2022 LG Security Specialist

ALPR Project Phase1

Team   2

Author   Woosuk Ahn

Heewon Ahn

Woosuk Jung

Hyunmin Kim

Jungsun Goh
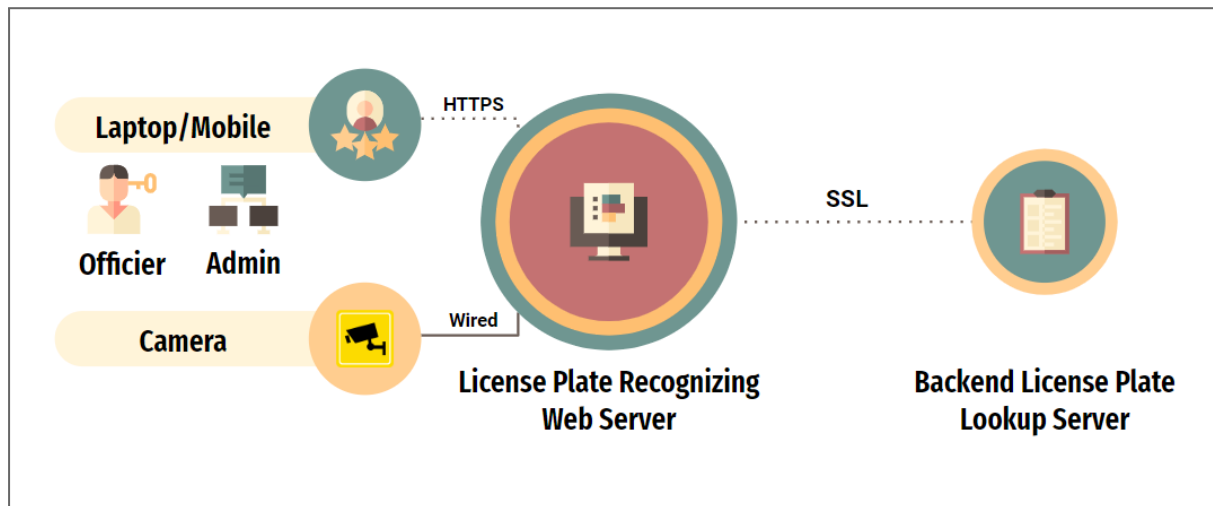
Hunjin Ha

Date   July. 5, 2022

Overview

The system is designed to support law enforcement by providing Automated License Plate Recognition Management based on a web based client-server system using OpenALPR, OpenCV. The system is split into a web server and backend license plate lookup server. And users can access the system via a secure web interface.

Figure 1. Overview of ALPR System

Team Organization

4

Member	Contact	Role & Responsibility
Woosuk Ahn	hytecahn@gmail.com	Implement UI and ALPR vehicle control and recognition system and Web
Heewon Ahn	anyone98@gmail.com	Implement the Web authentication
Woosuk Jung	alephjws@gmail.com	Implement Backend License Plate Server and DB
Hyunmin Kim	kimhm0205@gmail.com	Implement Backend License Plate Server and logging
Hunjin Ha	hjinha3@gmail.com	Implement SSL protocol
Jungsun Goh	jenna.jungsun.goh@gmail.com	Quality assurance and documentation

Table 1. Team Organization

Schedule

The project schedule is divided into two phases. In the first phase, the goal is to develop the Tartan System, and in the second phase, the target is to analyze the vulnerabilities of the Tartan System.

The first phase has been performed according to the SQUARE-based procedure. The second stage is planned as a process of analyzing the system, identifying vulnerabilities, and creating a report.

Phase	To Do	Action Item	Week 1					Week 2					Week 3				
			6/13	6/14	6/15	6/16	6/17	6/20	6/21	6/22	6/23	6/24	6/27	6/28	6/29	6/30	7/1
Phase 1	System Requirements	System Requirements analysis	▓														
	Agree of Definition	Agree of Definition		▓													
	Security Goal Identification	Asset Identification			▓												
		Security Goal Identification			▓												
	Artifact	DFD				▓											
		System Architecture				▓											
	Threat Modeling	PnG					▓										
		STRIDE					▓										
	Risk Assessment	Risk Assessment						▓									
	Security Requirement	Security Requirement							▓								
	Mitigation identification	Mitigation identification								▓							
	Implementation	Two Factor Authentication									▓	▓	▓	▓			
		TLS									▓	▓	▓				
		logging Feature											▓	▓			
		Configuration File Feature												▓	▓	▓	
		DB Encryption														▓	
	Verification	SW Feature Test														▓	▓

Phase	To Do	Action Item	Week 4					Week 5									
			7/4	7/5	7/6	7/7	7/8	7/11	7/12	7/13	7/14	7/15					
Phase 2	System Analysis	Artifact Analysis	▓														
		Source Code Analysis		▓	▓												
	Vulnerability Analysis	Vulnerability Analysis			▓	▓	▓	▓	▓	▓	▓						
		Vulnerabilit Report						▓	▓	▓	▓	▓					

Figure 2. Schedule of Project

Requirements

1. System Requirements

We analyzed the requirements in the studio project documents.
(2022 LG Security Project Description.pdf)
We have found and extracted the system requirements from the document and classified Functional Requirements and Quality Attributes.

1.1 Functional Requirements

ID	System	Description
FR-01	Server Client	The proposed system should be a client server system
FR-02	Server Client	The client application should communicate securely with a backend server that contains relevant information.
FR-03	Client	To access the ALPR system through a secure web interface
FR-04	Client	To login and authenticate users locally and to the backend license plate database lookup
FR-05	Client	Lost or compromised credentials must be handled in a reasonable way.
FR-06	Client	To select and save retrieved information locally
FR-07	Client	To send retrieved information to a mobile device
FR-08	Client	Provide secure communication between the client application and to the backend license plate database lookup system
FR-09	Client	Read images from the vehicle camera or a playback file and identify license plates for evaluation
FR-10	Client	Query the backend license plate server for details about the vehicle
FR-11	Client	Provide an area in the user interface that always contains the current camera /playback view
FR-12	Client	To choose between using a live camera and playback file in the UI

ID	System	Description
FR-13	Client	Alert officers of any communication errors or failures
FR-14	Server	Support license plate queries
FR-15	Server	Ensure secure communication with the client applications
FR-16	Server	Authenticate remote laptop users
FR-17	Server	Support multiple users
FR-18	Server	Support configurable values via a configuration file

Table 2. Functional Requirements

1.2 Quality Attributes

ID	System	Description
QA-01	Client	The system must use two factor authentication for sign on and user credentials must be protected.
QA-02	Client	Perform the ALPR function in real-time while maintaining a frame rate of at least 25fps
QA-03	Client	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
QA-04	Client	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
QA-05	Client	To display computed camera / playback frames per second, average time per frame, jitter and frame number.
QA-06	Client	The ability to detect network connectivity issues with the backend server

ID	System	Description
		within 5 seconds and automatically resolve the communication issue if possible
QA-07	Client	Fetch vehicle information in no more than 10 seconds as officers are often making queries in real time.
QA-08	Server	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.
QA-09	Server	Track the average number of queries per second for each user and overall queries per second, for all users
QA-10	Server	Track the number partial matches and no matches for each user and all users
QA-11	Common	Ensuring that all software in both applications are architected and coded to be secure and free of vulnerabilities
QA-12	Common	Conduct proper fault/error detection, recovery and reporting
QA-13	Common	Ensure the developed software adheres to the company coding standard and quality standards
QA-14	Common	Ensure the developed software is adequately tested.

Table 3. Quality Attributes

2. Agree on Definitions

We identified a bunch of terms that needed to be defined.

ID	Terms	Definition
DF-01	access control	Access control ensures that resources are only granted to those users who are entitled to them.
DF-02	access control list	A table that tells a computer operating system which access rights or explicit denials each user has to a particular system object, such as a file directory or individual file [TechTarget 05].
DF-03	artifact	The remnants of an intruder attack or incident activity. These could be software used by intruder(s), a collection of tools, malicious code, logs, files, output from tools, or the status of a system after an attack or intrusion [West-Brown 03].
DF-04	asset	A critical value that a company owns and wants to secure.
DF-05	attack	An action conducted by an adversary, the attacker, on a potential victim. A set of events that an observer believes to have information assurance consequences on some entity, the target of the attack [Ellison 03].
DF-07	authentication	The process of determining whether someone or something is, in fact, who or what it is declared to be [TechTarget 05].
DF-08	availability	The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them [Allen 99].
DF-11	buffer overflow	A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information—which has to go somewhere—can overflow into adjacent buffers, corrupting or overwriting the valid data held in them [SANS 05].
DF-12	confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes (i.e., to any unauthorized system entity) [SANS 05].
DF-13	control	An action, device, procedure, or technique that removes or reduces a vulnerability
DF-14	corruption	A threat action that undesirably alters system operation by adversely modifying system functions or data [SANS 05].

ID	Terms	Definition
DF-15	denial-of-service (DoS) attack	A form of attacking another computer or company by sending millions of requests every second, causing the network to slow down, cause errors, or shut down.
DF-16	disclosure	The dissemination of information to anyone who is not authorized to access that information [Alberts 03].
DF-17	disruption	A circumstance or event that interrupts or prevents the correct operation of system services and functions [Alberts 03].
DF-18	encryption	Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used [SANS 05].
DF-19	firewall	A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both [Webopedia 05].
DF-20	impact	The negative effect of an attack on a victim system by an attacker [Allen 99].
DF-21	incident	An adverse network event in an information system or network or the threat of the occurrence of such an event [SANS 05].
DF-22	incident handling	An action plan for dealing with intrusions, cyber theft, denial of service, fire, floods, and other security-related events [SANS 05].
DF-23	insider threat	The threat that authorized personnel of an organization will act counter to the organization's security and interest, especially for the purposes of sabotage and espionage [NIPC 02].
DF-24	integrity	For systems, the quality that a system has when it can perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation. For data, the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner [Allen 99].
DF-25	interception	Access to an asset gained by an unauthorized party [Pfleeger 03].
DF-26	interruption	An event that causes an asset of a system to be destroyed or become unavailable or unusable [Howard 97].
DF-27	intrusion	An attack on a network for the purpose of gaining access to or destroying privileged information or disrupting services to legitimate users [Ellison 03].
DF-28	liability	The responsibility of someone for damage or loss [West-Brown 03].

