LG VideoChat

Phase 1

Team 3

Contents

[1. Introduction 3](#_Toc139992297)

[2. Project Members and Role 4](#_Toc139992298)

[3. Schedule 5](#_Toc139992299)

[4. Functional Requirement 6](#_Toc139992300)

[5. Implementation (with primary requirement) 8](#_Toc139992301)

[6. Summary of Design of System 9](#_Toc139992302)

[6-1. S/W Architecture 10](#_Toc139992303)

[6-2. Static view 12](#_Toc139992304)

[6-3. Sequence diagram (User registration) 13](#_Toc139992305)

[6-4. Sequence diagram (Signaling and call accept) 14](#_Toc139992306)

[6-5. Sequence diagram (Signaling and call decline) 15](#_Toc139992307)

[6-6. Security View 16](#_Toc139992308)

[7. Threat Modeling 17](#_Toc139992309)

[8. 2 Factor Authentication 19](#_Toc139992310)

[9. Test Case 21](#_Toc139992311)

[10. Security Evaluation 25](#_Toc139992312)

[10-1. Dependency Check 25](#_Toc139992313)

[10-2. TLS Validation 25](#_Toc139992314)

[10-3. Static Analysis 26](#_Toc139992315)

# 1. Introduction

This report presents a comprehensive overview of the security phase1. It underscores the significance of understanding potential threats, countermeasures, and the necessity of regular updates and improvements in an ever-evolving cybersecurity landscape.

The goal of this report is to summarize the phase 1 implications of team 3, applying the learned principles and methodologies to real-world situations, and demonstrating how this knowledge can contribute to a safer cyber environment for all.

# 2. Project Members and Role

Architect, Signaling, Database – Seongjun Kim

Registration, Login – Seki Park

2 Factor authentication – Sungmin Kim

Peer connection – Donghoon Shin

Test case and validation – Jiyoung Yoon

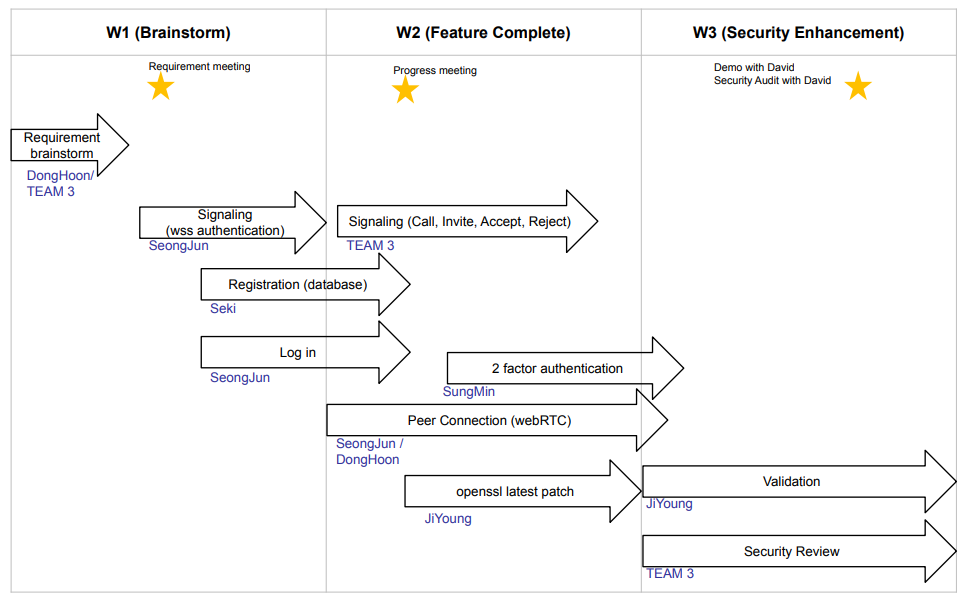
Mentor – David Belasco

# 3. Schedule

Here's a brief summary of phase 1 schedule.   
Over the course of 3 weeks, we focused on different aspects of our project. The first week will be dedicated to brainstorming requirements, setting up signaling processes, and completing the registration procedures.

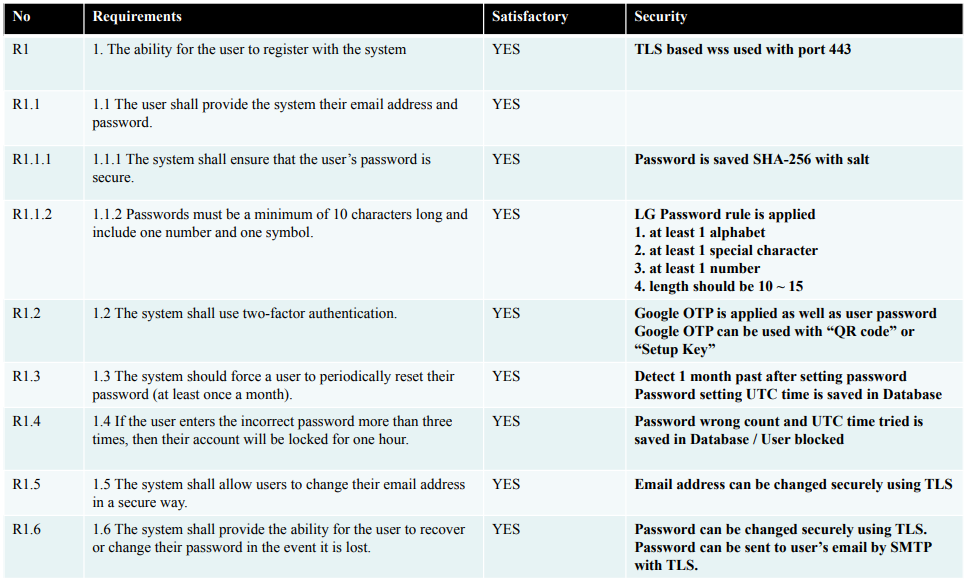
In the second week, we worked on establishing a database connection, implementing the login system, setting up a two-factor authentication process, and facilitating peer connections.

