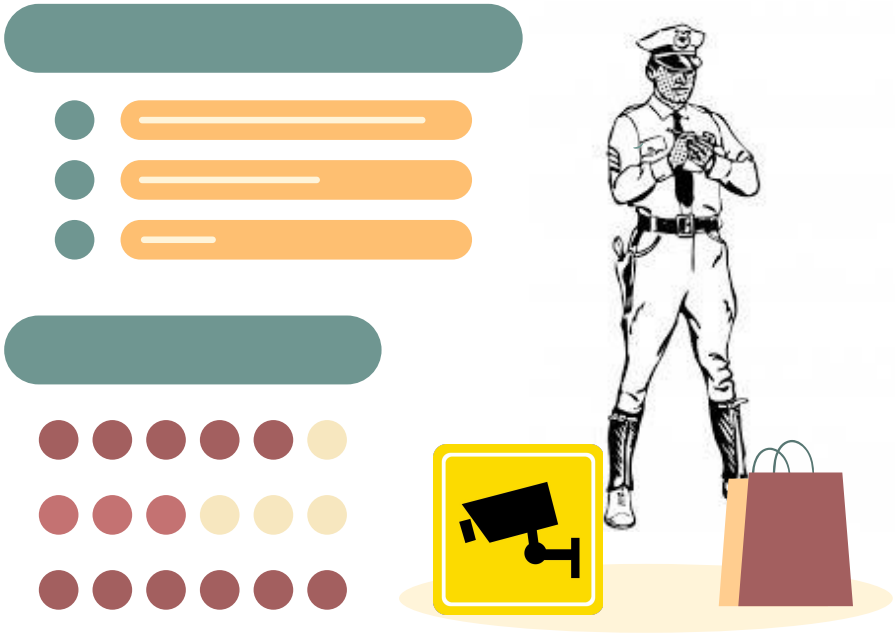
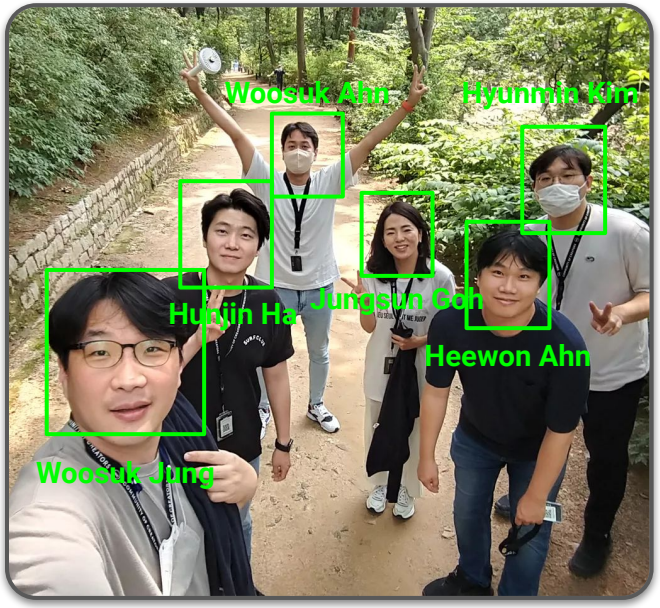
2022
LG Security Specialist
Studio Project
Team 2