ID	Terms	Definition
DF-29	man-in-the-middle attack	An attack in which the attacker is able to read, and possibly modify at will, messages between two parties without letting either party know that they have been attacked. The attacker must be able to observe and intercept messages going between the two victims [Farlex 05].
DF-30	modification	Situation in which an unauthorized party not only gains access to, but tampers with an asset [Howard 97].
DF-31	non-repudiation	The goal of non-repudiation is to prove that a message has been sent and received [SSI 05].
DF-32	privacy	The quality or condition of being secluded from the presence or view of others [Dictionary.com 05].
DF-33	recovery	A system's ability to restore services after an intrusion has occurred. Recovery also contributes to a system's ability to maintain essential services during intrusion [Ellison 03].
DF-34	replay attack	The interception of communications, such as an authentication communication, and subsequent impersonation of the sender by retransmitting the intercepted communication [FFIEC 04].
DF-35	risk	The product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack [SANS 05].
DF-36	risk assessment	The process by which risks are identified and the impact of those risks determined [SANS 05].
DF-37	security policy	A policy that addresses security issues [West-Brown 03].
DF-38	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 [Webopedia 04].
DF-39	stakeholder	Anyone who is a direct user, indirect user, manager of users, senior manager, operations staff member, support (help desk) staff member, developer working on other systems that integrate or interact with the one under development, or maintenance professionals potentially affected by the development and/or deployment of a software project [Ambler 04].
DF-40	target	The object of an attack, especially host, computer, network, system, site, person, organization, nation, company, government, or other group [Allen 99].
DF-41	threat	A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm [SANS 05].

ID	Terms	Definition
DF-42	threat assessment	The identification of the types of threats that an organization might be exposed to [SANS 05].
DF-43	threat model	Used to describe a given threat and the harm it could do to a system if it has a vulnerability [SANS 05].
DF-44	trust	Determines which permissions other systems or users have and what actions they can perform on remote machines [SANS 05].
DF-45	victim	That which is the target of an attack. An entity may be a victim of either a successful or unsuccessful attack [SANS 05].
DF-46	vulnerability	A condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat [Guttman 95].

Table 4. Definitions in Project

3. Assets and Security Goals

3.1 Assets

We have found 3 types of assets in our project: PII(Personal Identifiable Information), User credential information, and System configuration.

ID	Asset	Category	Damage Scenario
AID-01	License Plate Number	PII ▾	If a license plate number is manipulated, a police officer cannot get valid information or a criminal can avoid law enforcement.
AID-02	Status	PII ▾	If queried vehicle information is manipulated, a police officer cannot get valid information or a criminal can avoid law enforcement.
AID-03	Owner Name	PII ▾	Personally identifiable information (PII) may be leaked.
AID-04	Owner Date of Birth	PII ▾	Personally identifiable information (PII) may be leaked.
AID-05	Owner Street Address/ Location	PII ▾	Personally identifiable information (PII) may be leaked.
AID-10	Owner City, State and Zip Code	PII ▾	Personally identifiable information (PII) may be leaked.
AID-06	ID	Credentials ▾	Authentication information can be leaked and an abuser can access the system maliciously.
AID-07	Password	Credentials ▾	Authentication information can be leaked and an abuser can access the system maliciously.
AID-08	Configuration File	Configure ▾	If a configuration file is manipulated, a police officer cannot get valid information or a criminal can avoid law enforcement.
AID-09	Log file	Configure ▾	If a log file is manipulated, the server cannot provide access and query information, so the system cannot avoid non-repudiation.

Table 5. Recognized Assets

3.2 Excluded from Assets

We excluded the following data from Assets from the requirements.

No Asset	Category	Damage Scenario	Asset ID
Registration Expiration	No Damage ▾	-	-
Vehicle Year of Manufacture	No Damage ▾	-	-
Vehicle Make	No Damage ▾	-	-
Vehicle Model	No Damage ▾	-	-
Vehicle Color	No Damage ▾	-	-
Owner City, State and Zip Code	No Damage ▾	-	-

Table 6. List excluded from Assets

Key:

PII ▾   Personal Identifiable Information

Credentials ▾   Credential Information

Configure ▾   System Configuration

No Damage ▾   No Assets for Security

3.3 Security Goal

The client application should communicate securely with a backend server that contains relevant information.

3.4 Security Sub-Goals

1. A law enforcement officer shall securely control over the system's database and usages. (**Confidentiality, Integrity**)
2. The identity of the person accessing the data and resources of the system are verified before allowing access. (**Authentication**)
3. Admin shall access and modify a configuration file (**Authorization**)
4. A law enforcement officer shall use the system in real time at any time he or she wants. (**Availability**)

4. Artifacts

We have analyzed threats using Microsoft Threat Modeling Tool. We have attached the tm7 file into the document repository.

4.1 Data Flow Diagram (Between User and Web Server)
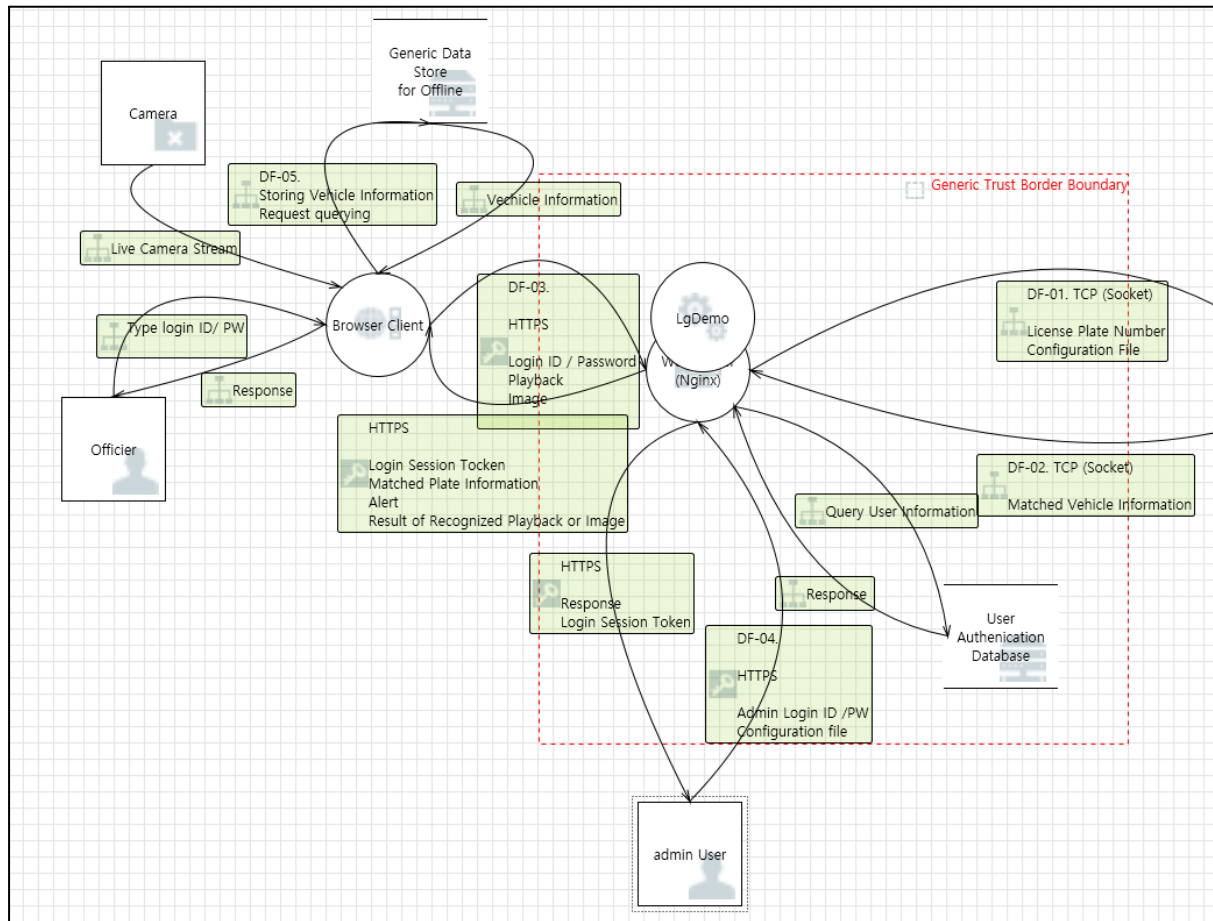
Figure 3. DFD (User and Web Server)