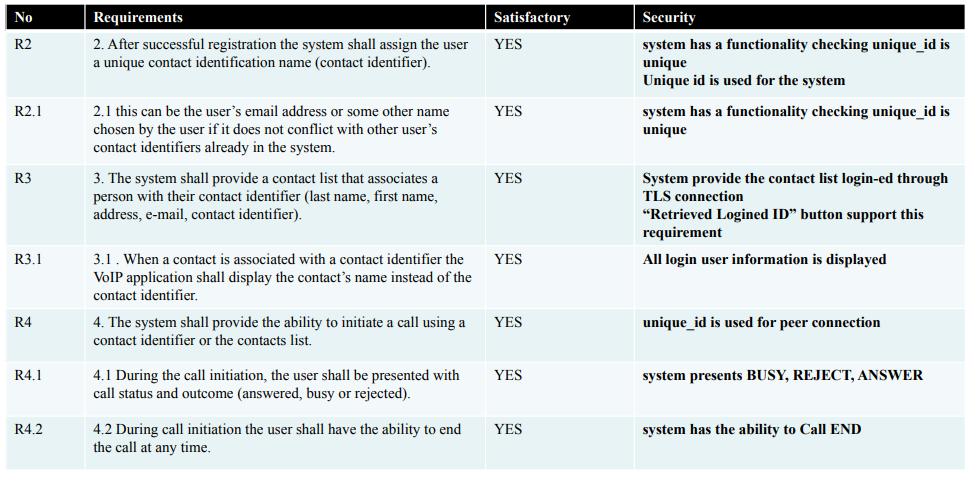
In continuation of the schedule, the third week was committed to performing validation checks and conducting a thorough security review. The objective is to ensure that the system is robust, secure, and functions as intended.

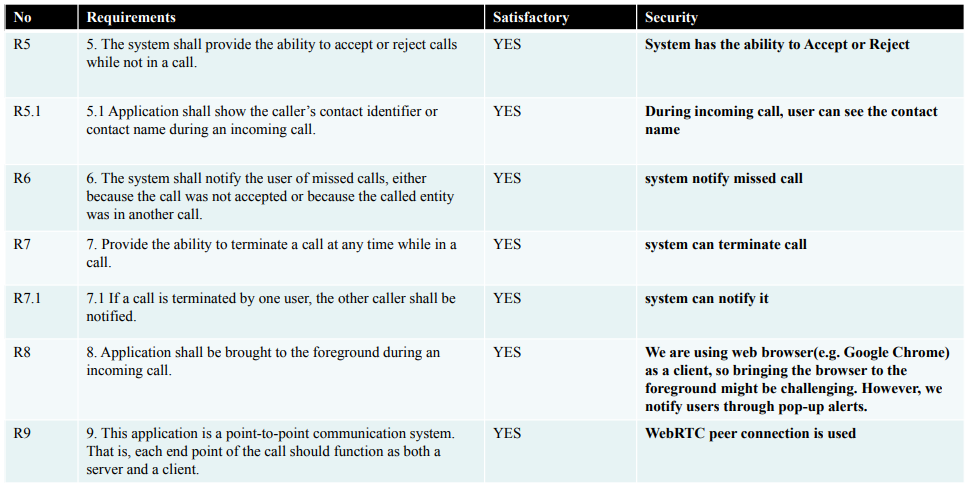


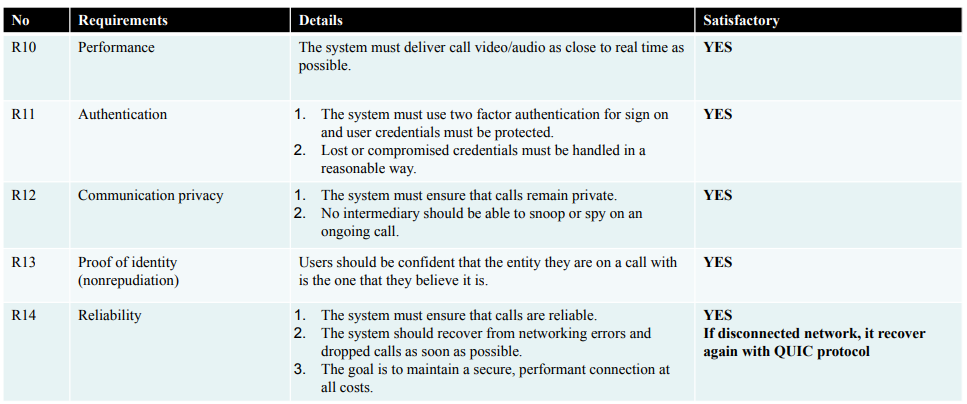
# 4. Functional Requirement

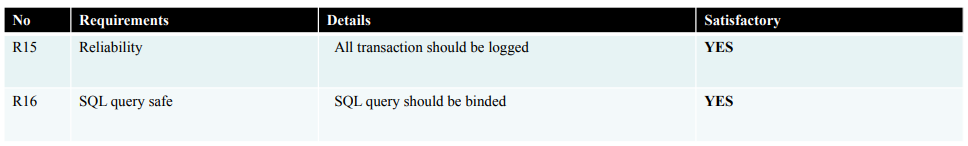
Based on the given requirements, we have constructed the following list to organize and detail these components. This list will act as a comprehensive guide, aiding us in understanding the core functionalities we need to develop, and it will serve as a reference throughout the development process.











# 5. Implementation (with primary requirement)

We mainly focus on to transfer the data of video call securely at very high level.

To do that we do not want to make any attack surface video call stack itself as much as possible and within very limited resources and due date.

Our team engaged in a rigorous brainstorming process to determine the most suitable technology to meet these needs. After careful consideration and comparison of various technologies, we unanimously concluded that WebRTC (Web Real-Time Communication) would be the most efficient and effective tool to fulfill the requirements as secure video chat.

# 6. Summary of Design of System

The system composed of three component.

Video call solution, login or authentication solution, user manage management solution

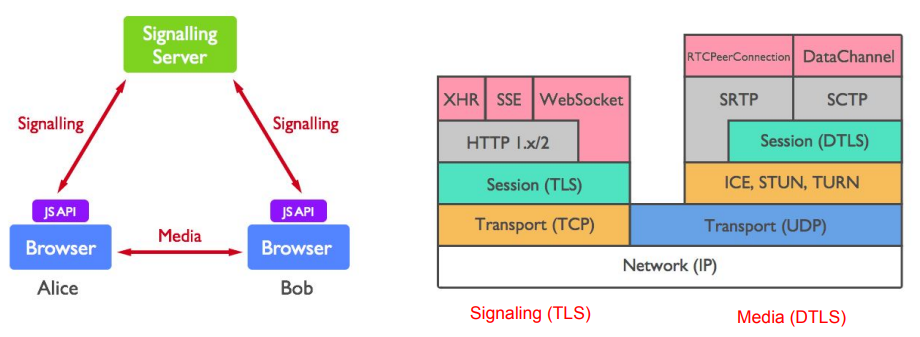
We use webRTC for video solution, 2fa authentication for login solution, and mysql database for user management.

