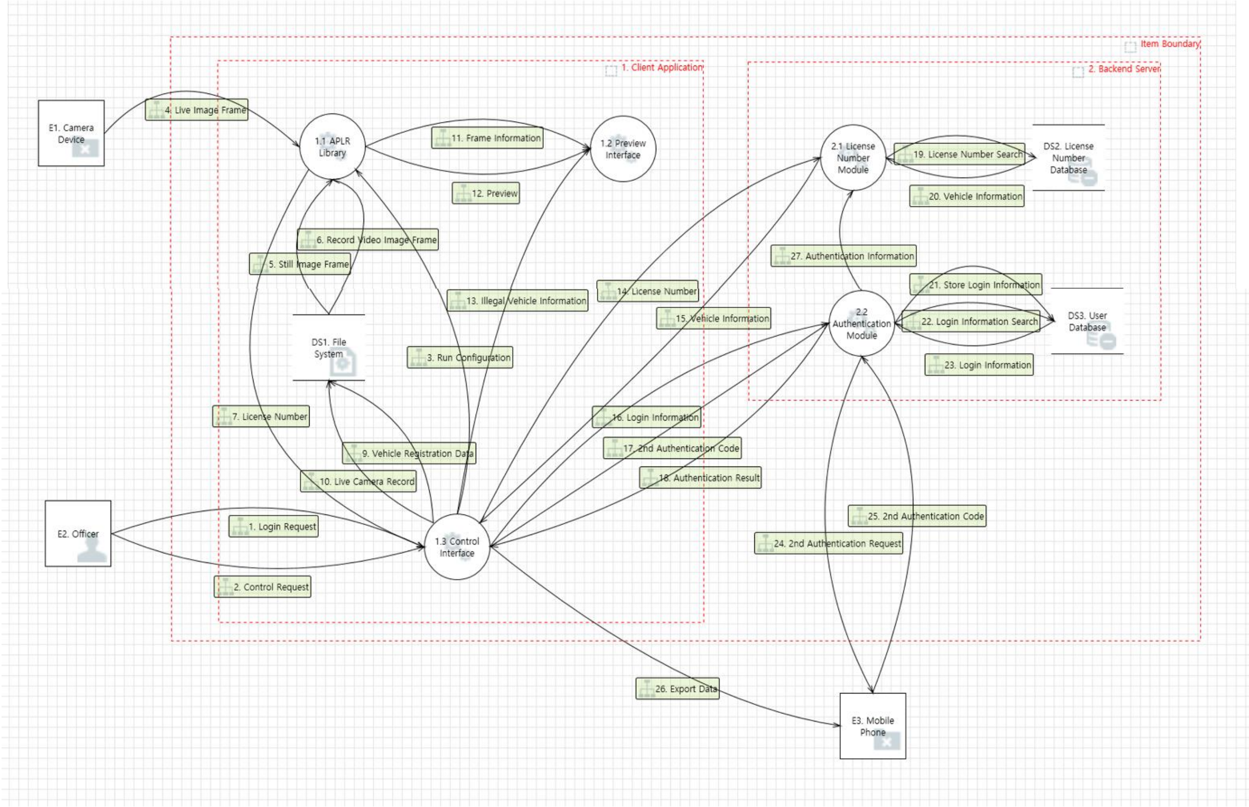


Figure 3 Data Flow Diagram

4.2 OWASP Risk Assessment

4.2.1 Risk Rating

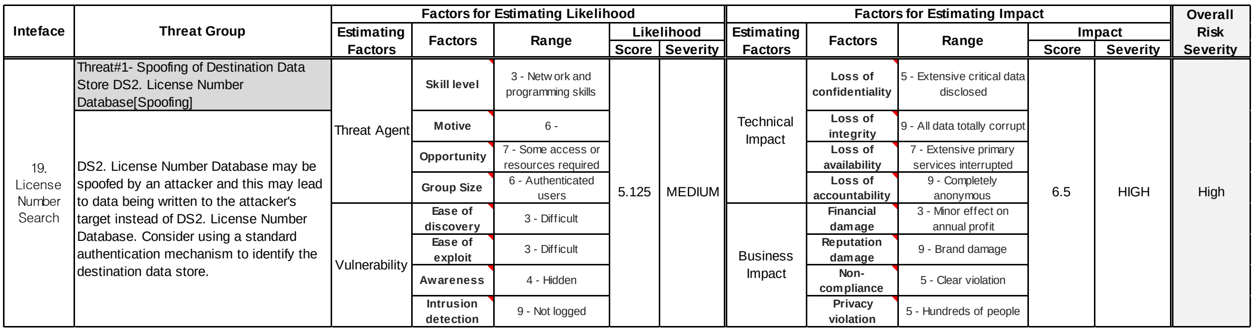
Table 8 Risk Rating

Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

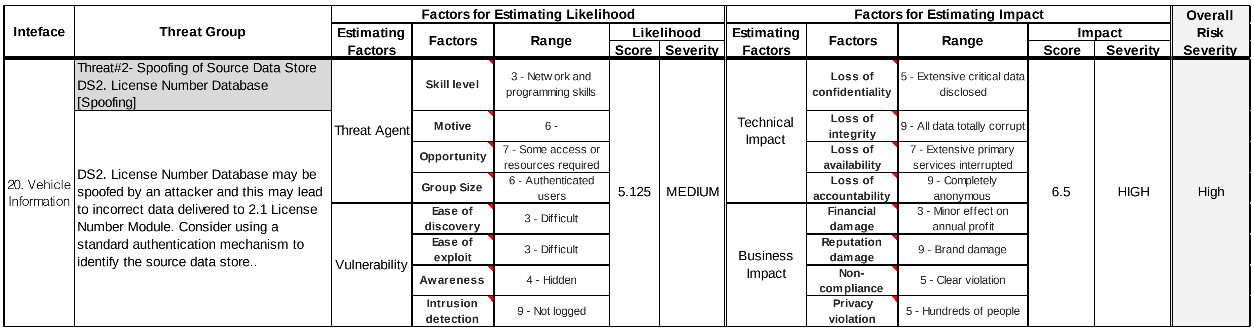
4.2.2 Server Threat List

Table 9 Server Threat 001



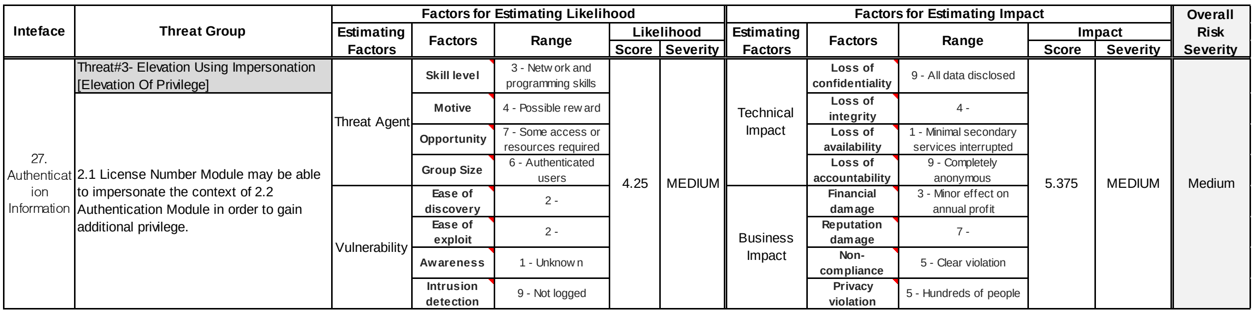
Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
19. License Number Search	Threat#1- Spoofing of Destination Data Store DS2. License Number Database[Spoofing]	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
	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.		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			