4.2 Data Flow Diagram (Between Web Server and Lookup Server)
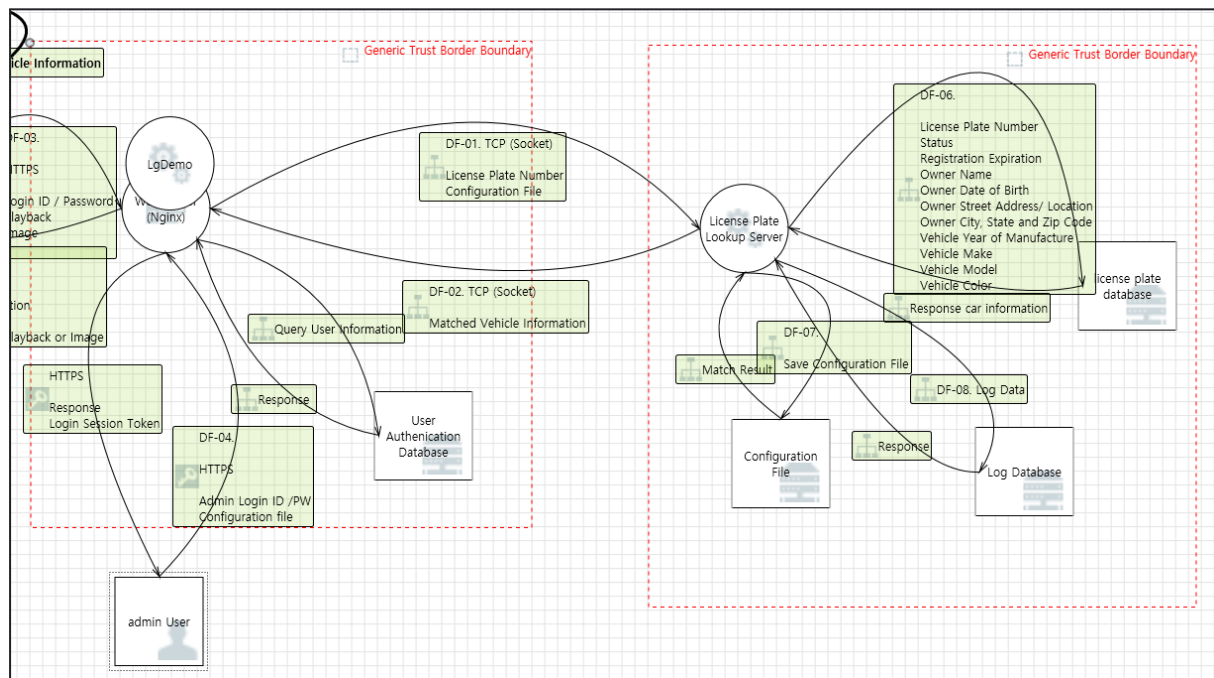
Figure 4. DFD (Web Server and Lookup Server)

5. Threat Modeling
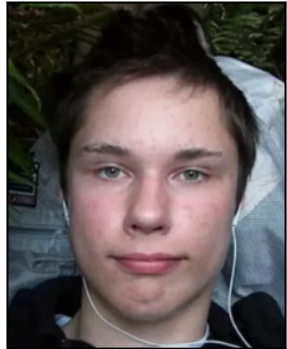
5.1 Persona and Granada

Definition of PnG Types

Disgruntled Employee	*Employees who are dissatisfied with the company can access and abuse the Tartan System with a malicious intent.*
Hostile Country	*A hostile country can acquire and misuse the other country's personal and vehicle information.*
White Hacker	*To strengthen the security of the Tartan system, a white hacker was hired to analyze and improve the vulnerability.*
Criminal	*Criminals or criminal organizations can steal vehicle information and use it for crimes.*

Table 7. Definition of PnG types

Criminals

Type	**PID-01:** Criminal	
Goals	To break into(invade) the millionaire's house and steal his wealth.	
Motivations	Moore is a professional thief and robber. He is looking for as many targets as possible. He is looking for the millionaires whose house has the automatic recognition plate number system to enter. He wants to get the car plate number and car information for the millionaire's houses to get into the millionaire's house garage. He is secretly looking at the police officer's id and password when he is typing and after he steals the officer's mobile and checks the locally saved information in the mobile device or sends license information to the server and gets the address information. After all, he can copy the plate number to get into the target(millionaire)'s garage and then he can steal or rob the millionaire's house.	**Colton Harris Moore**
Skills	He has fast hands. He has a lot of experience about stealing and robbing.	
Misuse Cases	1. Secretly looking at the officer's id and password 2. Steal a mobile device from a policeman 3. Get the locally saved plate and personal information in a mobile device. 4. Get the personal information from the server.	

Table 8. PnG Analysis (Criminal)

Disgruntled Employees

Type	PID-02: Disgruntled Employee	
Motivations	Dan is a retired police officer. He wants to know about a luxury car in the neighborhood where he lives and wants to know information about this car and the owner's information. He knows that his credential is not expired, and he can access the Tartan ALPR system.	
Goals	To retrieve specific vehicle information (include owner, and address)	**Daniel Plakosh**
Skills	He knows how the ALPR system works.	
Misuse Cases	1. Take a picture of the car of interest with the license plate visible. 2. Access Tartan ALPR System with a credential. 3. Upload picture taken by his personal phone, and wait to get vehicle information 4. Get the name of the owner and address.	

Table 9. PnG Analysis (Disgruntled Employee)

Hackers

Type	PID-03: Hacker	
Motivations	He is a champion of '2022 world CTF'. And Tartan requested him pentesting against their new ALPR system.	
Goals	To accomplish personal data without detection. To cause discomfort to connect the ALPR system.	
Skills	He has good Code and Hacking skills He knows whole ALPR System architectures	**Jeffrey Gennari**
Misuse Cases	1. Steal a mobile device from a policeman and disable alerts. 2. Intercept alert messages and change the message to a normal message. 3. Intercept response messages and restore another place and send the abnormal messages to a police officer.	

Table 10. PnG Analysis (Hacker)

18

Hostile Country

Type	**PID-04:** Hostile Country	
Motivations	Vladimir is the leader of a secret Russian organization. His organization needs several vehicles to complete its mission. So they plan to take over the vehicle they need. In order to freely use the stolen vehicle, Vladimir must hack the Tartan ALPR system and then manipulate the vehicle DB information.	
Goals	To manipulate the vehicle DB information (e.g. state : stolen → normal)	**Владимир (Vladimir)**
Skills	His organization has professional network experts and hackers. His organization has a variety of specialized equipment and financial resources.	
Misuse Cases	1. Steal the vehicles he needs. 2. Network experts and hackers of Russian secret organizations analyze the system and access the DB. 3. Access the DB and change the stolen vehicle information. (from stolen vehicle to normal vehicle) 4. Deletes traces of DB modifications from the log.	

Table 11. PnG Analysis (Hostile Country)

5.2 STRIDE

We've identified the following threats through the EoP(Elevation of Privilege) game.

ID	Threat Category	Assets	DFD Element	Threat Description
TID-01	**S**poofing	AID-06 AID-07	DF-03 DF-04	An attacker can try to access the web server by getting ID/PW.
TID-02	**T**ampering	AID-01 AID-02 AID-03 AID-04 AID-05 AID-10	DF-01 DF-02	An attacker can manipulate the plate number requested or responded by reading and modifying the transmitted data.
TID-03	**I**nformation Disclosure & **E**levation of Privilege	AID-01 AID-02 AID-03 AID-04 AID-05 AID-10	DF-05, DF-06, DF-07,DF-08	After the attacker obtains the server's authority using Elevation of Privilege, he may access the database and read the valuable information.
TID-04	**D**enial of Service	AID-08 AID-09	License Plate Lookup Server	The attacker sends a lot of requests to the Lookup server very quickly and makes the service not available.

Table 12. Mapping with Threat and Assets

5.3 Comparison of STRIDE and PnG

We confirmed that any single TMM is not enough to find out valid threats. Therefore, we need to apply several TMM methods together. This approach is called as hTMM.

STRIDE	Description	PnG	Validation
Spoofing	*[TID-01]* An attacker can try to access the web server by getting an ID/PW.	*[PID-01] Criminal* - [TID-05] : An attacker gets an account by sneaking across the officer's shoulders.	Missed in STRIDE ▾
		[PID-02] Disgruntled Employee - [TID-07] : An attacker can access the server with an not expired credential.	Missed in STRIDE ▾
Tampering	*[TID-02]* An attacker can manipulate the plate number requested or responded by reading and modifying the transmitted data.	*[PID-03] Hacker* - Similar with [TID-02]	Valid ▾
		[PID-04] Hostile Country - [TID-08] : An attacker can modify the sensitive information in DB.	Missed in STRIDE ▾
Repudiation	*No STRIDE cases*	*[PID-04] Hostile Country* - [TID-06] An attacker can erase traces of DB modifications from the log.	Missed in STRIDE ▾
Information Disclosure	[TID-03] After the attacker obtains the server's authority using Elevation of Privilege, he may access the database and read the valuable information.	*[PID-02] Disgruntled Employee* - Similar with [TID-03]	Valid ▾
		[PID-04] Hostile Country - Similar with [TID-03]	Valid ▾
Denial of Service	[TID-04] The attacker sends a lot of requests to the Lookup server very quickly and makes the service not available.	*No PnG cases*	Missed in PnG ▾
Elevation of Privilege	Same as [TID-03]	*No PnG cases*	Missed in PnG ▾

Table 13. Comparison PnG and STRIDE

21

6. Risk Assessment

A Risk Assessment was created based on the OWASP Risk Rating Methodology. For details, refer to "Risk Assessment.xlsx".

For more information on the OWASP Risk Rating Methodology approach, please see the link below. (https://owasp.org/www-community/OWASP_Risk_Rating_Methodology#references)

TID	TID Description	Related Asset	Likelihood						Impact						Overall Risk Severity
			Estimation Factor	Factor	Range	Score	Total Score	Severity	Estimation Factor	Factor	Range	Score	Total Score	Severity	
[TID-01]	An attacker can try to access the …	AID-06 AID-07	Threat Agent Factor	Skill Level	No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9)	1	6.375	HIGH	Technical Impact Factors	Loss of Confidentiality	Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)	7	6.25	HIGH	CRITICAL
				Motive	Low or no reward (1), possible reward (4), high reward (9)	4				Loss of Integrity	Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)	7			
				Opportunity	Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)	9				Loss of Availability	Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)	9			
				Size	Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous internet users (9)	9				Loss of Accountability	Fully traceable (1), possibly traceable (7), completely anonymous (9)	7			
			Vulnerability Factor	Ease of Discovery	Practically impossible (1), difficult (3), easy (7), automated tools available (9)	9			Business Impact Factors	Financial damage	Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)	2			
				Ease of Exploit	Theoretical (1), difficult (3), easy (5), automated tools available (9)	9				Reputation damage	Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)	4			
				Awareness	Unknown (1), hidden (4), obvious (6), public knowledge (9)	9				Non-compliance	Minor violation (2), clear violation (5), high profile violation (7)	7			
				Intrusion Detection	Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)	1				Privacy violation	One individual (3), hundreds of people (5), thousands of people (7), millions of people (9)	7			
[TID-02]	An attacker can manipulate the …	AID-01 AID-02 AID-03 AID-04 AID-05	Threat Agent Factor	Skill Level	No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9)	3	6.875	MEDIUM	Technical Impact Factors	Loss of Confidentiality	Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)	7	5.5	MEDIUM	MEDIUM
				Motive	Low or no reward (1), possible reward (4), high reward (9)	4				Loss of Integrity	Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt (9)	7			
				Opportunity	Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)	7				Loss of Availability	Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), …	1			
				Size	Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6)	9				Loss of Accountability	Fully traceable (1), possibly traceable (7), completely anonymous (9)	9			

Figure 9. Risk Assessment

7. Security Requirements

We have derived the security requirement through the PnG and STRIDE methodology.