A new user has to be register to user database system, and registered user can login via password and 2fa authentication and can video call each other.

## 6-1. S/W Architecture

Referring to the illustration on the left, it is evident how WebRTC facilitates the establishment of a peer connection between Alice and Bob through the signaling server. It effectively enables the direct exchange of audio/video data via this peer connection. This system allows both parties to send and receive data, ensuring efficient, real-time communication.

From a security perspective, as seen in the right-hand diagram, the signaling process employs Transport Layer Security (TLS) over TCP, ensuring secure and reliable communication. Similarly, the use of Datagram Transport Layer Security (DTLS) over UDP for peer connections guarantees the secure transmission of audio/video data. These measures significantly enhance the security of both signaling and data transfer processes, providing robust protection against potential cyber threats.



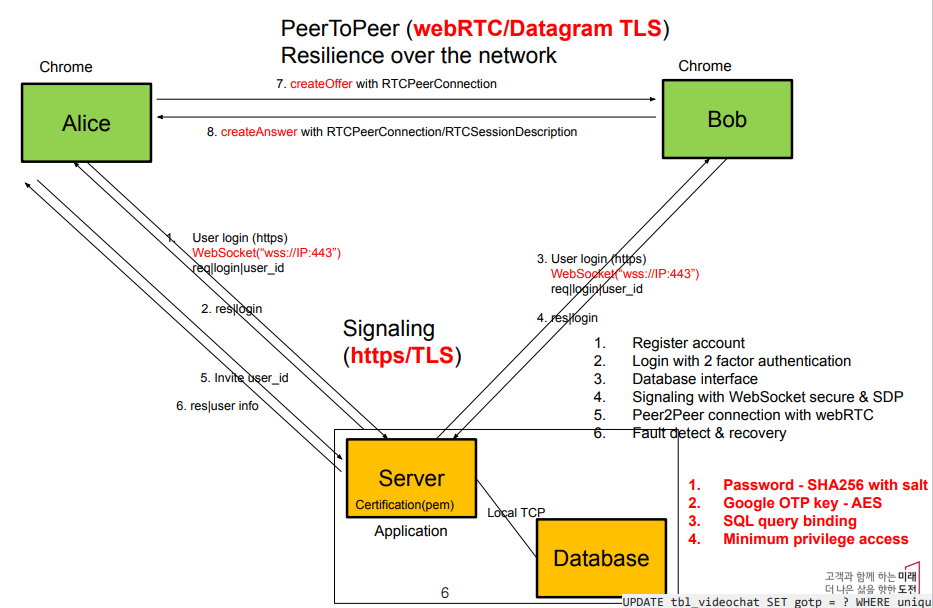
The overall architecture of the project undertaken by Team 3 is as follows: We establish signaling with the server through a secure WebSocket, and we facilitate peer-to-peer communication through the RTCPeerConnection.

Furthermore, we have constructed a database on the server to store user information. To protect sensitive data, particularly passwords, we have implemented encryption using SHA-256 and salt. This method strengthens our system's security by ensuring that user passwords are not stored in plain text.

For additional security, we have also implemented two-factor authentication using Google OTP. This provides an extra layer of security, making it considerably more challenging for unauthorized users to gain access.

In order to guard against SQL injection, a common exploit used to attack databases, we have employed SQL query binding techniques. This helps secure our system by ensuring that user input is always treated as data, rather than part of the SQL command.

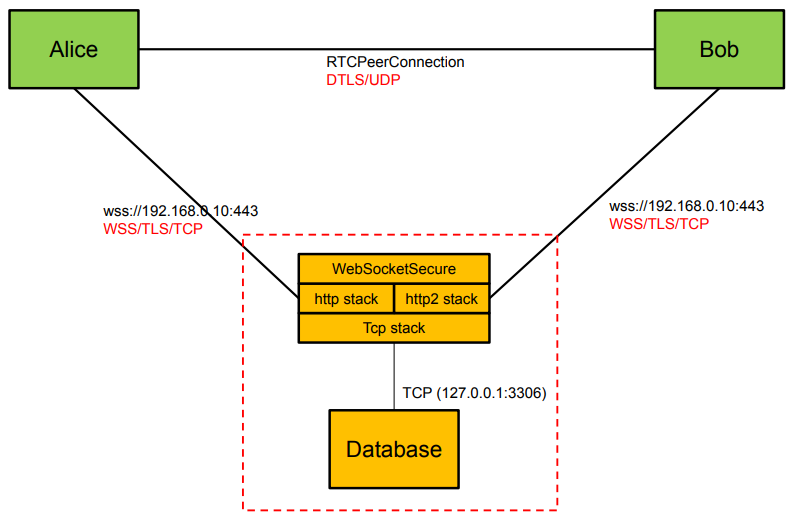
We have also applied the principle of minimum privilege access to our database. This means that each user or process is given the least amount of privilege necessary to perform its task, reducing the potential damage from errors or malicious attacks.



## 6-2. Static view

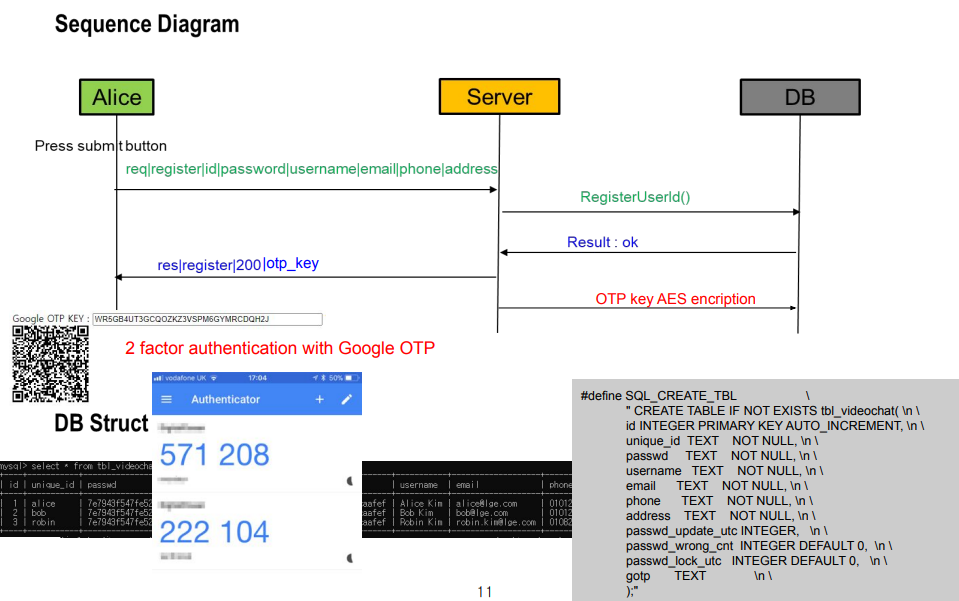
The following represents the static view.