Phase 1
July 1st, 2022

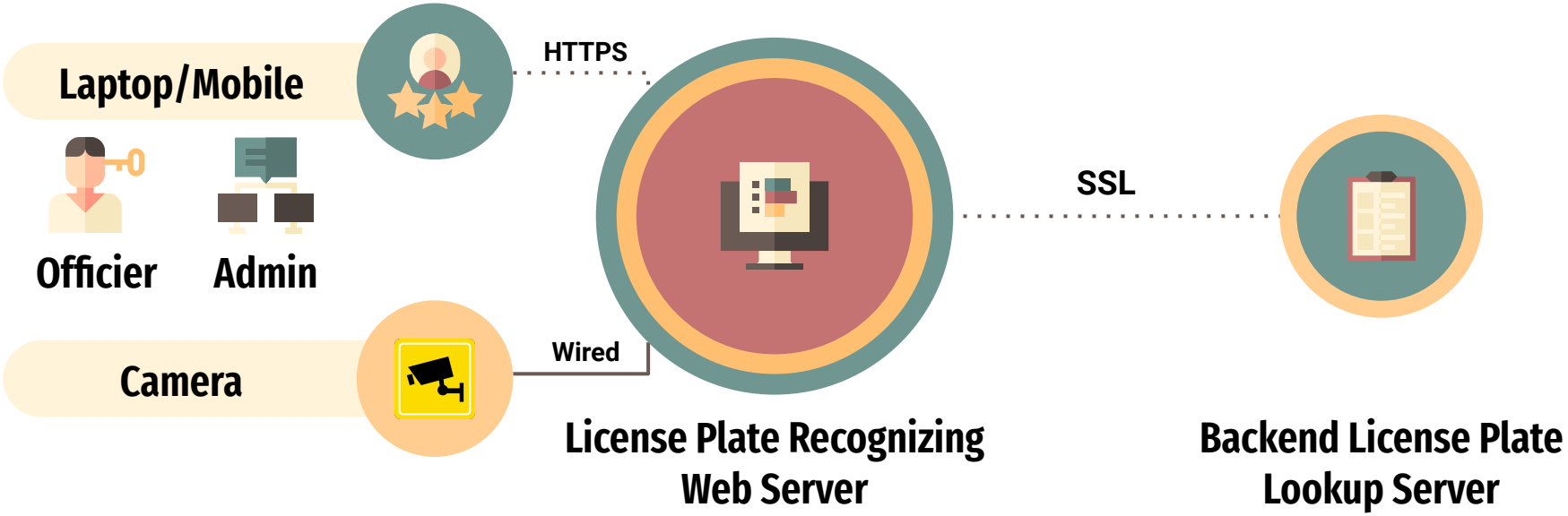


We Are AhnLab!



Members		Role & Responsibility
Woosuk Ahn	Web Backend	*Implement UI and ALPR vehicle control and recognition system and Web*
Heewon Ahn	Web Auth	*Implement the Web authentication part*
Woosuk Jung	Lookup Server	*Implement Backend License Plate Server and DB*
Hyunmin Kim	Lookup Server	*Implement Backend License Plate Server and logging part*
Hunjin Ha	Secure Channel	*Implement SSL protocol*
Jungsun Goh	Documentation	*Quality assurance and documentation*

Studio Project Overview



System Requirements

System Requirements

Phase 1: Development

Your team will develop a secure implementation of the ALPR system. Specifically, you must design and develop a system to meet the following notional requirements. The application should allow a law enforcement officer to use a video feed/picture to identify a license plate and then query that license plate number to determine if there are any outstanding fines or warrants against the vehicle's owner.

FR-01 The proposed system should be a client server system where the client is an on-board computer in a police vehicle or mobile device carried by an officer. The client application should FR-02 communicate securely with a backend server that contains relevant information. The client application has the following basic requirements:

1. The system shall allow FR-03 an officer to access the ALPR system through a secure web interface.
2. The system shall allow FR-04 an officer to login and authenticate users locally and to the backend license plate database lookup. The system must use two factor authentication QA-01 for sign on and user credentials must be protected.
3. Lost or compromised credentials must be handled FR-05 in a reasonable way.
4. The system should allow a law enforcement officer FR-06 to select and save retrieved information locally.
5. The system should allow a law enforcement officer FR-07 to send retrieved information to a mobile device, such as a mobile phone to use in the field.
6. The system should FR-08 provide secure communication between the client application and to the backend license plate database lookup system.
7. The system should FR-09 read images from the vehicle camera or a playback file and identify license plates for evaluation.
8. The system should QA-02 perform the ALPR function in real-time while maintaining a frame rate of at least 25fps.
9. The system should FR-10 query the backend license plate server for details about the vehicle.
10. QA-03 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.
11. QA-04 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.
12. The system should FR-11 provide an area in the user interface that always contains the current camera /playback view.
13. The system should allow officers QA-05 to configure computed camera / playback frames per second, average time per frame, jitter and frame number.
14. The system should allow the officer FR-12 to choose between using a live camera and playback file in the UI.
15. QA-06 The ability to detect network connectivity issues with the backend server within 5 seconds and automatically resolve the communication issue if possible.
16. The system should FR-13 alert officers of any communication errors or failures.
17. QA-07 The system must fetch vehicle information in no more than 10 seconds as officers are often making queries in real time.