ID	Requirement	Mitigation ID
SR-01	The system shall allow an officer to access the ALPR system through a secure web interface by two factor authentication.	MI-01-1 MI-01-2
SR-02	The system should provide secure communication between the client application and to the backend license plate database lookup system.	MI-02
SR-03	The system shall grant the admin user to access and modify configuration files.	MI-03
SR-04	The Plate DB must be encrypted data	MI-04
SR-05	The system save queries of plate number and vehicle information as a protected log and use as proof of non-repudiation	MI-05
SR-06	Terminate unwanted connections or services on the servers and routers.	MI-06

Table 14. Security Requirement and Mapping with Mitigation ID

23

8. Mitigation

ID	Mitigation	SR-ID
MI-01-1	The interface between browser and web server should be secure web interface ● Using https for encrypting interface data. ● certification should be signed by CA. ● The algorithm for rsa should be more than 2048 bit. ● symmetric key algorithm should be use more than aes 256 ● sha hash algorithm should be more than sha-256	SR-01
MI-01-2	The user accounts login should be two factor authentication. ● Even if the user id and password are exposed we need extra level of protection to user accounts. ● Another authentication factor can be added in case the registered device is stolen. ● 1.userid/password 2. registered device 3. biometric verification ● DUO is one of the solutions to be satisfied.	SR-01
MI-02	Secure communication between the client application and to the backend license plate database lookup system ● Secure communication using TLS 1.3 ● When using TLS 1.3, use a key with a length of at least 2048 bits for an asymmetric algorithm, and use a key with a length of at least 256 bits for a symmetric algorithm ● The client application verifies the server certificate before connecting to the server.	SR-02
MI-03	The administrator can access and modify the configuration file. ● The administrator can access the configuration file and change values of the Max Client User and the Minimum Confidence Threshold for partial matching. ● The administrator can change the values of the configuration file through the web access.	SR-03
MI-04	The Plate DB must be encrypted data. ● The information of vehicles are encrypted and stored in the license plate DB. ● Berkeley DB optionally supports encryption using the Rijndael/AES algorithm.	SR-04
MI-05	The queries of plate number and vehicle information as a protected log ● Do not expose the vehicle information. Only the plate number logging.	SR-05
MI-06	Terminated unwanted communication ● Only some client(Max client) able to connect the lookup server to protect Memory overflow	SR-06

Table 15. Mitigation List

Security Design

1. Two Factor Authentication

2-Factor Authentication is implemented. First, user id and password is authenticated. Second, we use the DUO solution for the 2-Factor Authentication. And the Duo server is checking the registered device and additional biometric verification. The Duo has an auto-locked function. If DUO authentication attempts fail 5 times in a row, the Duo authentication is locked for 5 minutes.
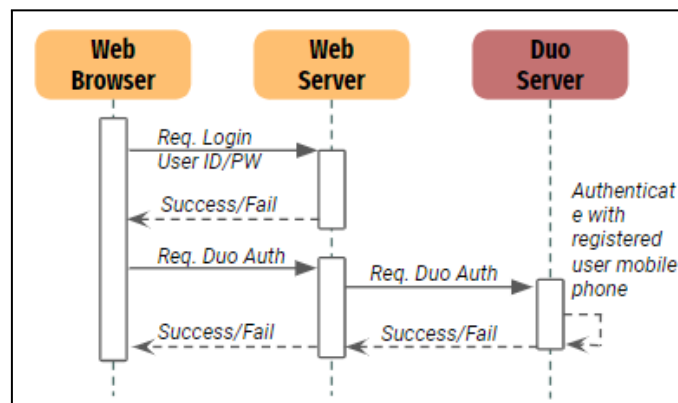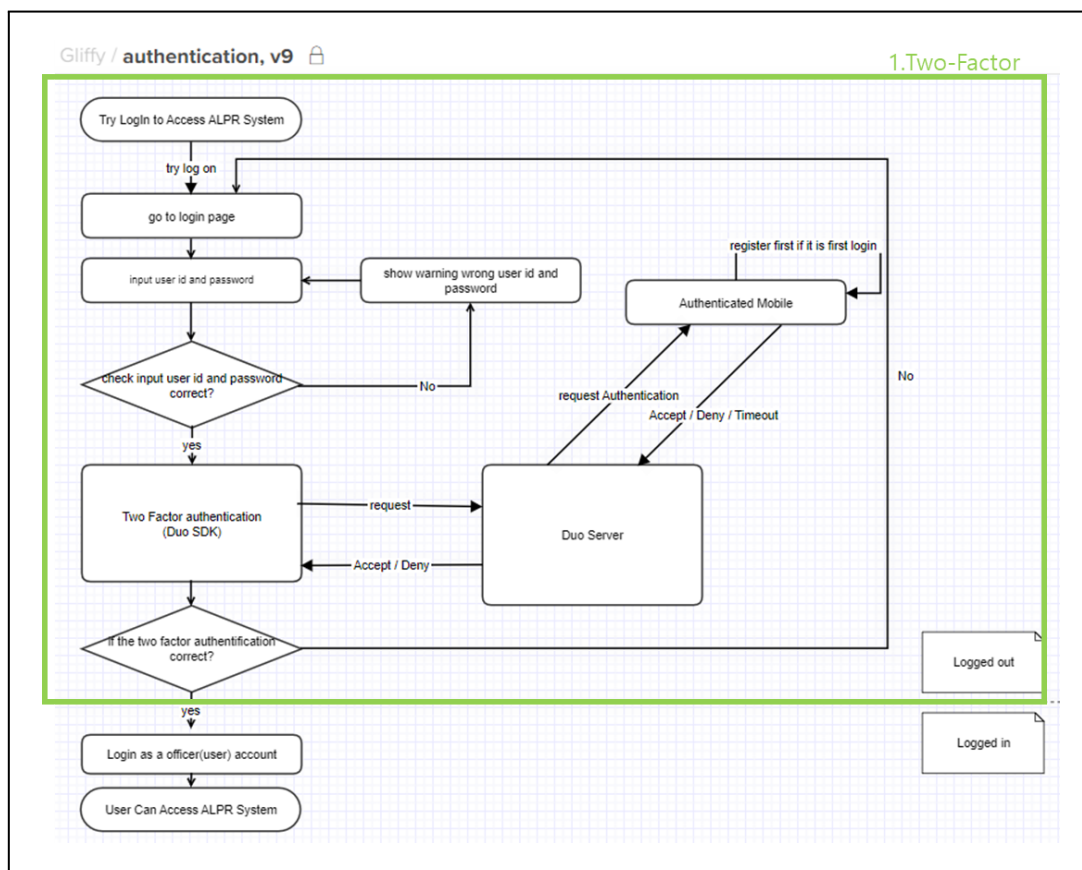

Figure 10. Two factor authentication

Figure 11. Flow chart of authentication

2. Database Encryption

The information of vehicles used in Lookup Server are encrypted and stored in the license plate DB. The license plate DB uses Berkley DB, Berkeley DB optionally supports encryption using the Rijndael/AES (also known as the Advanced Encryption Standard and Federal Information Processing Standard (FIPS) 197) algorithm for encryption or decryption.

https://docs.oracle.com/cd/E17275_01/html/programmer_reference/env_encrypt.html
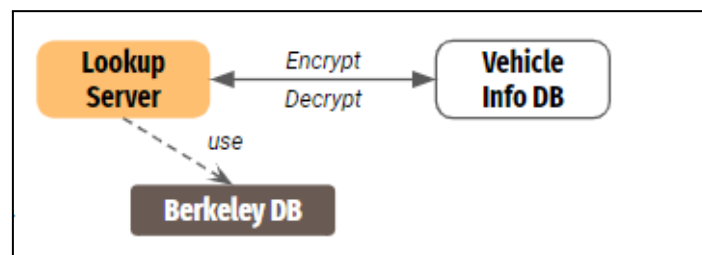
Figure 12. Vehicle Information Database Encryption

3. Data Logging

When the Lookup server receives a plate number message from the client,it requests the number of query with history to vehicle information DB. The Vehicle information DB responds to the message and the lookup server checks information of the matched plate number. If a matched plate number is available, the lookup server stored the logging data which are query information and plate number. The logging library name is Plog, which is an open source library.
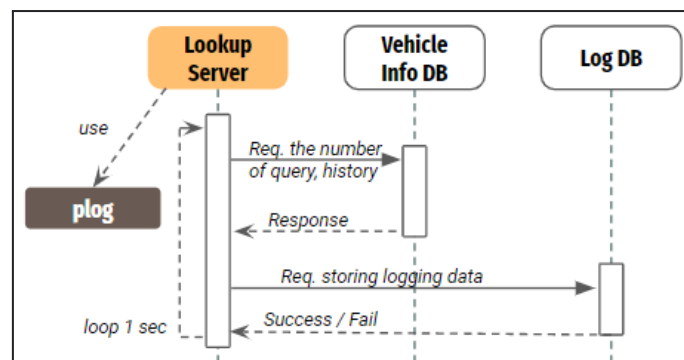
Figure 13. Data Logging for Non-repudiation

4. HTTPS Communication

The Webserver HTTPS is implemented by django-sslserver. The browser already supports HTTPS, but we need to register a certificate to the browser. The browser registers "ahnlab2-rootca.crt" as a trusted CA(rsa-2048 aes256) and "ahnlab2.com.crt"(sha256 rsa-2048 aes256) as a trusted publisher. "ahnlab2-rootca.crt" is a self signed certificate. "ahnlab2.com.crt" (sha256 rsa-2048 aes256) is certified by "ahnlab2-rootca". The domain name should be "ahnlab2.lge.com" and if we don't use this domain, the browser doesn't trust the HTTPS connection.