The server and signaling processes utilize secure WebSocket, while the peer connection employs Datagram Transport Layer Security (DTLS) over User Datagram Protocol (UDP).



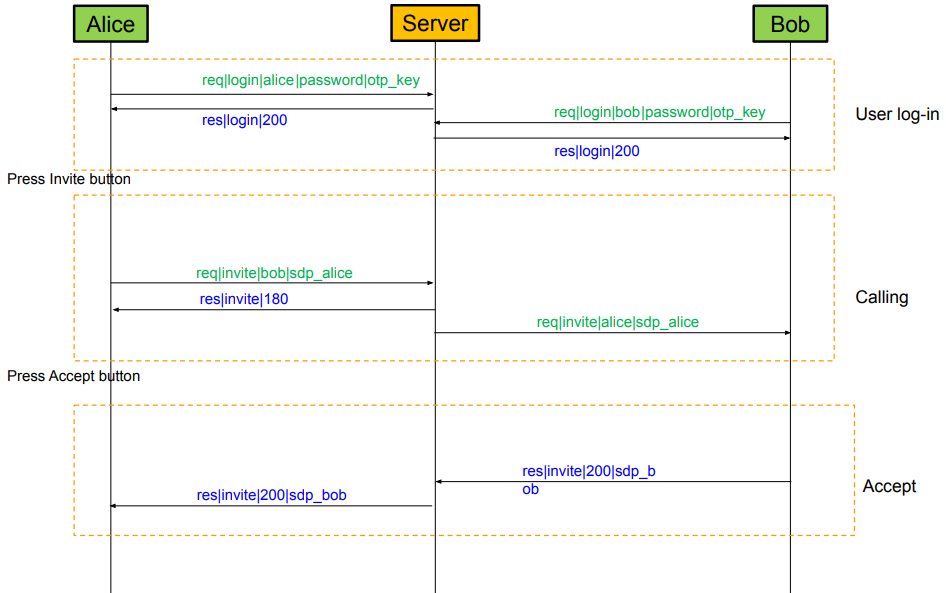
## 6-3. Sequence diagram (User registration)

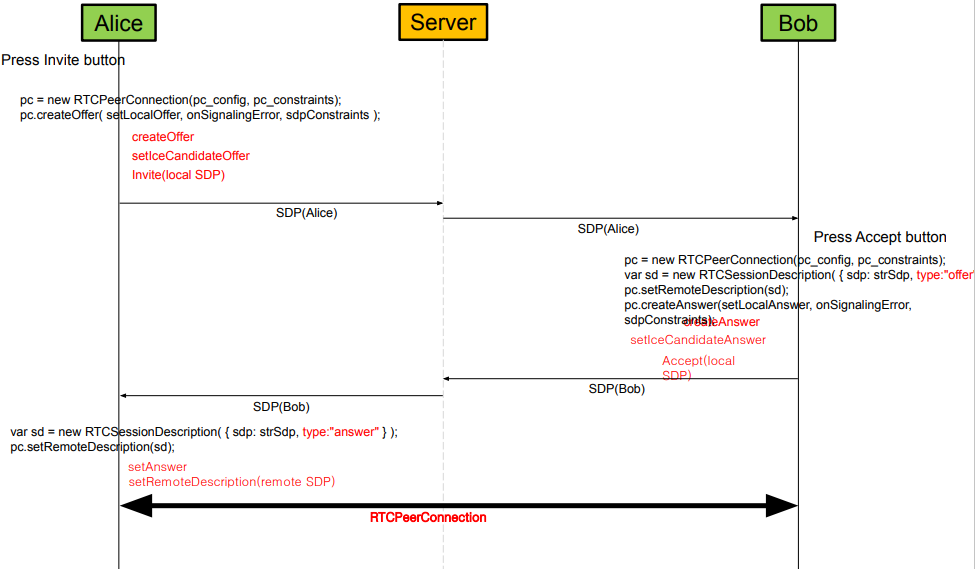
For the registration process, when Alice sends a request to the server, a Google OTP key is relayed back to Alice. This enables her to register by scanning the provided QR code. Additionally, in the database, passwords are stored in an encrypted format that includes salt.



## 6-4. Sequence diagram (Signaling and call accept)

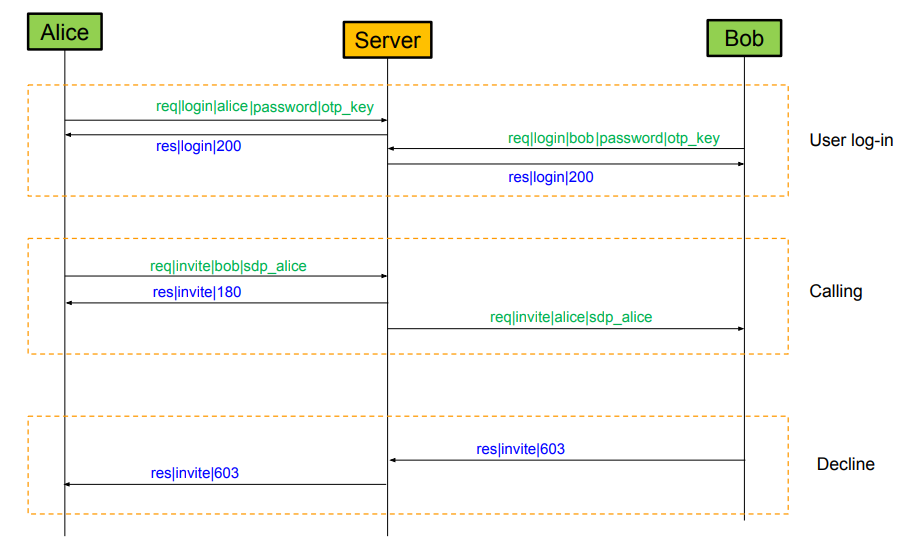
In order for Alice and Bob to communicate, signaling is initiated through an invite request, as depicted in the following diagram. Furthermore, communication is made directly via the RTCPeerConnection, facilitated by the Session Description Protocol (SDP).