The server application shall provide the following functionality

1. Support license plate queries. FR-14
2. Ensure secure communication with the client applications. FR-15
3. Authenticate remote laptop users. FR-16
4. Support multiple users. FR-17
5. QA-08 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.
6. QA-09 Track the average number of queries per second for each user and overall queries per second, for all users.
7. Track the number partial matches and no matches for each user and all users QA-10
8. Support configurable values via a configuration file. FR-18

Aside from these requirements, there are a number of basic quality concerns that must be addressed during development.

1. Ensuring that **all software** in both applications are architected and coded to be 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.

Function Requirements & Quality Attributes

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
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
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 within 5 seconds and automatically resolve the communication issue if
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
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

Security Goal

Goal

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

Confidentiality & Integrity

An officer shall securely access the system and uses data.

Authentication

The identity of the person who is accessing the data and resources in the system shall be verified before access.

Authorization

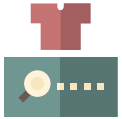
Administrators shall access and modify configuration file.

Availability

An officer shall use the system in real time at any time he or she wants.

Assets

Personal Information



License Plate Number
Vehicle Status
Owner Address
Owner Zip Code
Owner Birth of Date

User Credentials

User ID
User Password

System Config.

Number of Max User
Confidence Level
Lookup Server IP
System Logs

Threats

1 Asset Identification

Assets

Asset	Damage Scenario	Asset ID
License Plate Number	If a license plate number is manipulated, a police officer cannot get valid information or a criminal can avoid law enforcement.	AID-01
Status	If queried vehicle information is manipulated, a police officer cannot get valid information or a criminal can avoid law enforcement.	AID-02
Registration Expiration	No damage	-
Owner Name	Personally identifiable information (PII) may be leaked.	AID-03
Owner Date of Birth	Personally identifiable information (PII) may be leaked.	AID-04
Vehicle Year of Manufacture	No damage	-
Vehicle Make	No damage	-
Vehicle Model	No damage	-
Vehicle Color	No damage	-
Owner Street Address/ Location	Personally identifiable information (PII) may be leaked.	AID-05
Owner City, State and Zip Code	No damage	-
ID	Authentication information can be leaked and an abuser can access the system maliciously.	AID-06
Password	Authentication information can be leaked and an abuser can access the system maliciously.	AID-07
Configuration File	If a configuration file is manipulated, a police officer cannot get valid information or a criminal can avoid law enforcement.	AID-08
Log file	If a log file is manipulated, the server cannot provide access and query information, so the system cannot avoid non-repudiation.	AID-09

Table 2. Asset List

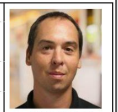
2 Threat Modeling

2) 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 knew that his credential is not expired, and he can access the Tartan ALPR system.
Goals	To retrieve specific vehicle information (include
Skills	
Misuse Ca	

3) Hackers

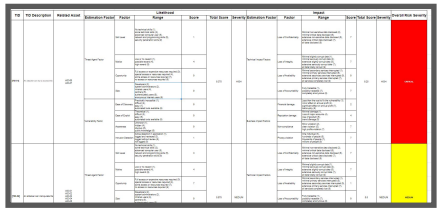
Type	**PID-03:** Hacker
Motivations	He is a champion of '2022 world CTF'. And Tartan requested him pentesting against their new ALPR system.
Goals	To accomplish personal data without detection To cause discomfort to connect the ALPR system.
Skills	He has good Code and Hacking skills He knows whole ALPR System architectures
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.