Figure 14. HTTPS Communications
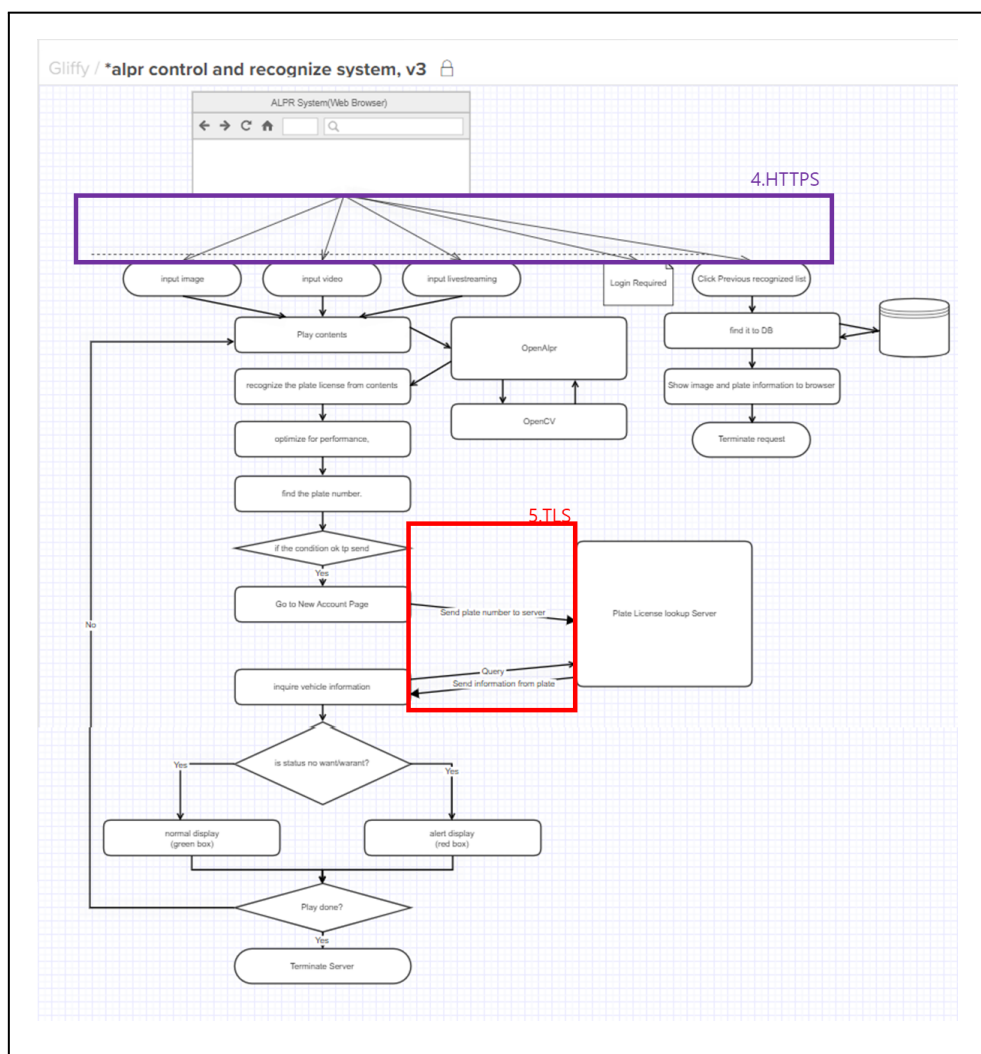
Figure 15. Flow chart of HTTPS Communication

5. Secure Channel between Web Server and Lookup Server

When the system and the query server communicate, they communicate using TLS1.3. The server sends a certificate to the system, and the system uses the RootCA to verify the server's certificate. If the server's certificate is a verified certificate, encrypted communication begins after establishing a secure session.
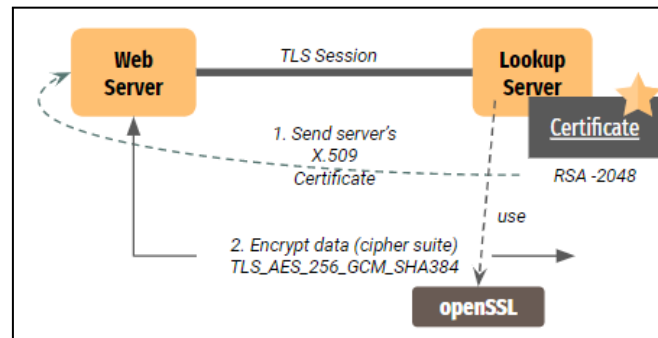
Figure 16. SSL Communication
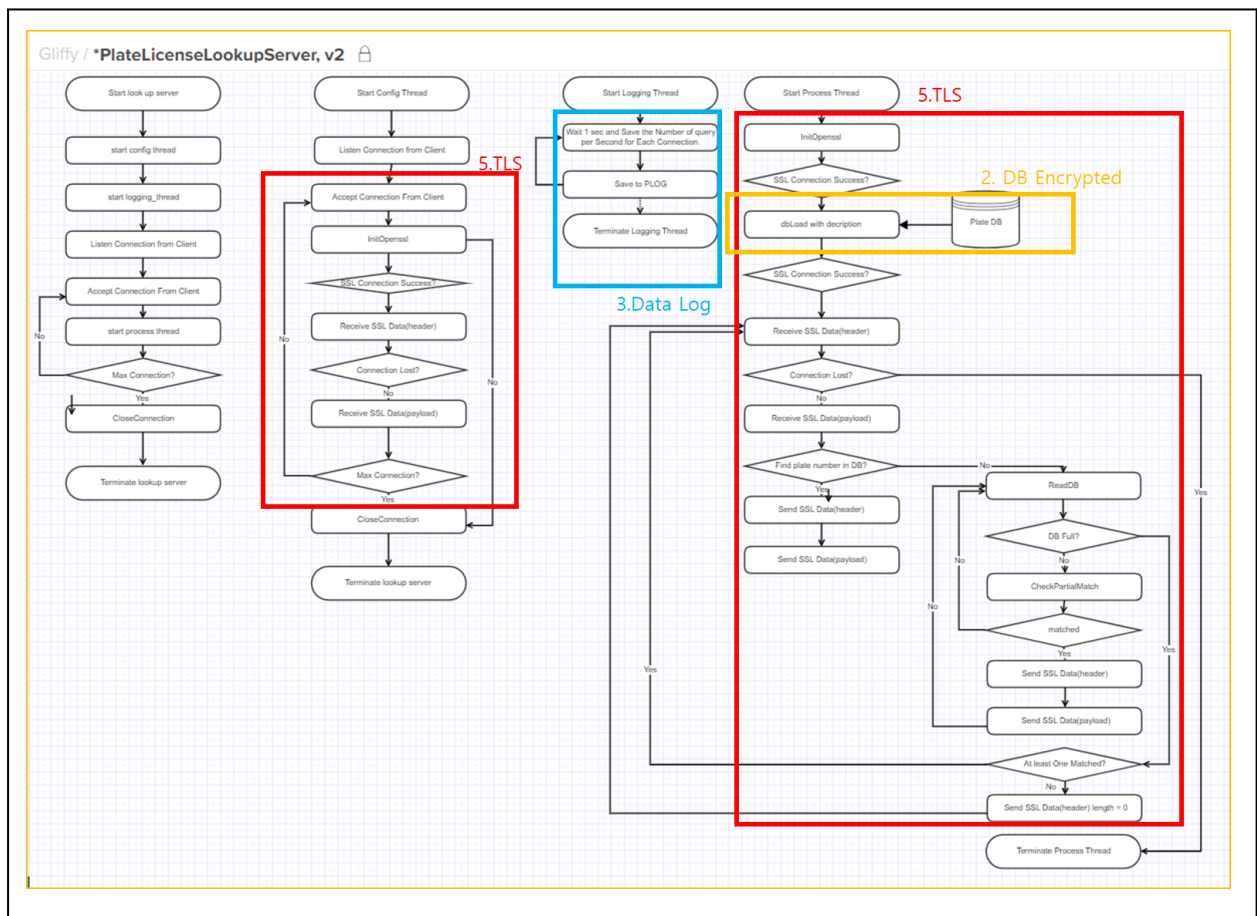
Figure 17. Flow chart of SSL communication

Implementation

Source Tree

1. **Web Server**
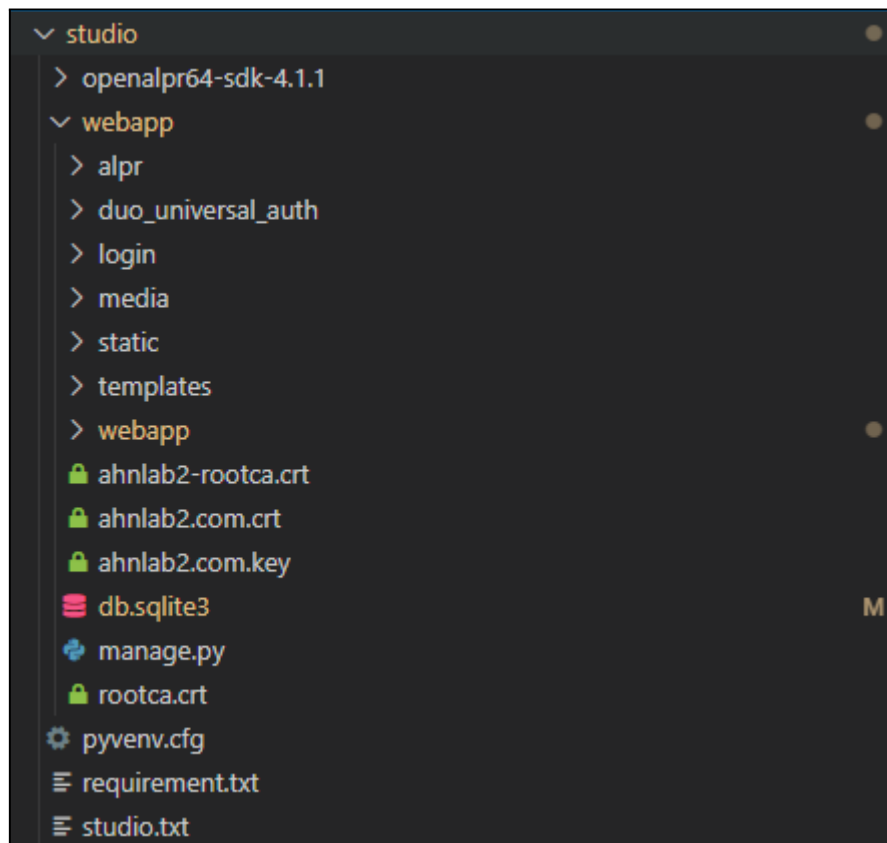
Figure 18. Web Server Source Tree