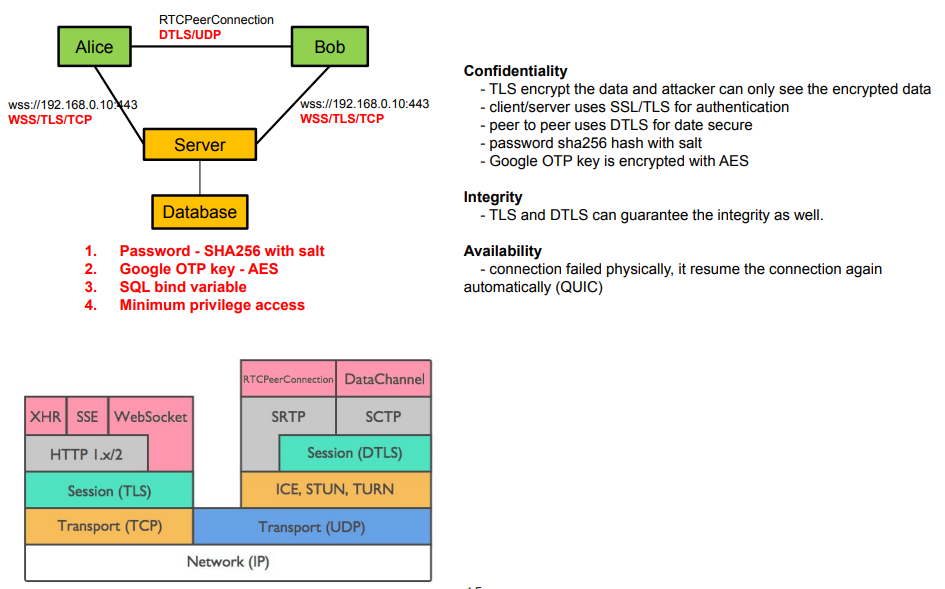


## 6-5. Sequence diagram (Signaling and call decline)

The following illustrates the scenario when a call is declined.