Table 10 Server Threat 002



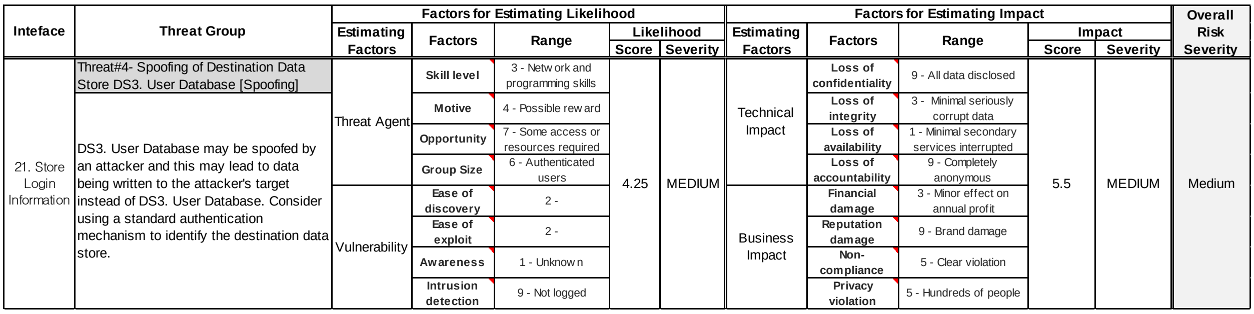
Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
20. Vehicle Information	Threat#2- Spoofing of Source Data Store DS2. License Number Database [Spoofing]	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
	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..		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			

Table 11 Server Threat 003



Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
27. Authentication Information	Threat#3- Elevation Using Impersonation [Elevation Of Privilege]	Threat Agent	Skill level	3 - Network and programming skills	4.25	MEDIUM	Technical Impact	Loss of confidentiality	9 - All data disclosed	5.375	MEDIUM	Medium
	2.1 License Number Module may be able to impersonate the context of 2.2 Authentication Module in order to gain additional privilege.		Motive	4 - Possible reward				Loss of integrity	4 -			
			Opportunity	7 - Some access or resources required				Loss of availability	1 - Minimal secondary services interrupted			
			Group Size	6 - Authenticated users				Loss of accountability	9 - Completely anonymous			
		Vulnerability	Ease of discovery	2 -			Business Impact	Financial damage	3 - Minor effect on annual profit			
			Ease of exploit	2 -				Reputation damage	7 -			
			Awareness	1 - Unknown				Non-compliance	5 - Clear violation			
			Intrusion detection	9 - Not logged				Privacy violation	5 - Hundreds of people			

Table 12 Server Threat 004



Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
21. Store Login Information	Threat#4- Spoofing of Destination Data Store DS3. User Database [Spoofing]	Threat Agent	Skill level	3 - Network and programming skills	4.25	MEDIUM	Technical Impact	Loss of confidentiality	9 - All data disclosed	5.5	MEDIUM	Medium
	DS3. User Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of DS3. User Database. Consider using a standard authentication mechanism to identify the destination data store.		Motive	4 - Possible reward				Loss of integrity	3 - Minimal seriously corrupt data			
			Opportunity	7 - Some access or resources required				Loss of availability	1 - Minimal secondary services interrupted			
			Group Size	6 - Authenticated users				Loss of accountability	9 - Completely anonymous			
		Vulnerability	Ease of discovery	2 -			Business Impact	Financial damage	3 - Minor effect on annual profit			
			Ease of exploit	2 -				Reputation damage	9 - Brand damage			
			Awareness	1 - Unknown				Non-compliance	5 - Clear violation			
			Intrusion detection	9 - Not logged				Privacy violation	5 - Hundreds of people			

Table 13 Server Threat 005

Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
21. Store Login Informaiton	Threat#5 - Denial of Service Data Store DS3. User Database [Denial of Service]	Threat Agent	Skill level	4 - Advanced computer user	6.25	HIGH	Technical Impact	Loss of confidentiality	1 -	4	MEDIUM	High
	Does 2.2 Authentication Module or DS3. User Database 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.		Motive	1 - Low or no reward				Loss of integrity	3 - Minimal seriously corrupt data			
			Opportunity	9 - No access or resources required				Loss of availability	7 - Extensive primary services interrupted			
			Group Size	9 - Anonymous Internet users				Loss of accountability	9 - Completely anonymous			
		Vulnerability	Ease of discovery	6 -			Business Impact	Financial damage	1 - Less than the cost to fix the vulnerability			
			Ease of exploit	6 -				Reputation damage	4 - Loss of major accounts			
			Awareness	6 - Obvious				Non-compliance	2 - Minor violation			
			Intrusion detection	9 - Not logged				Privacy violation	5 - Hundreds of people			

Table 14 Server Threat 006

Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
22. Login Information Search	Threat#6- Spoofing of Destination Data Store DS3. User Database [Spoofing]	Threat Agent	Skill level	3 - Network and programming skills	4.625	MEDIUM	Technical Impact	Loss of confidentiality	1 -	3.25	MEDIUM	Medium
	DS3. User Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of DS3. User Database. Consider using a standard authentication mechanism to identify the destination data store.		Motive	4 - Possible reward				Loss of integrity	1 - Minimal slightly corrupt data			
			Opportunity	8 -				Loss of availability	1 - Minimal secondary 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	4 - Loss of major accounts			
			Awareness	1 - Unknown				Non-compliance	5 - Clear violation			
			Intrusion detection	9 - Not logged				Privacy violation	2 -			

Table 15 Server Threat 007

Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
22. Login Information Search	Threat#7- Potential Excessive Resource Consumption for 2.2 Authentication Module or DS3. User Database[Denial Of Service]	Threat Agent	Skill level	4 - Advanced computer user	5.25	MEDIUM	Technical Impact	Loss of confidentiality	1 -	3.75	MEDIUM	Medium
	Does 2.2 Authentication Module or DS3. User Database 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.		Motive	1 - Low or no reward				Loss of integrity	1 - Minimal slightly corrupt data			
			Opportunity	7 - Some access or resources required				Loss of availability	5 - Minimal primary services interrupted, extensive secondary services interrupted			
			Group Size	8 -				Loss of accountability	9 - Completely anonymous			
		Vulnerability	Ease of discovery	7 - Easy			Business Impact	Financial damage	3 - Minor effect on annual profit			
			Ease of exploit	5 - Easy				Reputation damage	4 - Loss of major accounts			
			Awareness	1 - Unknown				Non-compliance	5 - Clear violation			
			Intrusion detection	9 - Not logged				Privacy violation	2 -			