2. DB Lookup Server
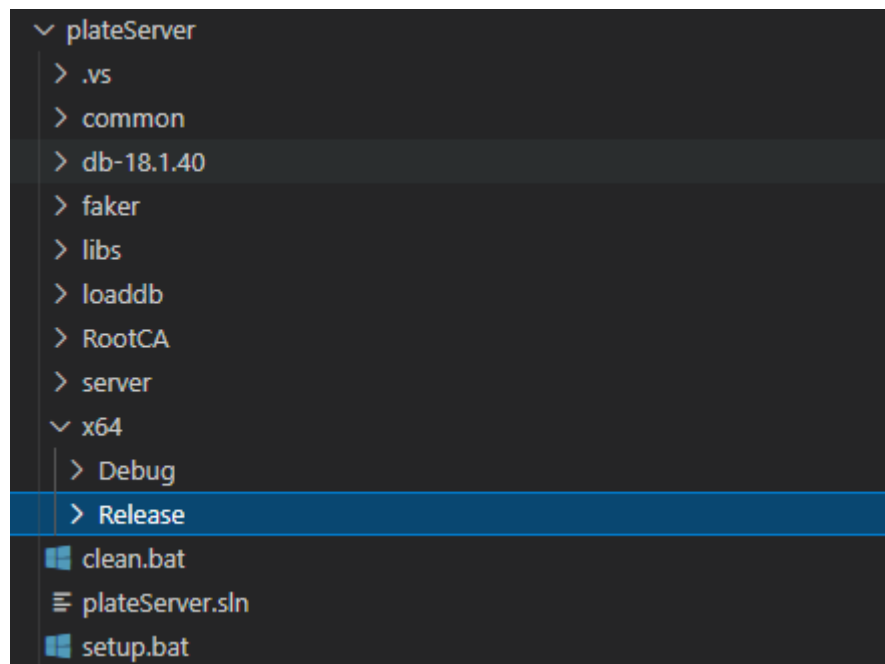
Figure 19. DB Lookup Server Source Tree

Dependency

Backend Lookup Server

For backend lookup server implementation, we used the open source components below. We mainly listed the primary top level components and please refer to the Software Composition Analysis section for details.

openssl	v3.0.3
BerkeleyDB	v18.1.40
plog	v1.1.6

Figure 20. main dependency of lookup server

Client Web Server

For client web server implementation, we used the open source components below. We mainly listed the primary top level components and please refer to the Software Composition Analysis section for details.

Django	v4.0.5
django-sslserver	v0.22
django-duo-universal	v2.0.1
PyJWT	v2.4.0
openalpr-python	v4.1.1
pyOpenSSL	v22.0.0

Figure 21. main dependency of Client Web Server

Test

1. Test Plans

We setup the test plans considering the following basic quality concerns:

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

2. Conduct proper fault/error detection, recovery and reporting.

3. Ensure the developed software adheres to the company coding standard and quality standards.

4. Ensure the developed software is adequately tested.

We developed with dependencies on numerous open sources. We will identify flaws and security vulnerabilities in open source and consider the SCRM plan, but improvements such as bug-fixes are only planned for the code developed by us.

1.1 Test Strategy

Activities	Description	Phase
Static Analysis	Analyze source codes periodically to detect potential SW defects, vulnerabilities and company coding standard violations. *Tool: Coverity 2022.03, Sonarcloud*	Implementation
Software Composition Analysis	Analyze open sources to discover known security vulnerabilities, and make mitigation or mitigation plans for those vulnerabilities. *Tool : FOSSID, OWASP dependency-check experimental analyzer*	Implementation
Testing	SW Integration & System testing is done to ensure compliance with the system and security requirements based on test cases.	Test

Table 16. Test Strategy

1.2 Pass Criteria

Activities	Criteria
Static Analysis	Number of High Impact Defects and Vulnerabilities is zero
Software Composition Analysis	Software Composition & SCRM Plan is created.
Testing	All test cases are passed.

Table 17. Pass Criteria

2. Static Analysis

To identify vulnerabilities and defects of the given software by CMU, we've run static analysis on that. And we could find there are lots of vulnerabilities especially in open source components.

2.1 Vulnerabilities on the given ALPR software
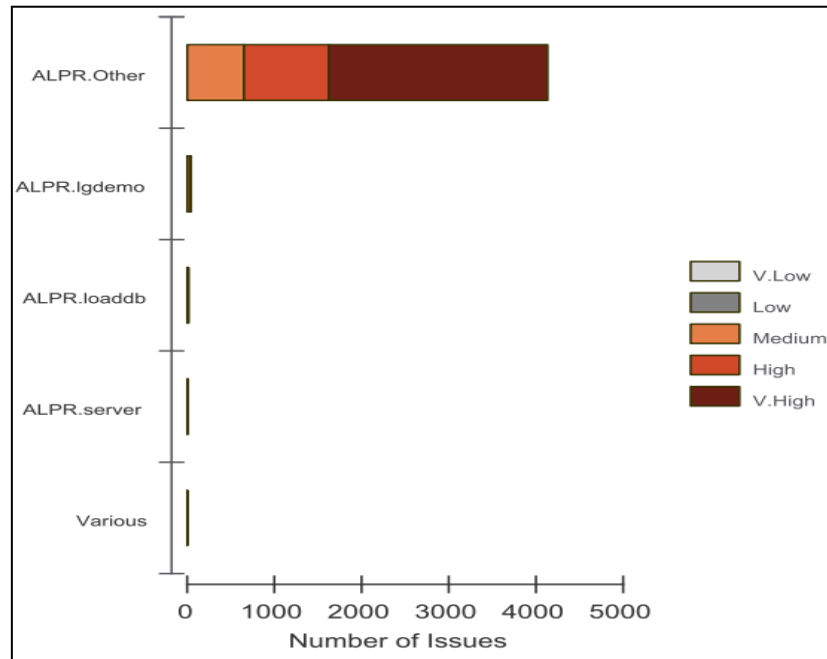
Figure 22. Severity by Component

A total of 4,201 security issues were found. Each issue was given a severity based on the severity mapping. The chart shows the number of occurrences of each of the six severity values. We found that most of the issues are detected in 'Other' components which we have designated to the open source components in advance.

Impact	Severity	Number of Issues
Execute unauthorized code	Very high	2,491
Gain privileges	Very high	22
Bypass protection mechanism	High	1,015
Modify data	High	20
Denial of service, Resource consumption	Medium	623
Read data	Medium	30

Table 18. Impact, Severity, and Number of Issues on the given ALPR

33

To comply with the 'client web interface' requirement, we've decided to replace the client C++ application 'lgdemo' with the python web application. Therefore, we don't give any considerations anymore on the initial identification of vulnerabilities on the given software.

2.2 Vulnerabilities on the new ALPR software

We've applied one of the most powerful static analysis tools, 'Coverity' and enabled the CERT C++ coding standard, CWE Top25, OWASP Top10 and other useful security checkers.
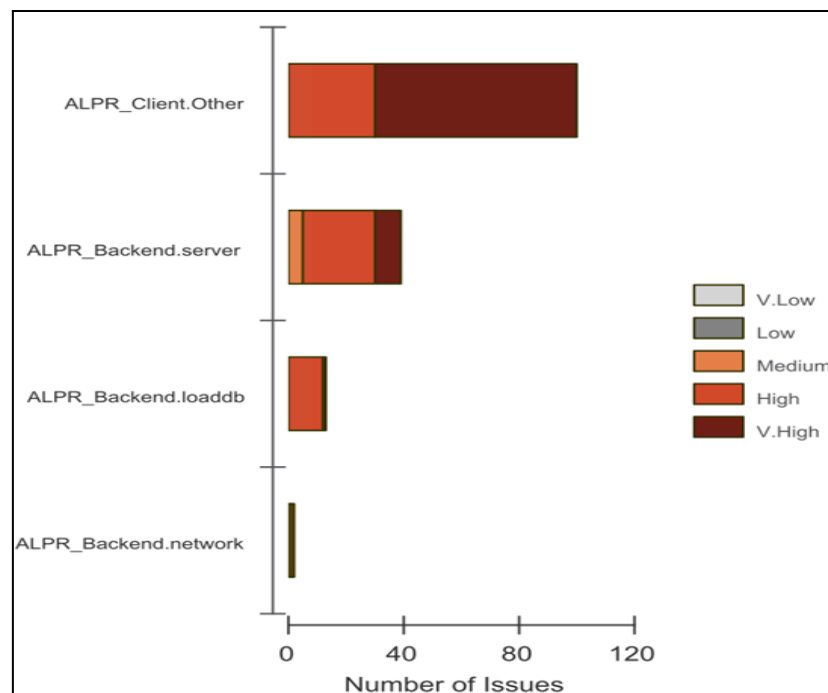
Figure 23. Severity by Component

A total of 154 security issues were found. Each issue was given a severity based on the severity mapping. The chart shows the number of occurrences of each of the six severity values.

Compared to the given source code, vulnerabilities of backend server and loaddb have increased.