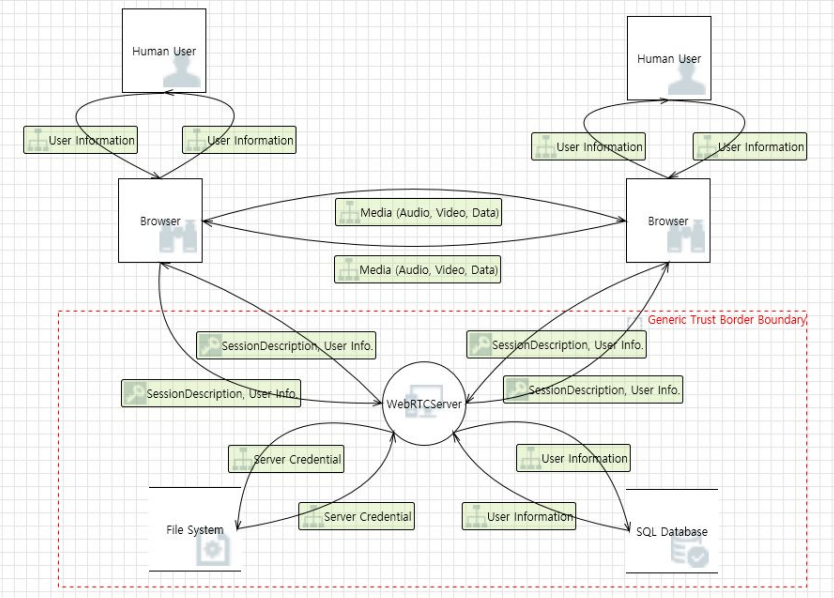


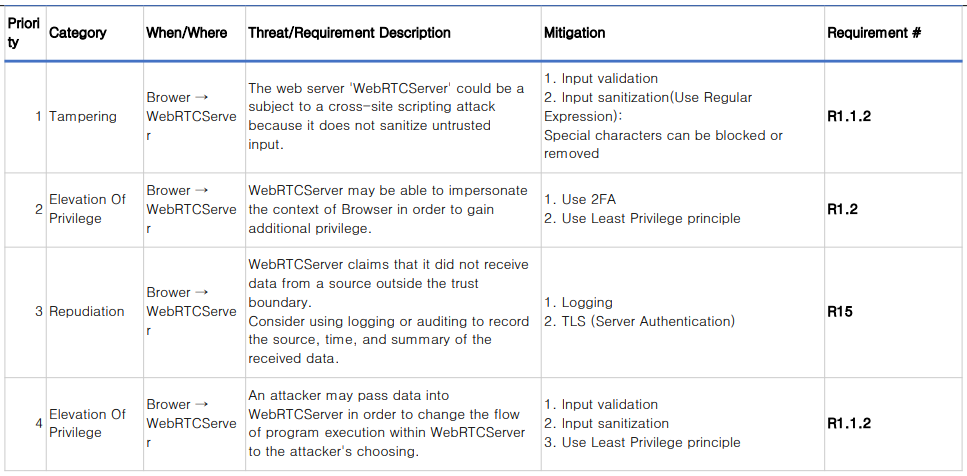
## 6-6. Security View

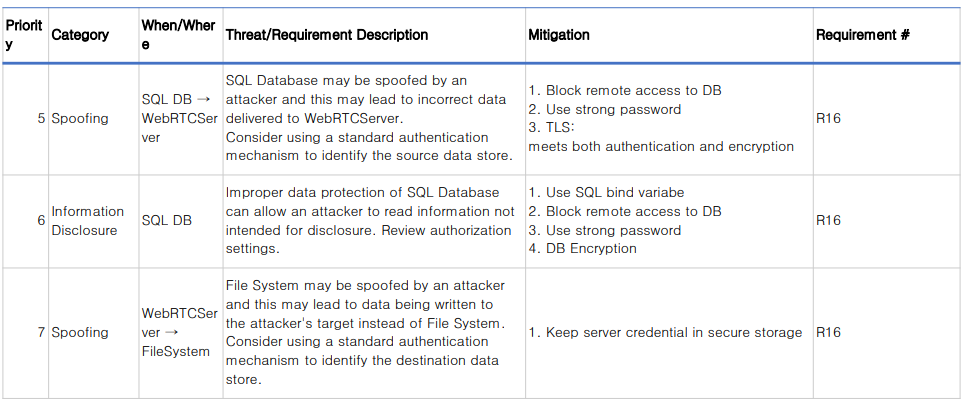


# 7. Threat Modeling

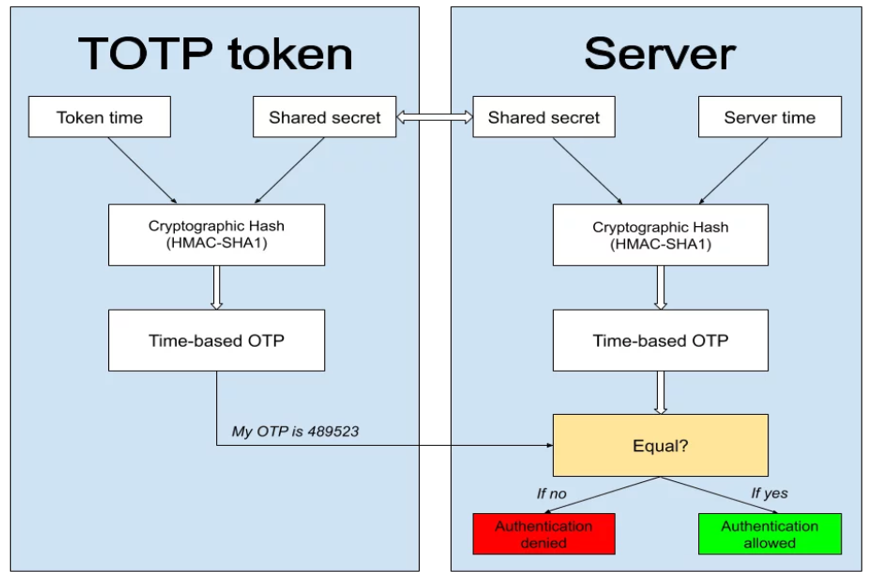
As part of our risk management process, we conducted threat modeling, the results of which are depicted in the following diagram. Through this process, we identified seven major threats to our system. These threats were subsequently analyzed and prioritized to ensure our system’s robustness and resilience against potential cyber-attacks.