Table 16 Server Threat 008

Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
23. Login Information	Threat#8- Spoofing of Source Data Store DS3. User Database [Spoofing]	Threat Agent	Skill level	3 - Network and programming skills	4.125	MEDIUM	Technical Impact	Loss of confidentiality	9 - All data disclosed	5.625	MEDIUM	Medium
	DS3. User Database may be spoofed by an attacker and this may lead to incorrect data delivered to 2.2 Authentication Module. Consider using a standard authentication mechanism to identify the source data store.		Motive	4 - Possible reward				Loss of integrity	5 - Extensive slightly corrupt data			
			Opportunity	4 - Special access or resources required				Loss of availability	1 - Minimal secondary 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	8 -			
			Awareness	1 - Unknown				Non-compliance	5 - Clear violation			
			Intrusion detection	9 - Not logged				Privacy violation	5 - Hundreds of people			

Table 12 Server Threat 009

Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
23. Login Information	Threat#9- Weak Access Control for a Resource[Information Disclosure]	Threat Agent	Skill level	3 - Network and programming skills	4.125	MEDIUM	Technical Impact	Loss of confidentiality	5 - Extensive critical data disclosed	4.75	MEDIUM	Medium
	Improper data protection of DS3. User Database can allow an attacker to read information not intended for disclosure. Review authorization seattings.		Motive	4 - Possible reward				Loss of integrity	1 - Minimal slightly corrupt data			
			Opportunity	4 - Special access or resources required				Loss of availability	1 - Minimal secondary 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	1 - Unknown				Non-compliance	5 - Clear violation			
			Intrusion detection	9 - Not logged				Privacy violation	5 - Hundreds of people			

4.2.1 Client Threat List

Table 18 Client Threat 001

Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
6. Record Video Image Frame (DS1. File System → APLR Lib)	Threat#2 - Weak Access Control for a Resource [Information Disclosure]	Threat Agent	Skill level	4 - Advanced computer user	6.375	HIGH	Technical Impact	Loss of confidentiality	2 - Minimal non-sensitive data disclosed	4.125	MEDIUM	High
	Improper data protection of DS1. File System can allow an attacker to read information not intended for disclosure. Review authorization settings.		Motive	4 - Possible reward				Loss of integrity	3 - Minimal seriously corrupt data			
			Opportunity	7 - Some access or resources required				Loss of availability	5 - Minimal 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 -			

Table 19 Client Threat 002

6. Record Video Image Frame (DS1. File System → APLR Lib)	Threat#3 - Spoofing of Source Data Store DS1. File System [Spoofing]	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
	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.		Motive	4 - Possible reward				Loss of integrity	1 - Minimal slightly corrupt data			
			Opportunity	7 - Some access or resources required				Loss of availability	5 - Minimal primary 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 -			

Table 20 Client Threat 003

9. Vehicle Registration Data (Control Interface → DS1. File System)	Threat#6 - Spoofing of Source Data Store DS1. File System [Spoofing]	Threat Agent	Skill level	4 - Advanced computer user	6.375	HIGH	Technical Impact	Loss of confidentiality	5 - Extensive critical data disclosed	4.75	MEDIUM	High
	DS1. File System may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of DS1. File System. Consider using a standard authentication mechanism to identify the destination data store.		Motive	4 - Possible reward				Loss of integrity	1 - Minimal slightly corrupt data			
			Opportunity	7 - Some access or resources required				Loss of availability	5 - Minimal primary 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	5 - Hundreds of people			

Table 21 Client Threat 004

9. Vehicle Registration Data (Control Interface → DS1. File System)	Threat#7 - Potential Excessive Resource Consumption for 1.3 Control Interface or DS1. File System [Denial Of Service]	Threat Agent	Skill level	4 - Advanced computer user	6.25	HIGH	Technical Impact	Loss of confidentiality	2 - Minimal non-sensitive data disclosed	5.125	MEDIUM	High
	Does 1.3 Control Interface or DS1. 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.		Motive	4 - Possible rew ard				Loss of integrity	3 - Minimal seriously corrupt data			
			Opportunity	7 - Some access or resources required				Loss of availability	9 - All services completely lost			
			Group Size	6 - Authenticated users				Loss of accountability	7 - Possibly traceable			
		Vulnerability	Ease of discovery	7 - Easy			Business Impact	Financial damage	3 - Minor effect on annual profit			
			Ease of exploit	5 - Easy				Reputation damage	9 - Brand damage			
			Awareness	9 - Public know ledge				Non-compliance	7 - High profile violation			
			Intrusion detection	8 - Logged w ithout review				Privacy violation	1 -			

Table 22 Client Threat 005

Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
1. Login Request/ 2. Control Request	Threat# - Spoofing the E2. Officer External Entity [Spoofing]	Threat Agent	Skill level	9 - No technical skills	5.5	MEDIUM	Technical Impact	Loss of confidentiality	9 - All data disclosed	6.5	HIGH	High
	E2 Officer may be spoofed by an attacker and this may lead to unauthorized access to 1.3 Control Interface. Consider using a standard authentication mechanism to identify the external entity.		Motive	4 - Possible rew ard				Loss of integrity	3 - Minimal seriously corrupt data			
			Opportunity	4 - Special access or resources required				Loss of availability	7 - Extensive primary services interrupted			
			Group Size	6 - Authenticated users				Loss of accountability	7 - Possibly traceable			
		Vulnerability	Ease of discovery	3 - Difficult			Business Impact	Financial damage	7 - Significant effect on annual profit			
			Ease of exploit	3 - Difficult				Reputation damage	9 - Brand damage			
			Awareness	6 - Obvious				Non-compliance	5 - Clear violation			
			Intrusion detection	9 - Not logged				Privacy violation	5 - Hundreds of people			

Table 23 Client Threat 006

Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
1. Login Request/ 2. Control Request	Threat# - Data Flow Sniffing [Information Disclosure]	Threat Agent	Skill level	9 - No technical skills	6.125	HIGH	Technical Impact	Loss of confidentiality	9 - All data disclosed	6.5	HIGH	Critical
	Data flowing across 1. Login Request 2. Control Request 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.		Motive	9 - High rew ard				Loss of integrity	3 - Minimal seriously corrupt data			
			Opportunity	4 - Special access or resources required				Loss of availability	7 - Extensive primary services interrupted			
			Group Size	6 - Authenticated users				Loss of accountability	7 - Possibly traceable			
		Vulnerability	Ease of discovery	3 - Difficult			Business Impact	Financial damage	7 - Significant effect on annual profit			
			Ease of exploit	3 - Difficult				Reputation damage	9 - Brand damage			
			Awareness	6 - Obvious				Non-compliance	5 - Clear violation			
			Intrusion detection	9 - Not logged				Privacy violation	5 - Hundreds of people			

Table 24 Client Threat 007

Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
1. Login Request/ 2. Control Request	Threat# - Potential Process Crash or Stop for 1.3 Control Interface [Denial Of Service]	Threat Agent	Skill level	4 - Advanced computer user	6	HIGH	Technical Impact	Loss of confidentiality	2 - Minimal non-sensitive data disclosed	3.25	MEDIUM	High
	1.3 Control Interface crashes, halts, stops or runs slowly; in all cases violating an availability metric.		Motive	1 - Low or no rew ard				Loss of integrity	1 - Minimal slightly corrupt data			
			Opportunity	7 - Some access or resources required				Loss of availability	7 - Extensive primary services interrupted			
			Group Size	6 - Authenticated users				Loss of accountability	7 - Possibly traceable			
		Vulnerability	Ease of discovery	7 - Easy			Business Impact	Financial damage	3 - Minor effect on annual profit			
			Ease of exploit	5 - Easy				Reputation damage	4 - Loss of major accounts			
			Awareness	9 - Public know ledge				Non-compliance	2 - Minor violation			
			Intrusion detection	9 - Not logged				Privacy violation	0 -			