Jeffrey Gennari

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

3 Risk Assessment



Step 4: Determining the Severity of the Risk

In this step, the likelihood estimate and the impact estimate are put together to calculate an overall severity for this risk. This is done by figuring out whether the likelihood is low, medium, or high and then do the same for impact. The 0 to 9 scale is split into three parts:

Likelihood and Impact Levels	
0 to <3	LOW

Determining Severity

However the tester arrives at the likelihood and impact estimates, they can now combine them to get a final severity rating for this risk. Note that if they have good business impact information, they should use that instead of the technical impact information. But if they have no information about the business, then technical impact is the next best thing.

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

PnG, STRIDE

OWASP

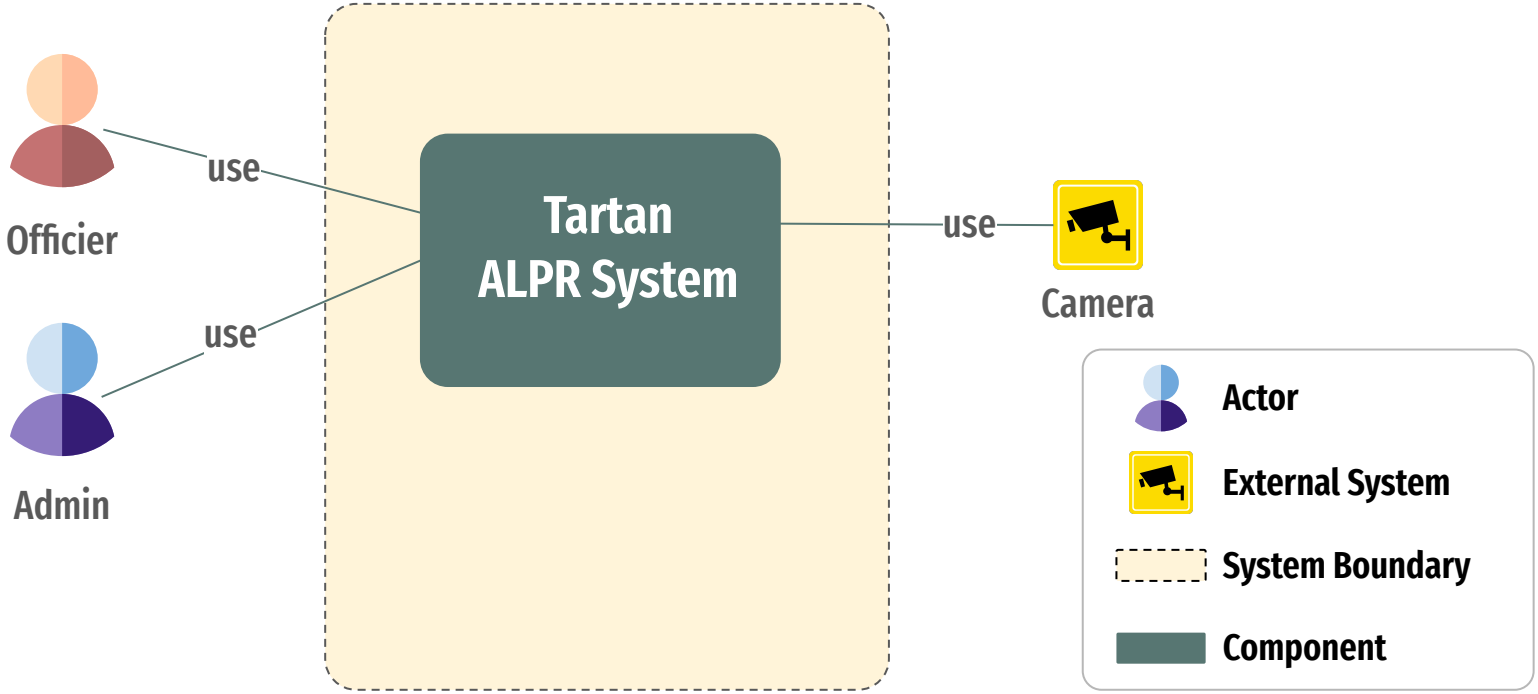
Threats Analysis

TID	TID Description	Related Asset	Overall Risk Severity	Related SR
TID-01	An attacker can try to access the web server by getting an ID/Password.	AID-06 AID-07	CRITICAL	SR-01
TID-02	An attacker can manipulate the plate number requested or responded by reading and modifying the transmitted data.	AID-01 AID-02 AID-03 AID-04 AID-05	MEDIUM	SR-02
TID-03	After the attacker obtains the server's authority using Elevation of Privilege, he may access the database and read the valuable information.	AID-01 AID-02 AID-03 AID-04 AID-05	HIGH	SR-03 SR-04
TID-04	The attacker sends a lot of requests to the Lookup server very quickly and makes the service not available.	AID-01 AID-02 AID-03 AID-04 AID-05	MEDIUM	SR-06
TID-05	An attacker secretly sees a police officer typing ID and PW and obtains ID and PW.	AID-06 AID-07	MEDIUM	SR-01
TID-06	An attacker can erase traces of Database modifications from the log.	AID-09	MEDIUM	SR-05
TID-07	An attacker can access the server with an not expired credential.	AID-01 AID-02 AID-03 AID-04 AID-05 AID-08	LOW	SR-01
TID-08	An attacker can modify the sensitive information in Database	AID-01 AID-02 AID-03 AID-04 AID-05	HIGH	SR-04