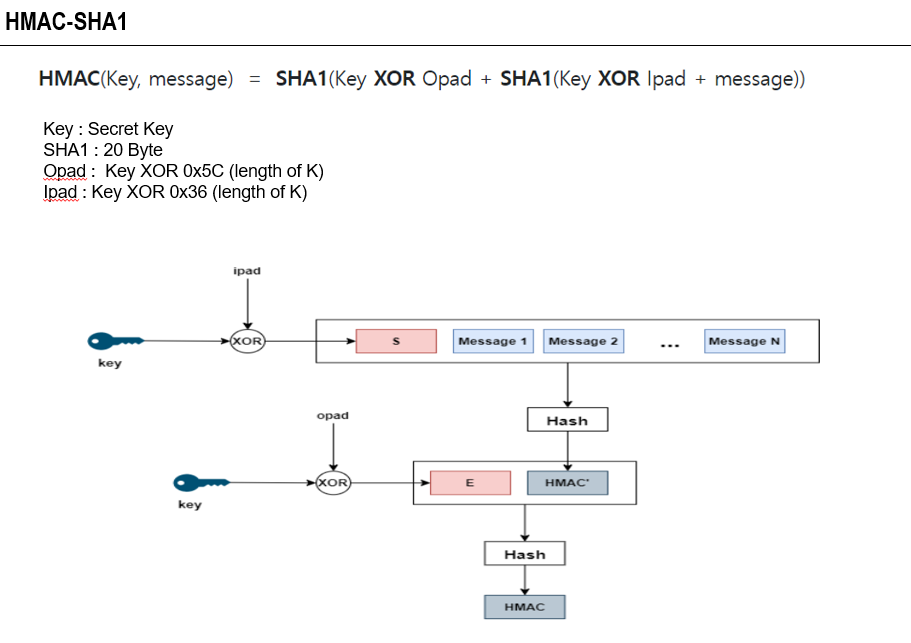


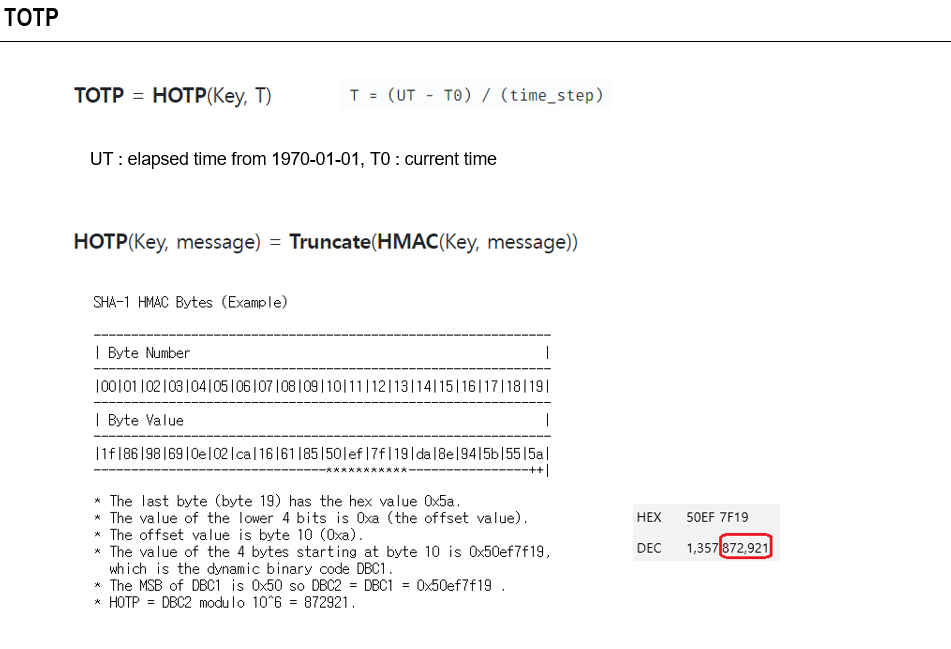




# 8. 2 Factor Authentication

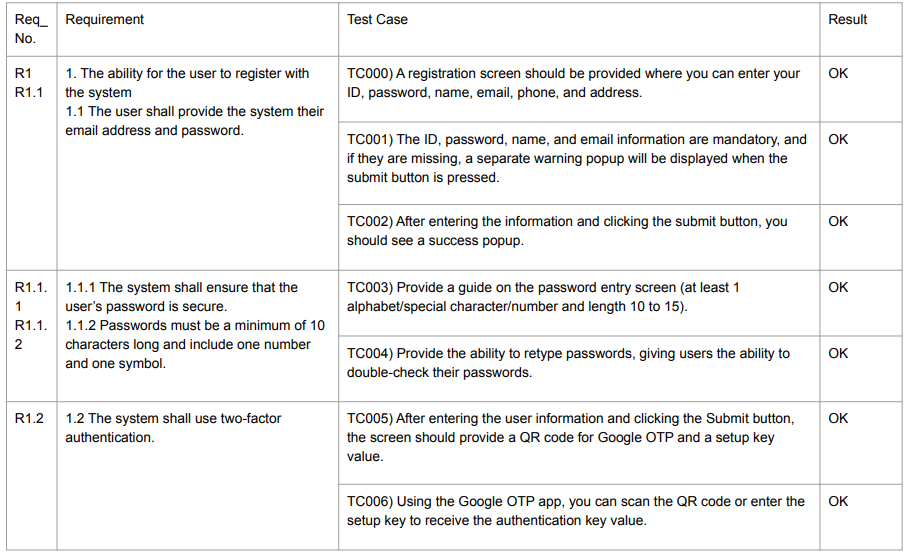


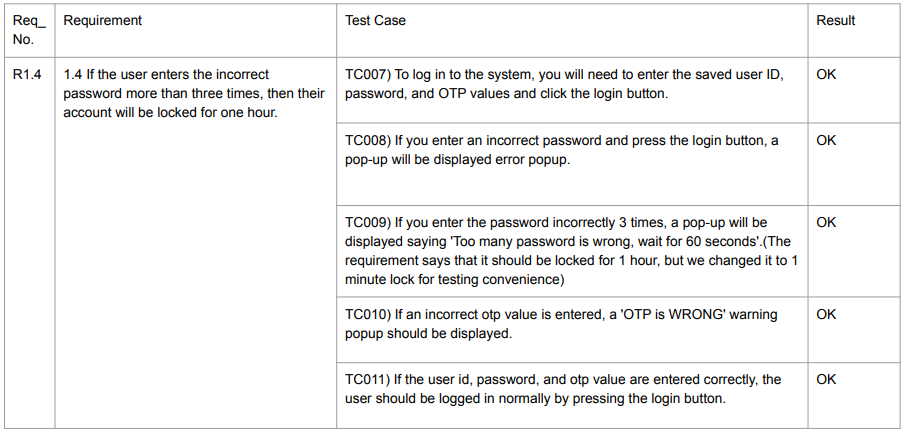


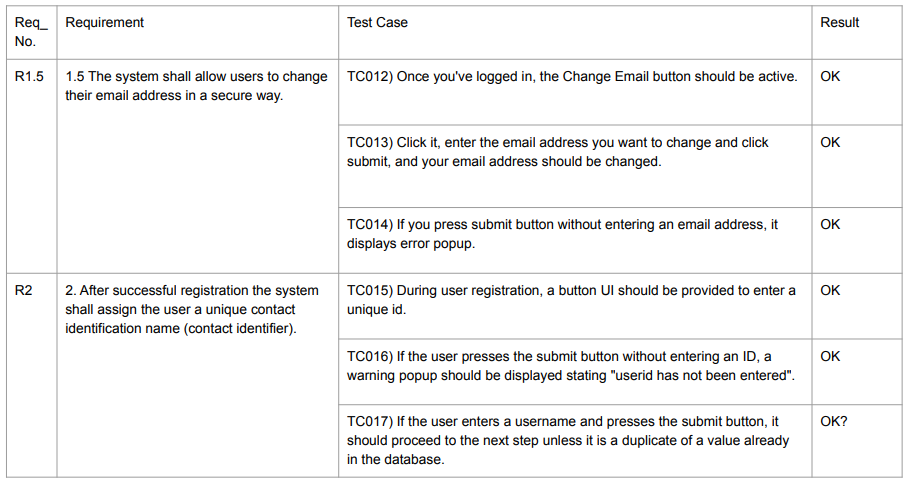


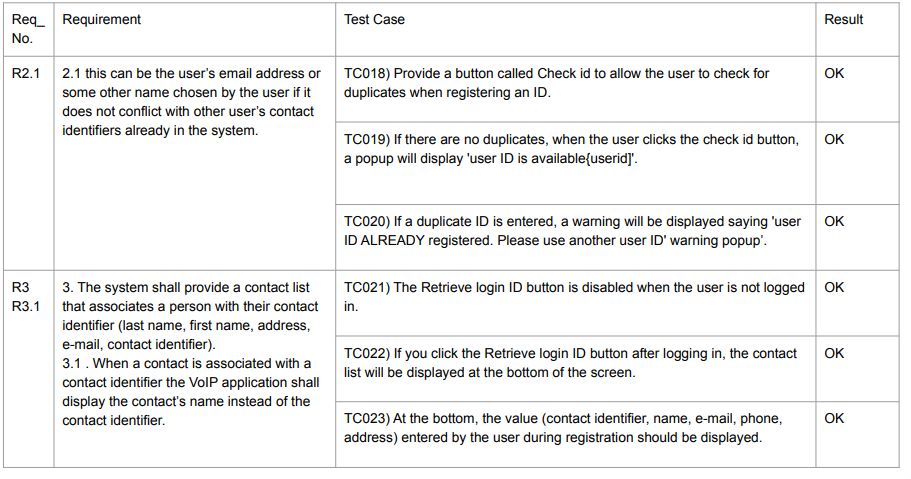
# 9. Test Case

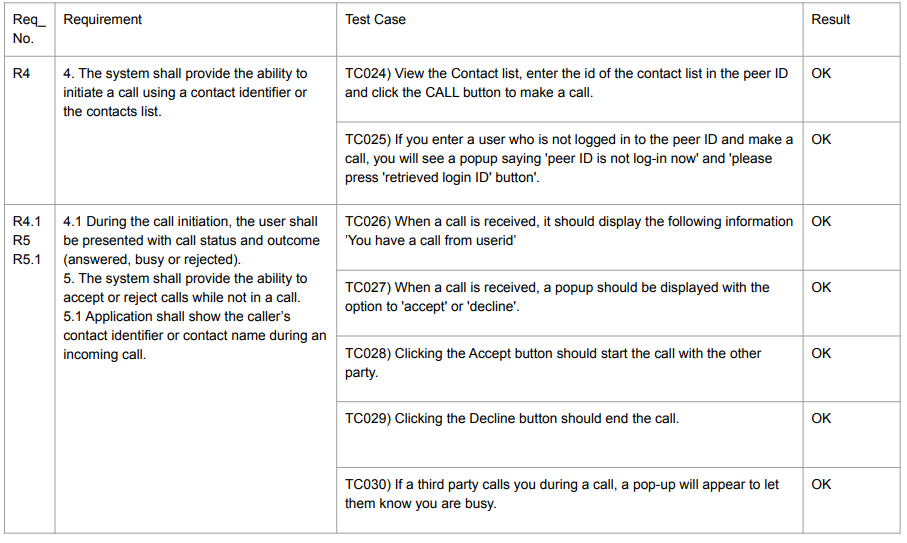
The following showcases the test cases that have been devised based on the requirements, accompanied by the corresponding test results.