Table 25 Client Threat 008

Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
1. Login Request/ 2. Control Request	Threat# - Elevation by Changing the Execution Flow in 1.3 Control Interface [Elevation Of Privilege]	Threat Agent	Skill level	1 - Security penetration skills	5.25	MEDIUM	Technical Impact	Loss of confidentiality	5 - Extensive critical data disclosed	5.75	MEDIUM	Medium
	An attacker may pass data into 1.3 Control Interface in order to change the flow of program execution within 1.3 Control Interface to the attacker's choosing.		Motive	9 - High reward				Loss of integrity	3 - Minimal seriously corrupt data			
			Opportunity	7 - Some access or resources required				Loss of availability	7 - Extensive primary services interrupted			
			Group Size	6 - Authenticated users				Loss of accountability	7 - Possibly traceable			
		Vulnerability	Ease of discovery	3 - Difficult			Business Impact	Financial damage	7 - Significant 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	3 - One individual			

4.2.2 Network Threat List

Table 26 Network Threat 001

Inteface	Threat Group	Factors for Estimating Likelihood					Factors for Estimating Impact					Overall Risk Severity
		Estimating Factors	Factors	Range	Likelihood		Estimating Factors	Factors	Range	Impact		
					Score	Severity				Score	Severity	
License Number	Threat#1- Spoofing the 1.3 Control Interface Process [Spoofing]	Threat Agent	Skill level	3 - Network and programming skills	5	MEDIUM	Technical Impact	Loss of confidentiality	5 - Extensive critical data disclosed	5.125	MEDIUM	Medium
	License Number Module may be spoofed by an attacker and this may lead to information disclosure by 1.3 Control Interface. Consider using a standard authentication mechanism to identify the destination process.		Motive	4 - Possible reward				Loss of integrity	7 - Extensive seriously corrupt data			
			Opportunity	4 - Special access or resources required				Loss of availability	7 - Extensive primary services interrupted			
			Group Size	6 - Authenticated users				Loss of accountability	7 - Possibly traceable			
		Vulnerability	Ease of discovery	7 - Easy			Business Impact	Financial damage	3 - Minor effect on annual profit			
			Ease of exploit	5 - Easy				Reputation damage	4 - Loss of major accounts			
			Awareness	8 -				Non-compliance	5 - Clear violation			
			Intrusion detection	3 - Logged and reviewed				Privacy violation	3 - One individual			

Table 23 Network Threat 002

License Number	Threat#3-Potential Data Repudiation by 2.1 License Number Module [Repudiation]	Threat Agent	Skill level	9 - No technical skills	7.25	HIGH	Technical Impact	Loss of confidentiality	4 - Minimal critical data disclosed, extensive non-sensitive data disclosed	3.625	MEDIUM	High
	License Number Module 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.		Motive	4 - Possible reward				Loss of integrity	3 - Minimal seriously corrupt data			
			Opportunity	7 - Some access or resources required				Loss of availability	5 - Minimal primary services interrupted, extensive secondary services interrupted			
			Group Size	9 - Anonymous Internet users				Loss of accountability	4 -			
		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	4 - Loss of major accounts			
			Awareness	9 - Public knowledge				Non-compliance	5 - Clear violation			
			Intrusion detection	8 - Logged without review				Privacy violation	3 - One individual			

Table 28 Network Threat 003

License Number	Threat#4-Data Flow Sniffing [Sniffing]	Threat Agent	Skill level	4 - Advanced computer user	6.25	HIGH	Technical Impact	Loss of confidentiality	9 - All data disclosed	5.875	MEDIUM	High
	License Number 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.		Motive	4 - Possible reward				Loss of integrity	7 - Extensive seriously corrupt data			
			Opportunity	7 - Some access or resources required				Loss of availability	7 - Extensive primary services interrupted			
			Group Size	6 - Authenticated users				Loss of accountability	7 - Possibly traceable			
		Vulnerability	Ease of discovery	7 - Easy			Business Impact	Financial damage	3 - Minor effect on annual profit			
			Ease of exploit	5 - Easy				Reputation damage	4 - Loss of major accounts			
			Awareness	9 - Public knowledge				Non-compliance	5 - Clear violation			
			Intrusion detection	8 - Logged without review				Privacy violation	5 - Hundreds of people			

Table 29 Network Threat 004

License Number	Threat#5-Potential Process Crash or Stop [DoS]	Threat Agent	Skill level	3 - Network and programming skills	6.125	HIGH	Technical Impact	Loss of confidentiality	4 - Minimal critical data disclosed, extensive non-sensitive data disclosed	4.75	MEDIUM	High
	License Number Module crashes, halts, stops or runs slowly; in all cases violating an availability metric.		Motive	4 - Possible reward				Loss of integrity	3 - Minimal seriously corrupt data			
			Opportunity	4 - Special access or resources required				Loss of availability	7 - Extensive primary services interrupted			
			Group Size	9 - Anonymous Internet users				Loss of accountability	7 - Possibly traceable			
		Vulnerability	Ease of discovery	7 - Easy			Business Impact	Financial damage	7 - Significant effect on annual profit			
			Ease of exploit	5 - Easy				Reputation damage	4 - Loss of major accounts			
			Awareness	9 - Public knowledge				Non-compliance	5 - Clear violation			
			Intrusion detection	8 - Logged without review				Privacy violation	1 -			

Table 30 Network Threat 005

16. Login Information	Threat#6-Spoofing the 1.3 Control Interface Process [Spoofing]	Threat Agent	Skill level	4 - Advanced computer user	5.375	MEDIUM	Technical Impact	Loss of confidentiality	9 - All data disclosed	6.125	HIGH	High
	1.3 Control Interface may be spoofed by an attacker and this may lead to unauthorized access to 2.2 Authentication Module. Consider using a standard authentication mechanism to identify the source process.		Motive	4 - Possible reward				Loss of integrity	7 - Extensive seriously corrupt data			
			Opportunity	5 -				Loss of availability	7 - Extensive primary services interrupted			
			Group Size	6 - Authenticated users				Loss of accountability	7 - Possibly traceable			
		Vulnerability	Ease of discovery	7 - Easy			Business Impact	Financial damage	5 -			
			Ease of exploit	3 - Difficult				Reputation damage	4 - Loss of major accounts			
			Awareness	6 - Obvious				Non-compliance	5 - Clear violation			
			Intrusion detection	8 - Logged without review				Privacy violation	5 - Hundreds of people			