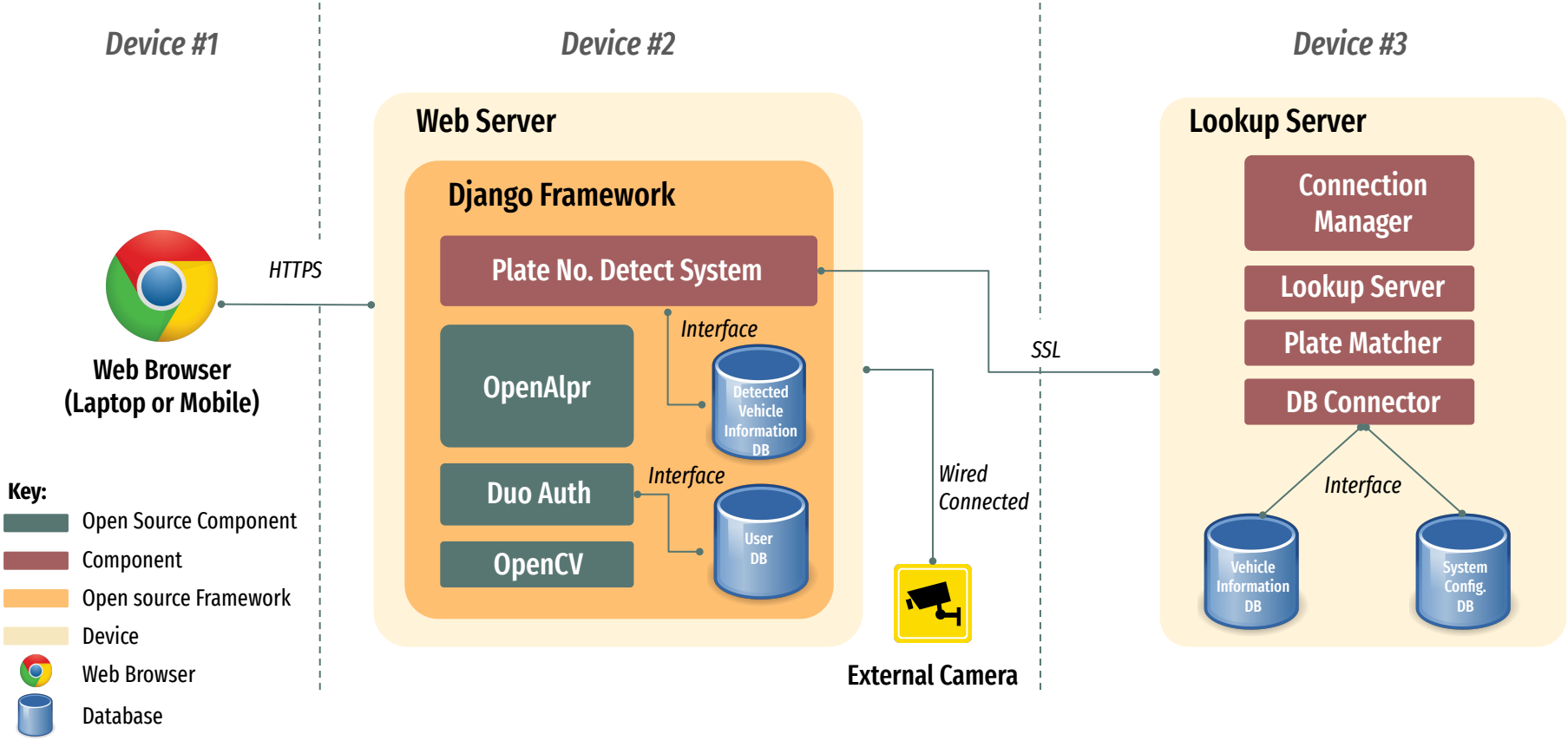
Security Requirements

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

System Context

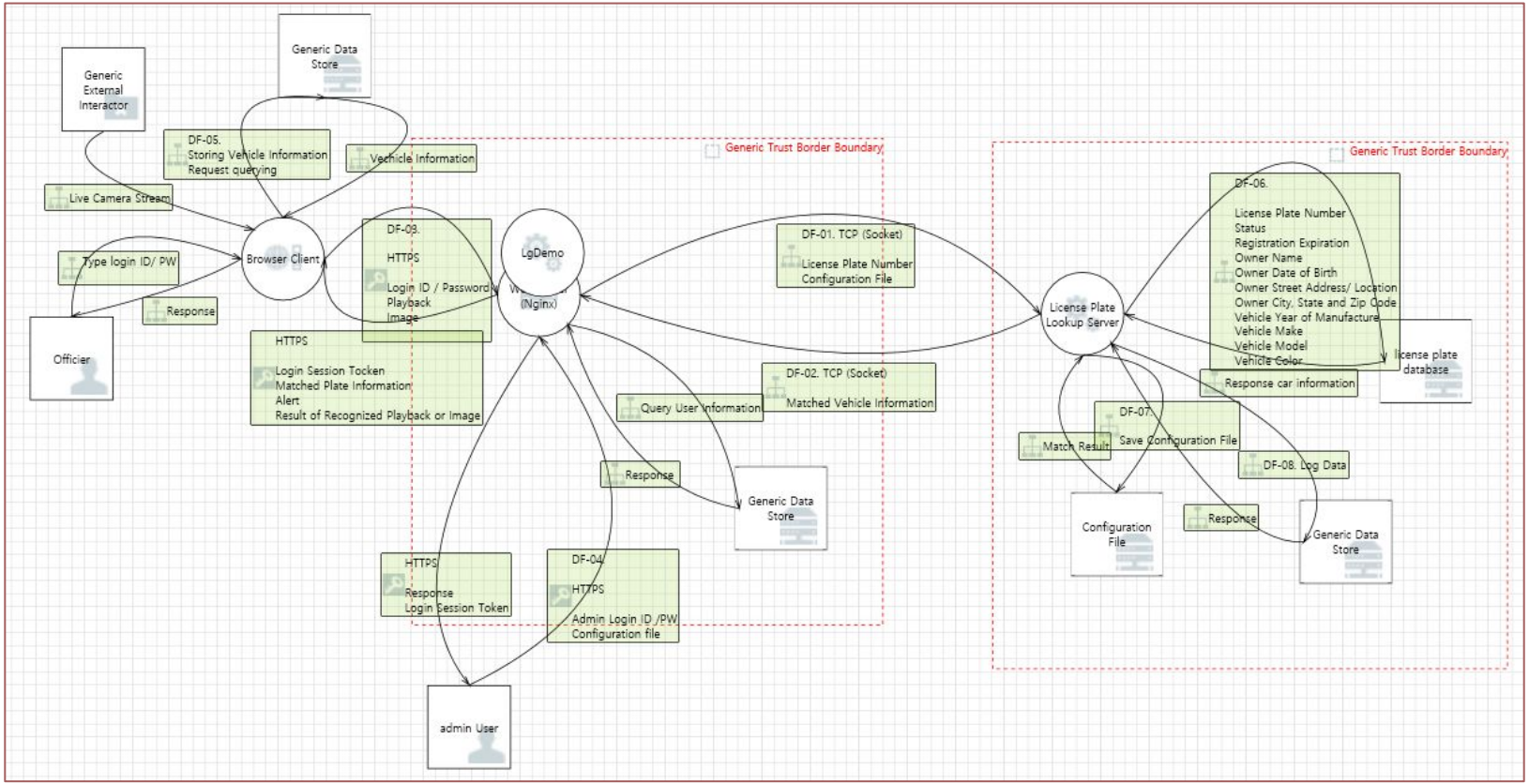