In the case of client web servers, Coverity showed relatively lower detection capability in python compared to C++. We found only 112 vulnerabilities in the client side's open source and couldn't find any vulnerabilities in our proprietary python code. Since we replaced C++ client app with the python web server, we have lots of python open source dependencies. So, we were concerned that the client web server would have a lot of false negatives.

Impact	Severity	Number of Issues
Execute unauthorized code	Very high	80
Gain privileges	Very high	0
Bypass protection mechanism	High	0
Modify data	High	2
Denial of service, Resource consumption	Medium	4
Read data	Medium	2

Table 19. Impact, Severity, and Number of Issues on the new ALPR

To improve detection capability for the client web server based on python and check the vulnerabilities continuously, we've applied the sonarcloud to the client web application server. With sonar-scanner, we newly found 3 vulnerabilities and 62 code smells in web app.
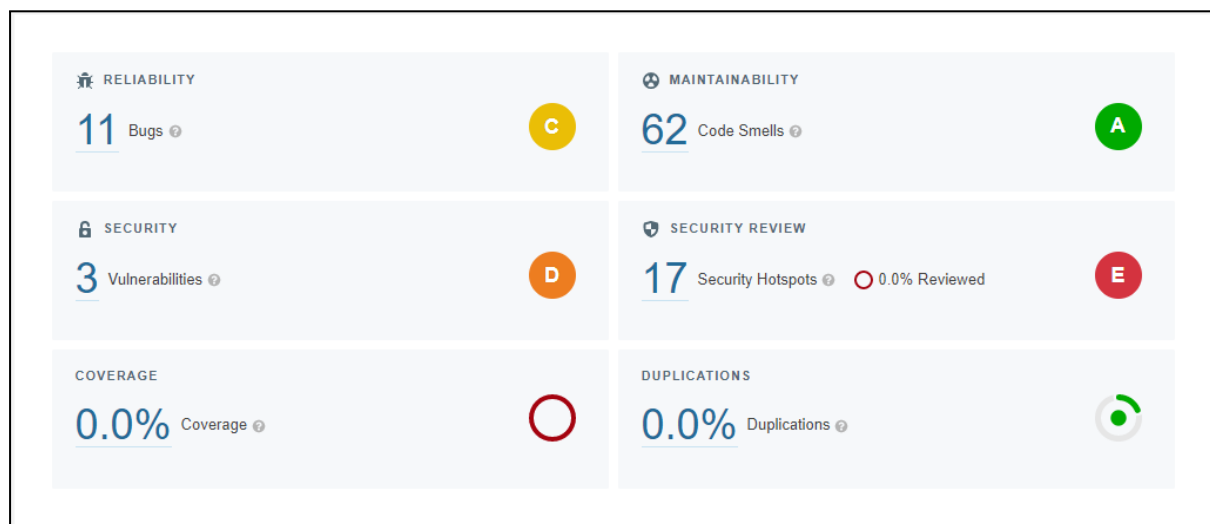
Figure 24. Sonar-Scanner Result Summary

You can see all the issues in the "documents/test/static analysis" directory.

3. Software Composition Analysis

To identify open source components we've used, we tried to apply the experimental analyzer of OWASP dependency-check for C++ and python. But the experimental analyzer provides limited results and we cannot get meaningful results from the result.

3.1 OWASP dependency-check result on Client Web server

Figure 25. OWASP dependency-check Result for Client Web Server

3.2 OWASP dependency-check result on Backend Lookup Server

Figure 26. OWASP dependency-check Result for Backend Lookup Server

So, we decided to apply FossID, one of the well known commercial software composition analysis tools and got a temporary license. FossID finds a lot of dependencies, but frequently shows ambiguous information in version or open source name. To clarify, we need to identify all the components information one by one such as name, version, repository, vulnerabilities and dependency-relationship. It requests considerable effort and time. Therefore, in this project, we mainly identified top-level components, and we will not address transitive dependencies. Based on analysis results, there are only a few known security vulnerabilities because we applied the latest open source version.

3.3 FossID Result : Client Web Server

Component	Version	Last updated	Vulnerabilities
aioredis	1.3.1	2019-12-02	-
asgiref	3.5.2	2022-05-17	-

Component	Version	Last updated	Vulnerabilities
async-timeout	4.0.2	2021-12-20	-
attrs	21.4.0	2021-12-29	-
autobahn	22.5.1	2022-06-03	-
Automat	20.2.0	2020-02-17	-
certifi	2022.6.15	2022-06-16	-
cffi	1.15.0	2021-08-14	-
charset-normalizer	2.0.12	2022-02-12	-
constantly	15.1.0	2015-09-11	-
cryptography	37.0.2	2022-05-04	-
daphne	3.0.2	2021-04-08	-
Django	4.0.5	2022-07-04	CVE-2022-34265
django-bootstrap-icons	0.7.9	2022-04-15	-
django-sslserver	0.22	2019-12-10	-
duo-universal	2.0.1	2021-03-26	-
hyperlink	21.0.0	2021-01-08	-
idna	3.3	2022-05-11	-
incremental	21.3.0	2022-02-15	-
msgpack	1.0.4	2021-04-30	-
numpy	1.22.4	2022-07-05	-
opencv-python	4.6.0.66	2022-07-05	-
Pillow	9.2.0	2022-07-05	-
pyasn1	0.4.8	2020-03-22	-
pyasn1-modules	0.2.8	2019-11-17	-

Component	Version	Last updated	Vulnerabilities
pycparser	2.21	2022-01-26	-
PyJWT	2.4.0	2022-07-05	-
pyOpenSSL	22.0.0	2022-06-29	-
requests	2.28.0	2022-06-30	-
service-identity	21.1.0	2021-05-20	-
six	1.16.0	2021-11-22	-
sqlparse	0.4.2	2022-04-29	-
Twisted	22.4.0	2022-06-29	CVE-2022-24801
twisted-iocpsupport	1.0.2	2021-09-06	-
txaio	22.2.1	2022-02-24	-
typing_extensions	4.2.0	2022-06-01	-
tzdata	2022.1	2022-05-18	-
urllib3	1.26.9	2022-05-16	-
zope.interface	5.4.0	2021-04-15	-

Table 20. FossID Software Composition Analysis Result For Client Web Server

3.4 FossID Result : Backend Lookup Server

Component	Version	Last updated	Vulnerabilities
openssl	3.0.3	2022-07-01	CVE-2022-2068, CVE-2022-2274
Berkeley DB	18.1.40	2020-07-24	-
plog	1.1.6	2015-06-24	-

Table 21. FossID Software Composition Analysis Result For Backend Lookup Server

You can see the analysis results in the "documents/test/software composition analysis" folder.

4. SCRM plan

We will not directly fix open source vulnerabilities. However, for supply chain risk management, we will notify any vulnerabilities we've found to the open source community and monitor updates and patches. When any patch is released or the mitigation method is informed, we will apply it as soon as possible.

5. Test Cases

The Test Cases are based on the Functional Requirements and the Quality Attributes refined previously as well as the Security Requirements. See "Team2_TestCase.xlsx" for details. All the Test Cases have been passed.

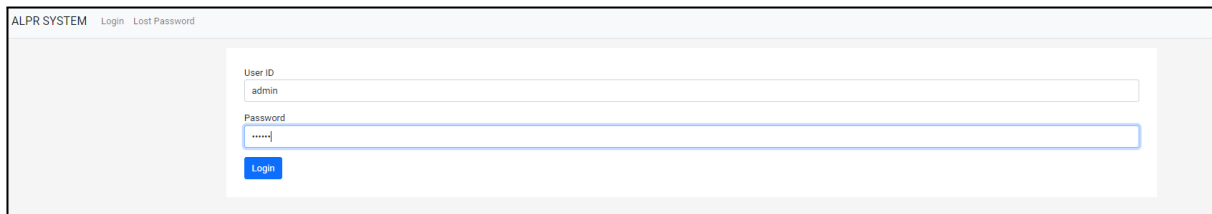| No	TC ID	Category	Sub category	Brief Description	Precondition	Procedure	Expected Rusult	Result	Comments
1	TC-001	Login	Registered User Login	Check the 2 factor login of the registered user in web browser	1. Open the web browser (with chrome) 2. Type web server domain - https://ahnlab2.lge.com:8000	1. Enter the registered User ID and password. 2. 2-factor authentication with Duo	Registered User succeeds in login after 2-factor authentication.	Pass	SR-01
2	TC-002	Login	Registered Admin Login	Check the 2 factor of the administrator in web browser	1. Open the web browser (with chrome) 2. Type web server domain - https://ahnlab2.lge.com:8000	1. Enter the administrator ID and password. 2. 2-factor authentication with Duo	Administrator succeeds in login after 2-factor authentication.	Pass	SR-01
3	TC-003	Login	Unregistered User Login	Check the 2 factor login of the registered user in web browser	1. Open the web browser (with chrome) 2. Type web server domain - https://ahnlab2.lge.com:8000	1. Enter the unregistered User ID and password.	Login failure message is shown. "Please enter a correct username and password. Note that both fields may be case-sensitive."	Pass	SR-01
4	TC-004	Secure Communication	TLS1.3	Check using the TLS protocol to communicate with the lookup server.	1.The test PC should have a packet capture tool (eg wireshark) installed. 2. Open the web browser (with chrome) 3. Type web server domain - https://ahnlab2.lge.com:8000	1. Start the Packet Capture Tool 2. Start the Lookup server 3. Enter the administrator ID and password. 4. Two-step verification via Duo 5. Start packet capture 6. Upload playback video (ex. beaver1.avi) 7. Play video playback (ex. beaver1.avi) 8. Stop Capture Packets	TLS1.3 is used when communicating with Web server and Lookup server.	Pass	SR-02
5	TC-005	Web Server	HTTPS	The client connects to the web server with HTTPS using the web browser.	1. Start Web server 2. Start Lookup server	1. Open the web browser (with chrome) 2. Type web server domain - http://ahnlab2.lge.com:8000	If the client access the web server(ahnlab2.lge.com) using HTTP instead of HTTPS, cannot connect to the domain	Pass	SR-01
6	TC-006	Web Server	HTTPS	The client connects to the web server with the domain name, not the IP address. Also, it should be checked whether the certificate was issued with the domain name of the web server.	1. Start Web server 2. Start Lookup server	1. Open the web browser (with chrome) 2. Type web server IP address and port number - https://10.58.6.103:8000	If the client access the web server(ahnlab2.lge.com) using HTTP instead of the domain name, a web browser is shown a certificate error.	Pass	SR-01
7	TC-007	Lookup Server	Logging information	The lookup server should save the queries of plate number and total query number as a proof of non-repudiation.	1. Open the web browser (with chrome) 2. Type web server domain - https://ahnlab2.lge.com:8000	1. Start Web server 2. Start Lookup server 3. Play the video at client server side(ex. beaver1.avi) 4. check the logging text file.	Check the plate number 2022-07-04 18:16:28.161 DEBUG [36920] [Logging_Index@19] Port Number (Client Port number) requested plate (Plate number)	Pass	SR-05
8	TC-008	Lookup Server	Logging query information	Check the logging correctly	1. Open the web browser (with chrome) 2. Type web server domain - https://ahnlab2.lge.com:8000	1. Start Web server 2. Start Lookup server 3. Play the video at client server side(ex. beaver1.avi) 4. check the logging text file.	Check the right format 2022-07-04 18:16:28.182 DEBUG [33828] [Logging_Index@19] Total Query = 2 Port Number : 412 , Query Per Second : 2	Pass	QA-09
9	TC-009	Lookup Server	Configuration File	The administrator can access and modify the configuration file.	1. Open the web browser (with chrome) 2. Type web server domain - https://ahnlab2.lge.com:8000	1. Login with an administrator account 2. Go to the web page for changing configurable values - https://ahnlab2.lge.com:8000/alpr/config 3. Change max user and confidence level 4. Web server sends the config message	The lookup server receives the config message from the web server, and updates configuration values and file.	Pass	SR-03
10	TC-010	Lookup Server	Encrypt DB	The vehicle information is encrypted and stored in licenseplate DB.	1. Make a new datafile.txt with vehicle information(raw data).	1. Execute loaddb.exe 2. Make a new licenseplate.db from datafile.txt	The licenseplate.db is encrypted. (Open with Notepad++)	Pass	SR-04
11	TC-011	Lookup Server	Decrypt DB	The vehicle information is decrypted and delivered to the web server.	1. Make an encrypted lincenseplate.db usingloaddb.exe	1. Start Web server 2. Start Lookup server 3. Play the video at client server side(ex. beaver1.avi)	The lookup server decrypts the encrypted DB and sends vehicle information that matches the plate query requested from the web server.	Pass	SR-04