Table 31 Network Threat 006

16. Login Information	Threat#7-Potential Lack of Input Validation for 2.2 Authentication Modul [Tampering]	Threat Agent	Skill level	3 - Network and programming skills	4.125	MEDIUM	Technical Impact	Loss of confidentiality	5 - Extensive critical data disclosed	4.875	MEDIUM	Medium
	Data flowing across 16. Login Information may be tampered with by an attacker. This may lead to a denial of service attack against 2.2 Authentication Module or an elevation of privilege attack against 2.2 Authentication Module or an information disclosure by 2.2 Authentication Module. 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.		Motive	4 - Possible reward				Loss of integrity	7 - Extensive seriously corrupt data			
			Opportunity	7 - Some access or resources required				Loss of availability	7 - Extensive primary services interrupted			
			Group Size	6 - Authenticated users				Loss of accountability	7 - Possibly traceable			
		Vulnerability	Ease of discovery	3 - Difficult			Business Impact	Financial damage	3 - Minor effect on annual profit			
			Ease of exploit	3 - Difficult				Reputation damage	4 - Loss of major accounts			
			Awareness	4 - Hidden				Non-compliance	5 - Clear violation			
			Intrusion detection	3 - Logged and reviewed				Privacy violation	1 -			

Table 32 Network Threat 007

16. Login Information	Threat#8-Data Flow Sniffing[Information Disclosure]	Threat Agent	Skill level	9 - No technical skills	7.25	HIGH	Technical Impact	Loss of confidentiality	5 - Extensive critical data disclosed	4.875	MEDIUM	High
	Data flowing across 16. Login Information 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..		Motive	4 - Possible reward				Loss of integrity	7 - Extensive seriously corrupt data			
			Opportunity	7 - Some access or resources required				Loss of availability	7 - Extensive primary services interrupted			
			Group Size	9 - Anonymous Internet users				Loss of accountability	7 - Possibly traceable			
		Vulnerability	Ease of discovery	7 - Easy			Business Impact	Financial damage	3 - Minor effect on annual profit			
			Ease of exploit	5 - Easy				Reputation damage	4 - Loss of major accounts			
			Awareness	9 - Public knowledge				Non-compliance	5 - Clear violation			
			Intrusion detection	8 - Logged without review				Privacy violation	1 -			

Table 33 Network Threat 008

16. Login Information	Threat#9-Potential Process Crash or Stop for 2.2 Authentication Module[Denial Of Service]	Threat Agent	Skill level	3 - Network and programming skills	5.75	MEDIUM	Technical Impact	Loss of confidentiality	0 -	3.875	MEDIUM	Medium
	2.2 Authentication Module crashes, halts, stops or runs slowly; in all cases violating an availability metric.		Motive	1 - Low or no reward				Loss of integrity	1 - Minimal slightly corrupt data			
			Opportunity	9 - No access or resources required				Loss of availability	9 - All services completely lost			
			Group Size	9 - Anonymous Internet users				Loss of accountability	9 - Completely anonymous			
		Vulnerability	Ease of discovery	7 - Easy			Business Impact	Financial damage	3 - Minor effect on annual profit			
			Ease of exploit	5 - Easy				Reputation damage	4 - Loss of major accounts			
			Awareness	9 - Public knowledge				Non-compliance	5 - Clear violation			
			Intrusion detection	3 - Logged and reviewed				Privacy violation	0 -			

Table 34Network Threat 009

16. Login Information	Threat#10-Elevation by Changing the Execution Flow in 2.2 Authentication Module[Elevation Of Privilege]	Threat Agent	Skill level	3 - Network and programming skills	4.125	MEDIUM	Technical Impact	Loss of confidentiality	9 - All data disclosed	4.75	MEDIUM	Medium
	An attacker may pass data into 2.2 Authentication Module in order to change the flow of program execution within 2.2 Authentication Module to the attacker's choosing.		Motive	4 - Possible reward				Loss of integrity	5 - Extensive slightly corrupt data			
			Opportunity	7 - Some access or resources required				Loss of availability	7 - Extensive primary services interrupted			
			Group Size	6 - Authenticated users				Loss of accountability	7 - Possibly traceable			
		Vulnerability	Ease of discovery	3 - Difficult			Business Impact	Financial damage	1 - Less than the cost to fix the vulnerability			
			Ease of exploit	3 - Difficult				Reputation damage	4 - Loss of major accounts			
			Awareness	4 - Hidden				Non-compliance	5 - Clear violation			
			Intrusion detection	3 - Logged and reviewed				Privacy violation	0 -			

Table 35 Network Threat 010

16. Login Information	Threat#11-Potential Data Repudiation by 2.2 Authentication Module[Repudiation]	Threat Agent	Skill level	9 - No technical skills	7.25	HIGH	Technical Impact	Loss of confidentiality	5 - Extensive critical data disclosed	4.875	MEDIUM	High
	2.2 Authentication Module 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.		Motive	4 - Possible reward				Loss of integrity	7 - Extensive seriously corrupt data			
			Opportunity	7 - Some access or resources required				Loss of availability	7 - Extensive primary services interrupted			
			Group Size	9 - Anonymous Internet users				Loss of accountability	7 - Possibly traceable			
		Vulnerability	Ease of discovery	7 - Easy			Business Impact	Financial damage	3 - Minor effect on annual profit			
			Ease of exploit	5 - Easy				Reputation damage	4 - Loss of major accounts			
			Awareness	9 - Public knowledge				Non-compliance	5 - Clear violation			
			Intrusion detection	8 - Logged without review				Privacy violation	1 -			

4.3 PnG Risk Assessment

4.3.1 Identify the PnG types, goals, motivations, skills

Table 36 PnG 1

PnG 1	Type	server developer
	Goal	Cause ALPR system malfunction, to ruin the Tartan's reputation
	Motivation	He is anger and want to revenge, because there are too much work, lower reward and he is finally fired
	Skill	Extensive knowledge of ALPR system, especially server side, computers, relevant programs, DB, PKI system and access to server system with administrator authority.
	Misuse case	1. Using a backdoor of server system, modify sensitive database file causing system malfunction 2. DDoS/DRDoS attack to known server's IP

Table 37 PnG 2

PnG 2	Type	License revoked driver
	Goal	Manipulating driver's license record
	Motivation	This person's license was revoked for multiple traffic violations. He wants to get his license back and drive normally.
	Skill	Trying to login with brute force
	Misuse case	1. Buying hackers or police officers with money to tamper with license records 2. Attempts to login with a brute force and succeeds in tampering with the license record

Table 38 PnG 3

PnG 3	Type	Police Officer
	Goal	Modify the plate information
	Motivation	Receive money and change plate information
	Skill	1. takeover a backdoor account accessing to Backend Server 2. repudiate that he has never accessed the backend server
	Misuse case	1.Using a second ID 2. remove audit

Table 39 PnG 4

PnG 4	Type	Hacker
	Goal	Show the anti-government slogans on the client screen.
	Motivation	He is an anarchist and hates the power of the nation.
	Skill	Code Injection, Buffer Overflow Attack, DDOS
	Misuse case	Hacker steals the system admin privilege and injects code to display slogans, then executes that code. He can also do DDOS attack.

Table 40 PnG 5

PnG 5	Type	Criminal
894512 POLICE DEPT. DATE: XX-XX-XXXX NUMBER: XXXX-XXXX dreamstime.com	**Goal**	Retrieve and tamper with traffic violation information. and it is used for crime.
	Motivation	to get financial gain
	Skill	subsumption ability and network of criminal engineers in various fields.
	Misuse case	He stole personal privacy information and used them for fraudulent crime.