Deployment View



Microsoft Thread Modeling Tool

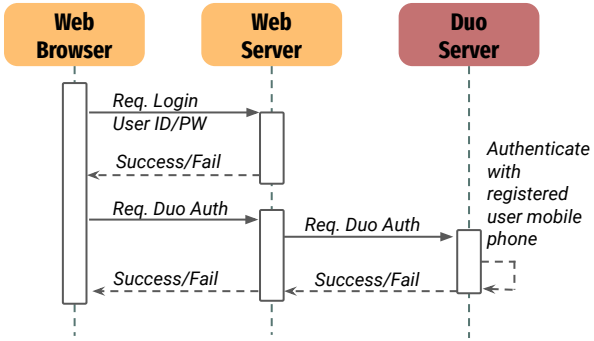
Data Flow Diagram



Main Security Design

Web Client

2-Factor Authentication

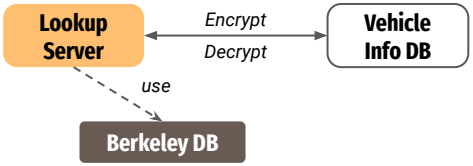


Key:

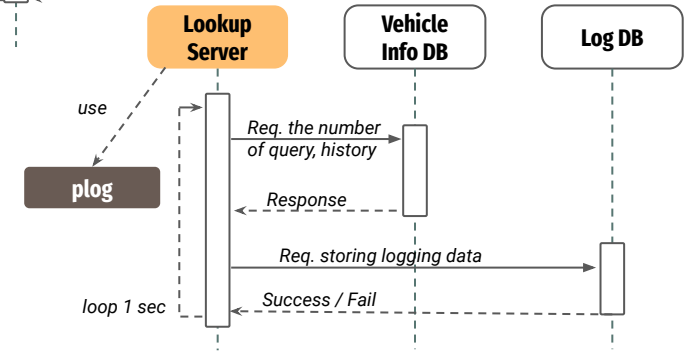
- Device
- External Device
- Database
- Open Source Library
- Certificate (X.509)