Figure 27. Test Cases

Developer Guide

You can see the developer guide document to external reference. (Document/Developers Guide (Team 2).pdf)
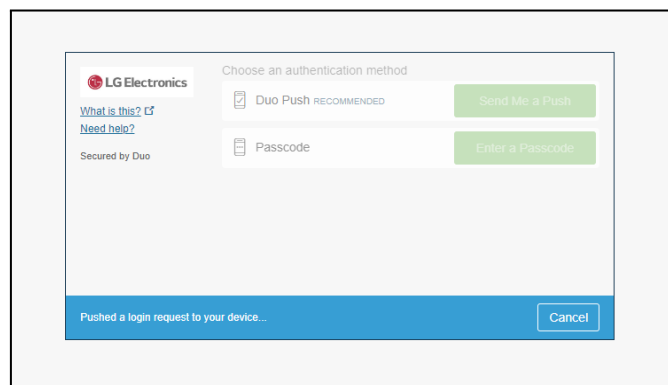
Demo

Client Web Server

The first page is the login client web server. Users can login by entering User ID and password.

Figure 28. Login UI

If the ID and password are correct, the second authentication is performed through Duo.

Figure 29. Two Factor Authentication Page (Duo)

After successfully finishing the second authentication, The User will see the ALPR UI page as you can see in Fig.30. ALPR supports 3 ways of control such as play the live video, upload and play the video file, and upload and play the image file.

Before start, Settings allows you to change the Configure value of the Lookup server and users can choose the 3 ways of control.

The user can upload a video file or image file via the button on the top left. After the Uploaded Videos tab, you can check the history of uploaded files.

If the user wants to live cam, the user turns live cam on and off from the menu tab.

After uploaded files, those files can be seen as an upload video tap and the user pushes the play button to play.

The ALPR system is started and the user can see the lists of the recognized license plate information history at The Detected Information tab. The live video is output in the largest tab

on the left. The vehicle information tab displays the most recently recognized license plate information.
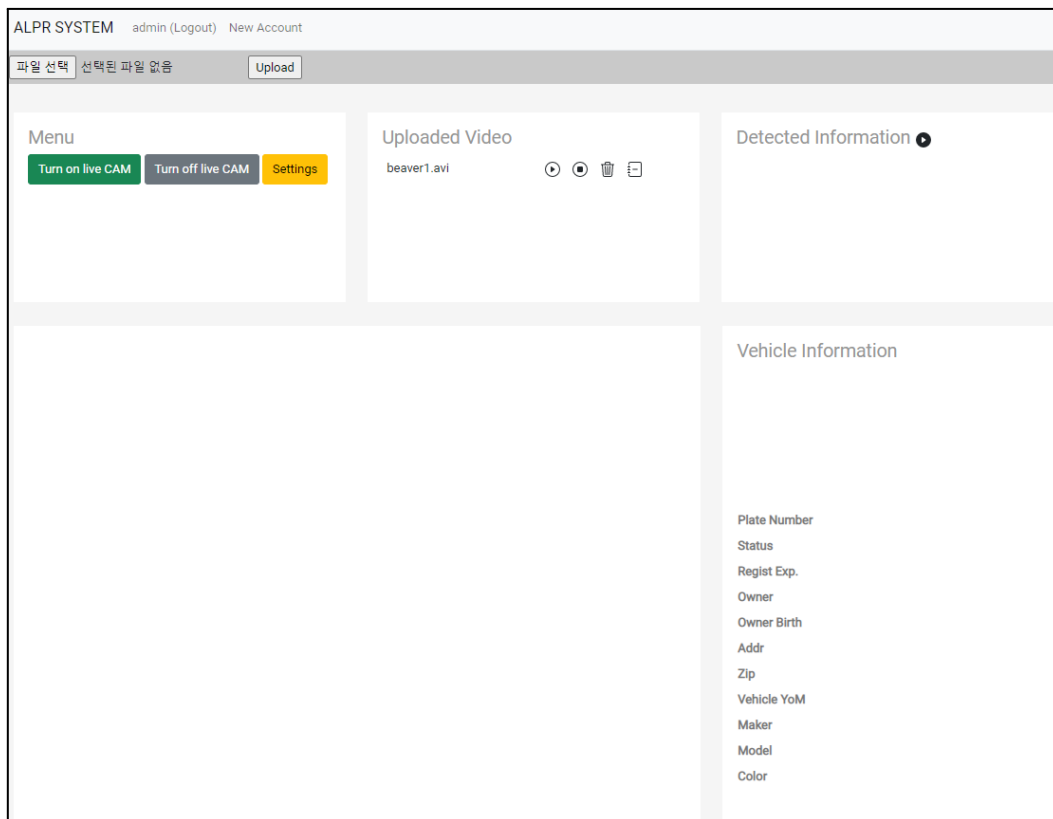
Figure 30. UI of Client Browser

In figure.31, the user can see that the web server and the Lookup server are connected by TLS1.3.
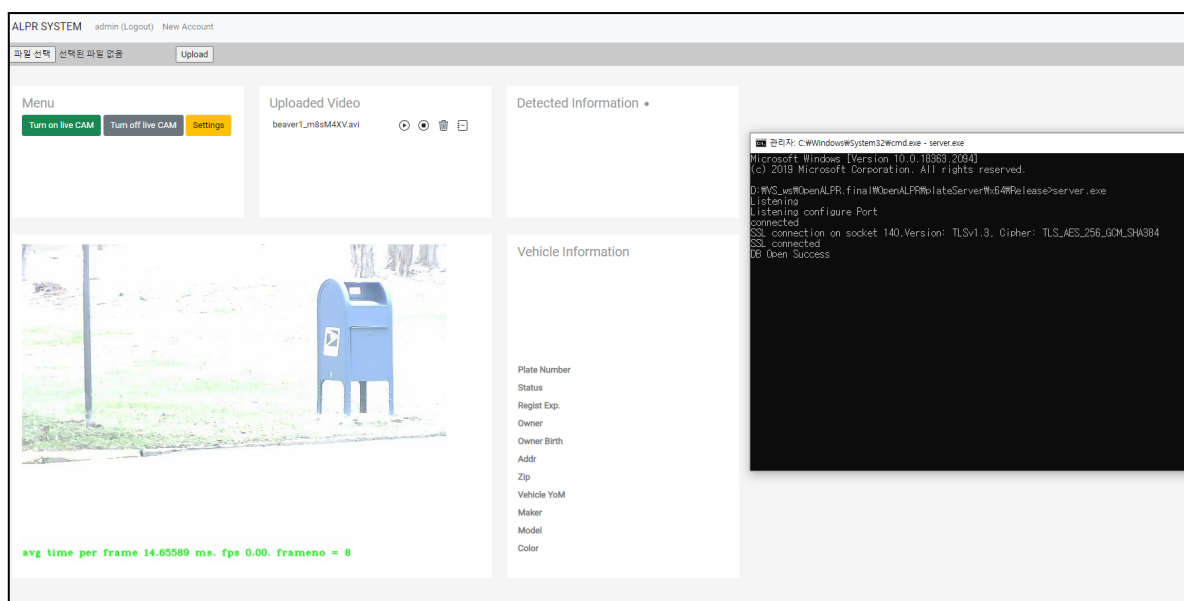
Figure 31. Connect with Lookup Server

When the vehicle number is recognized in the video, the client requests the vehicle information to the lookup server. The Lookup server transmits vehicle information that matches the vehicle number through DB inquiry to the web server, and the web server outputs this information to the vehicle information tab.

Figure 32. Query vehicle information from Lookup Server