Table 41 PnG 6

PnG 6	Type	System Manager
	Goal	Sneaking all information
	Motivation	Making a fortune
	Skill	Data replication using covert channel
	Misuse case	

4.3.2 Comparison with STRIDE

Indicate whether they discovered threats that did not appear with STRIDE or whether it reinforced the STRIDE results

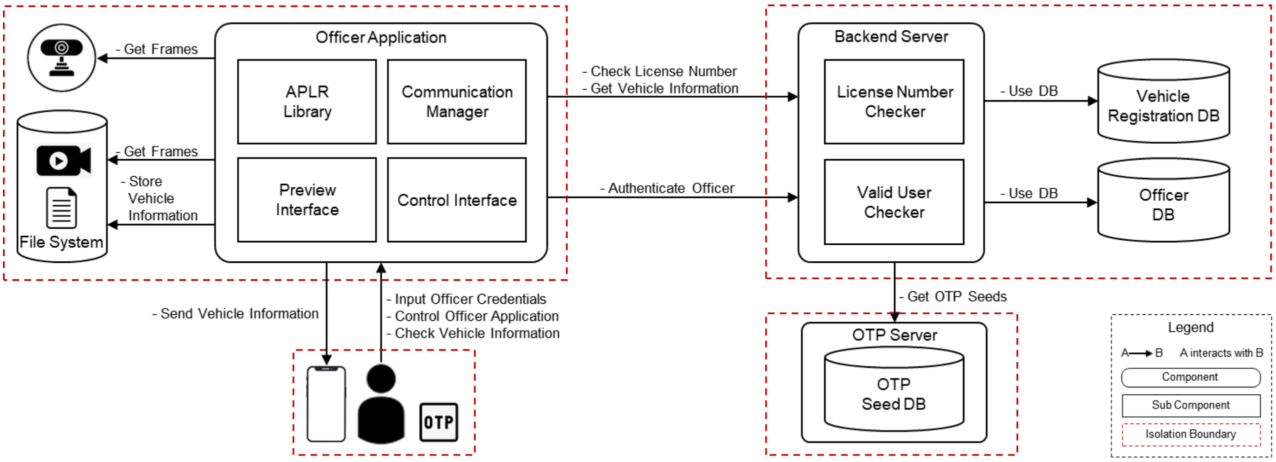
Table 42 Comparision With STRIDE

Threat		Comparison PnG
Spoofing	TID-S1, TID-S2	Similar with PnG case 4 & 5
Tampering	TID-N6 Login Information	Similar with PnG case 1 & 2 & 3 & 4
Repudiation	TID-N2, TID-N10, Repudiation User Authentication, License Number	Similar with PnG case 3
Information disclosure	TID-N3, TID-N7 User ID/PW, License Number	Similar with PnG case 4 & 5
Denial of Service	TID-S5, TID-N8, TID-N4 16. Login Information 21. Store Login Informaiton License Number	Similar with PnG case 1 & 4
Elevation of Privilege	TID-S3 TID-C8 TID-N9	Similar with PnG case 1 & 4

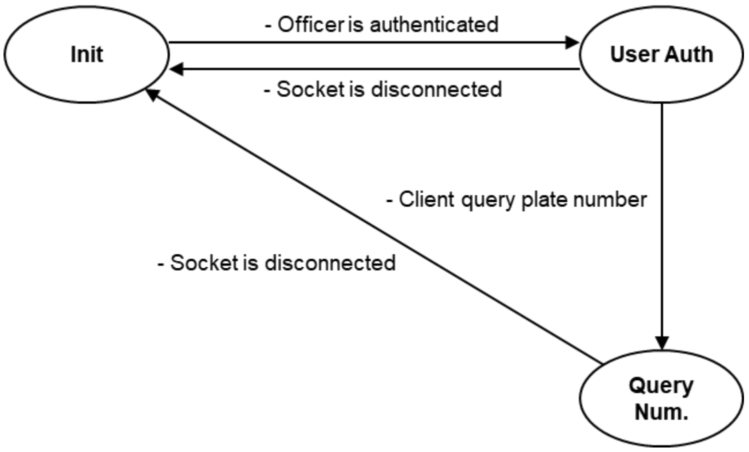
5 Architecture Design

5.1 System Architecture

5.1.1 System Context Diagram



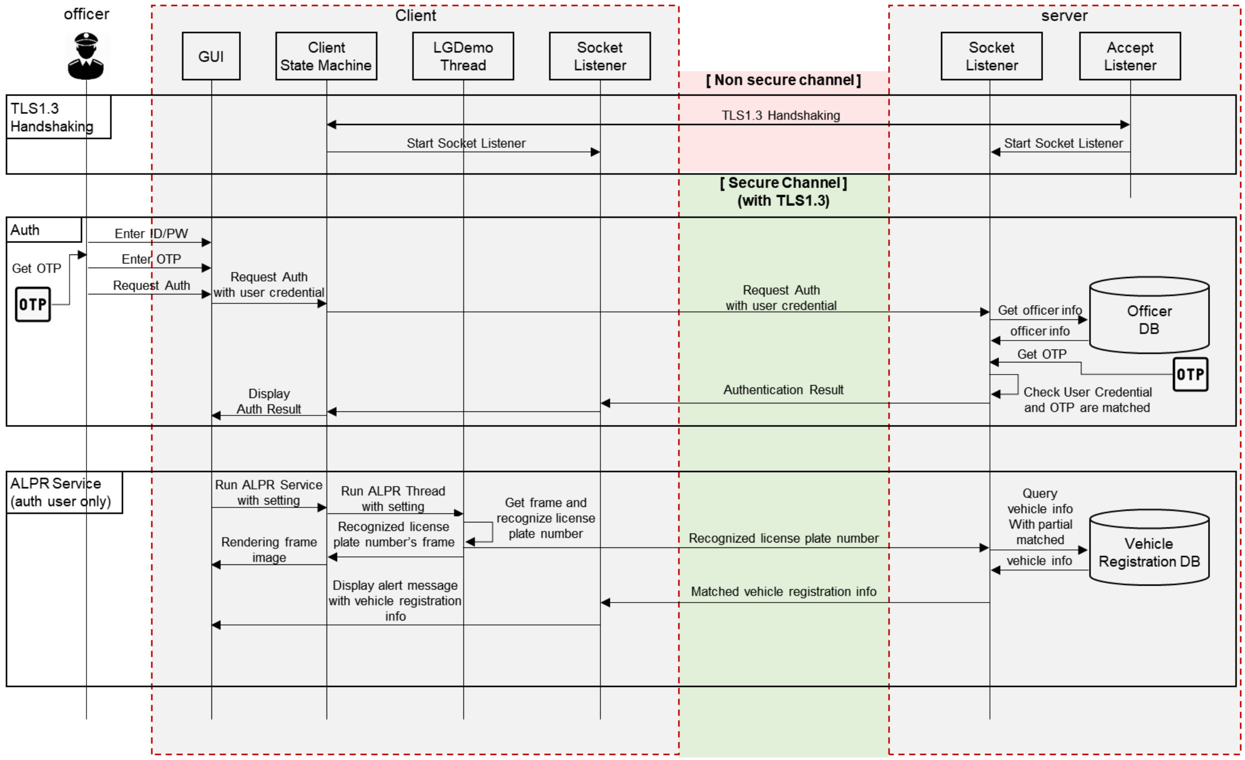
5.1.2 State Transition



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.