Lookup Server

Database Encryption

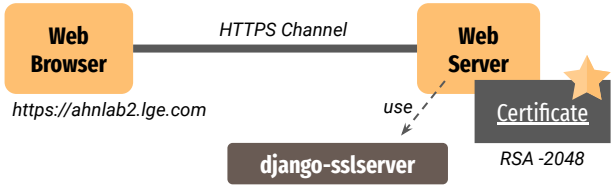


Data Logging

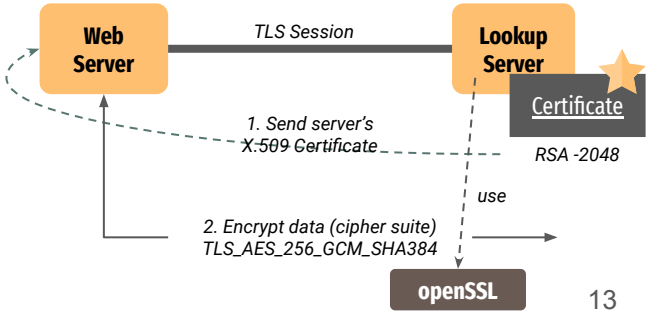


Secure Channel

HTTPS communication



TLS v1.3 communication



Off-the-shelf Libraries, Framework, Tools

Web Server

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*

Lookup Server

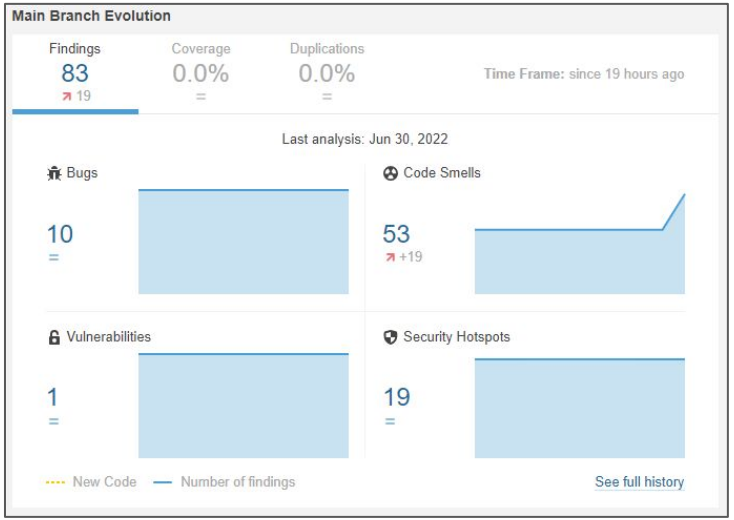
openssl	*v3.0.3*
BerkeleyDB	*v18.1.40*
plog	*v1.1.6*

Tools

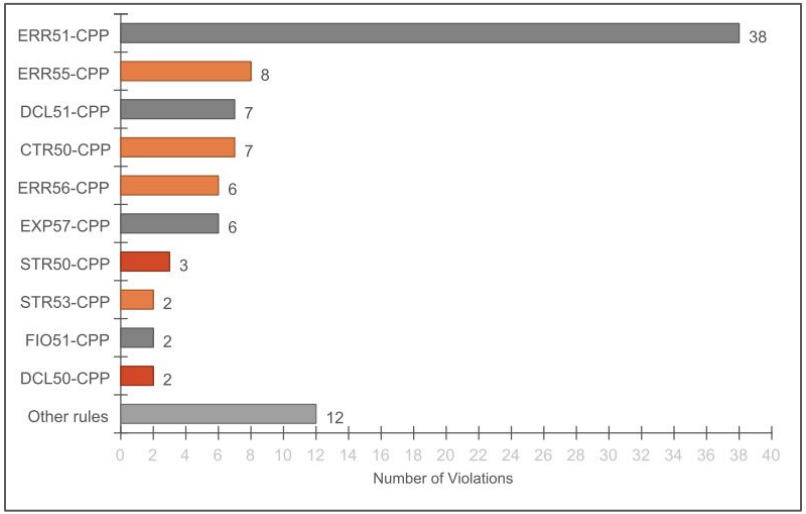
GitHub
FOSSID
Coverity®
DEPENDENCY-CHECK
CERT
sonarcloud
Travis CI
OWASP TOP10
Top 25

Analysis

Static Analysis Results for python & js (client web server)



Static Analysis Results for C++ (backend plate server)



GitHub FOSSID DEPENDENCY-CHECK Coverity® sonarcloud Travis CI CERT OWASP TOP10 Top 25

Demo