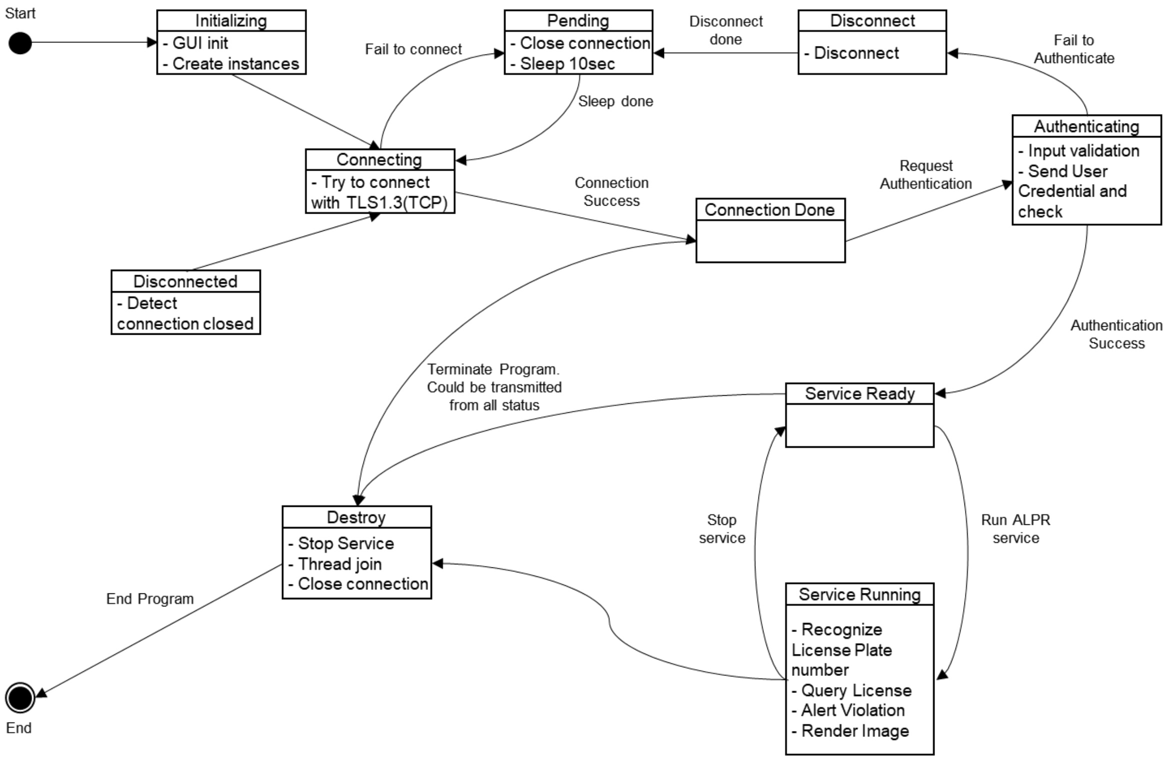
	- If connection is closed, state is switched to “Init” state

5.1.3 System Service Sequence


officer
Client
server
GUI
Client State Machine
LGDemo Thread
Socket Listener
[Non secure channel]
Socket Listener
Accept Listener
TLS1.3 Handshaking
TLS1.3 Handshaking
Start Socket Listener
Start Socket Listener
[Secure Channel] (with TLS1.3)
Auth
Get OTP
OTP
Enter ID/PW
Enter OTP
Request Auth
Request Auth with user credential
Request Auth with user credential
Get officer info
officer info
Officer DB
Get OTP
OTP
Check User Credential and OTP are matched
Authentication Result
Display Auth Result
ALPR Service (auth user only)
Run ALPR Service with setting
Run ALPR Thread with setting
Get frame and recognize license plate number
Recognized license plate number's frame
Rendering frame image
Recognized license plate number
Query vehicle info With partial matched
vehicle info
Vehicle Registration DB
Matched vehicle registration info
Display alert message with vehicle registration info

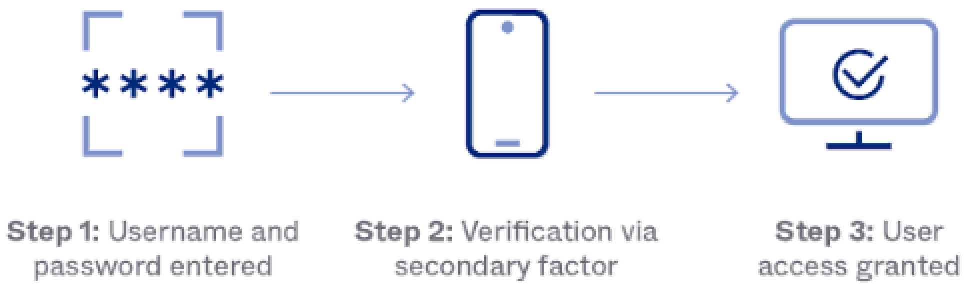
5.2 Client Architecture

5.2.1 Client State Diagram

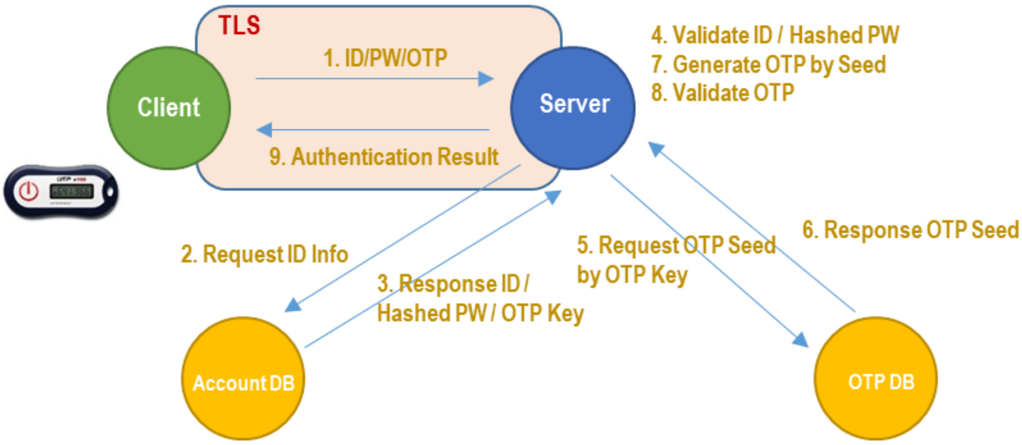


5.3 2 Factor Authentication.

5.3.1 Basic Concept


****
Step 1: Username and password entered
Step 2: Verification via secondary factor
Step 3: User access granted

5.3.2 Cross-verifies users with two different forms of identification

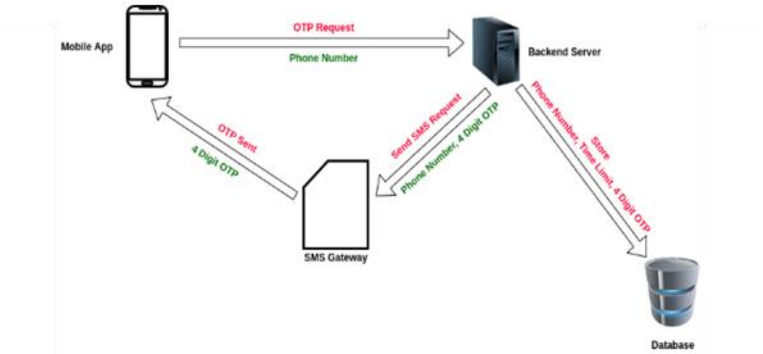


Username
LOGIN
564872
Enter Code

The user enters in their username and password.

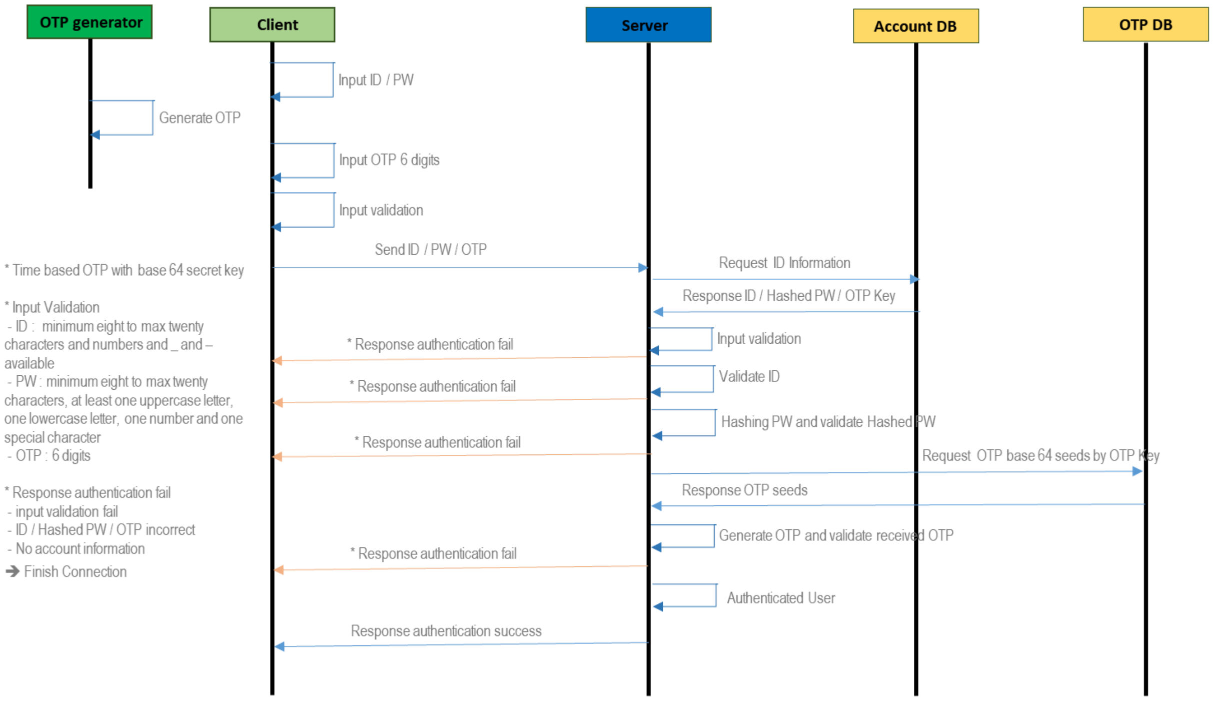
An authentication code is sent to the user's mobile device.

The user enters in their authentication code to log into the application.



5.3.3 2FA Basic Scenario

aaa

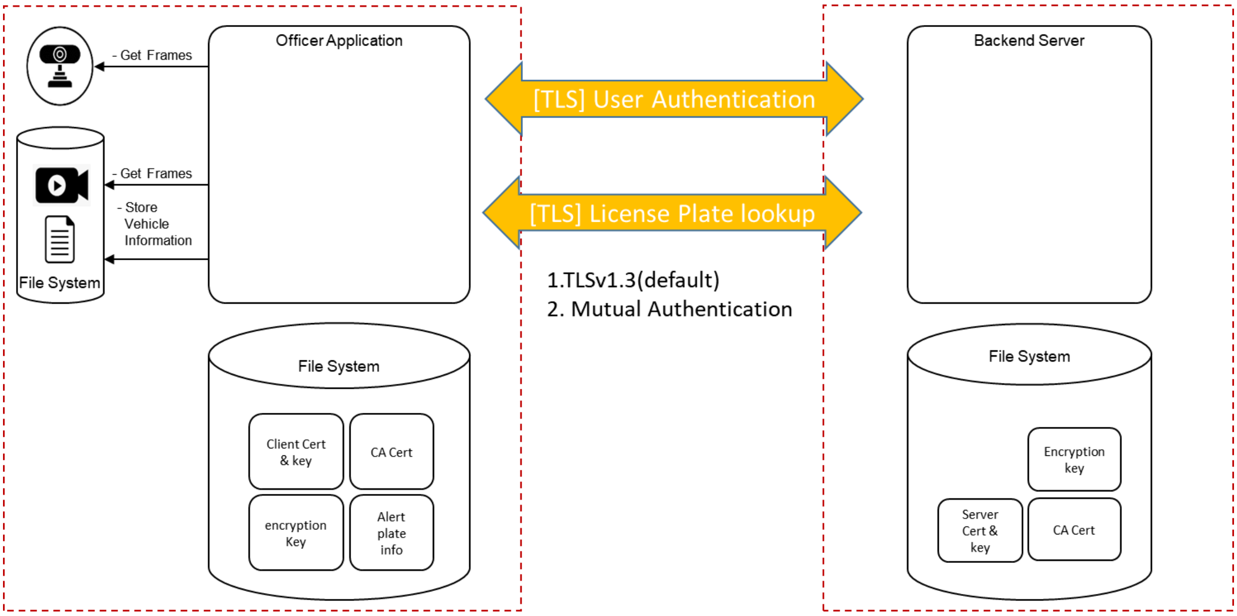

OTP generator
Client
Server
Account DB
OTP DB
Input ID / PW
Generate OTP
Input OTP 6 digits
Input validation
Send ID / PW / OTP
Request ID Information
Response ID / Hashed PW / OTP Key
Input validation
* Response authentication fail
Validate ID
* Response authentication fail
Hashing PW and validate Hashed PW
* Response authentication fail
Request OTP base 64 seeds by OTP Key
Response OTP seeds
Generate OTP and validate received OTP
* Response authentication fail
Authenticated User
Response authentication success

* Time based OTP with base 64 secret key

* Input Validation
- ID : minimum eight to max twenty characters and numbers and _ and – available
- PW : minimum eight to max twenty characters, at least one uppercase letter, one lowercase letter, one number and one special character
- OTP : 6 digits

* Response authentication fail
- input validation fail
- ID / Hashed PW / OTP incorrect
- No account information
➔ Finish Connection

5.4 TLS/SSL


- Get Frames
Officer Application
- 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(default)
2. Mutual Authentication
Backend Server
File System
Encryption key
Server Cert & key
CA Cert