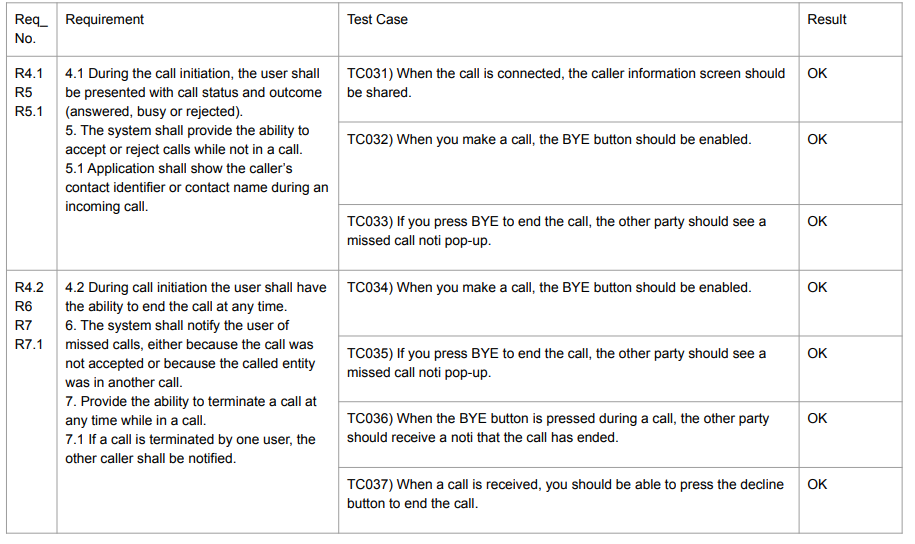


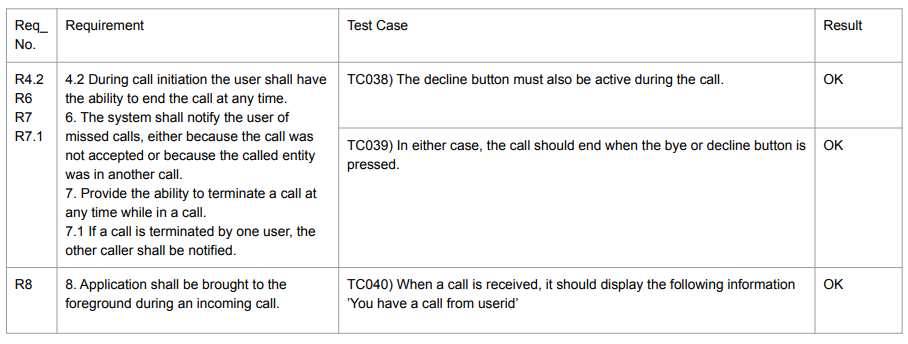






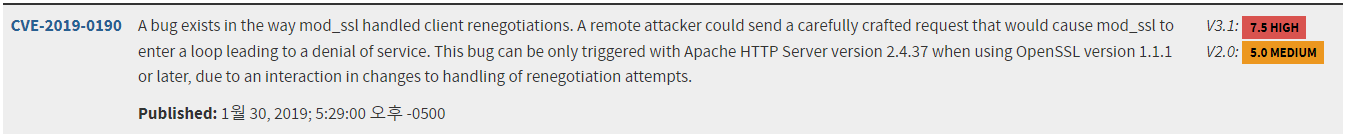
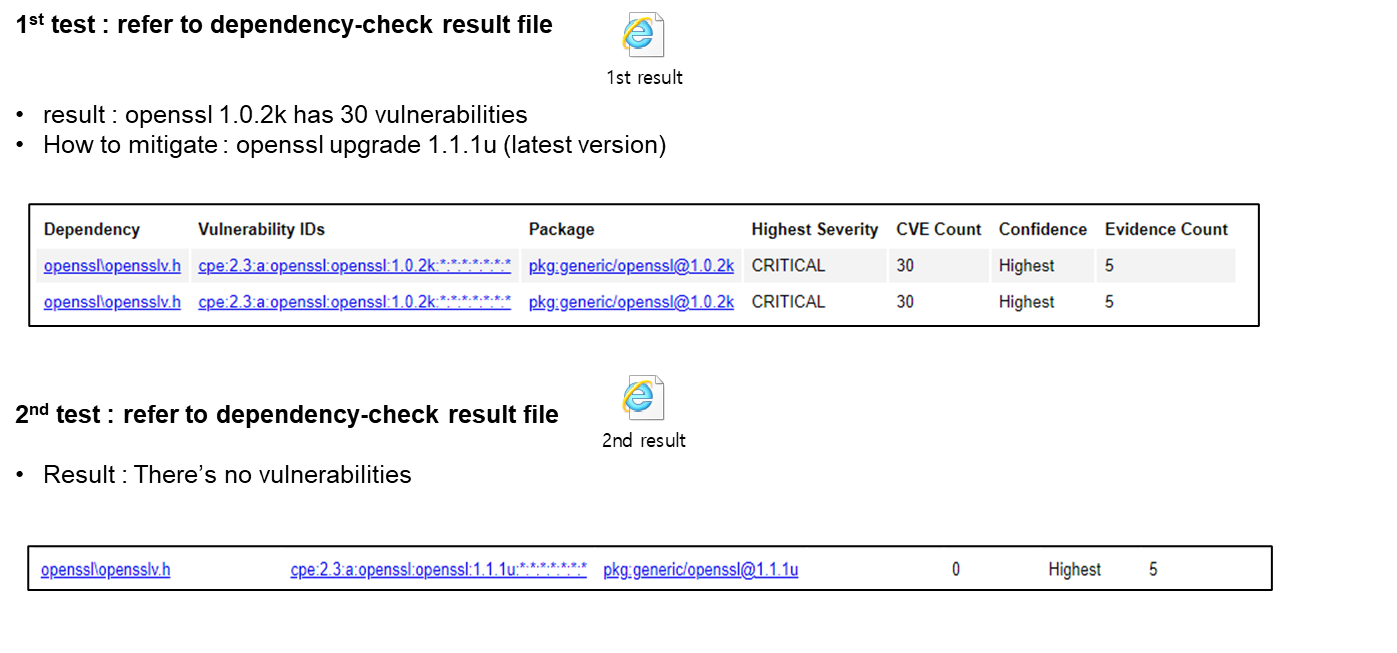






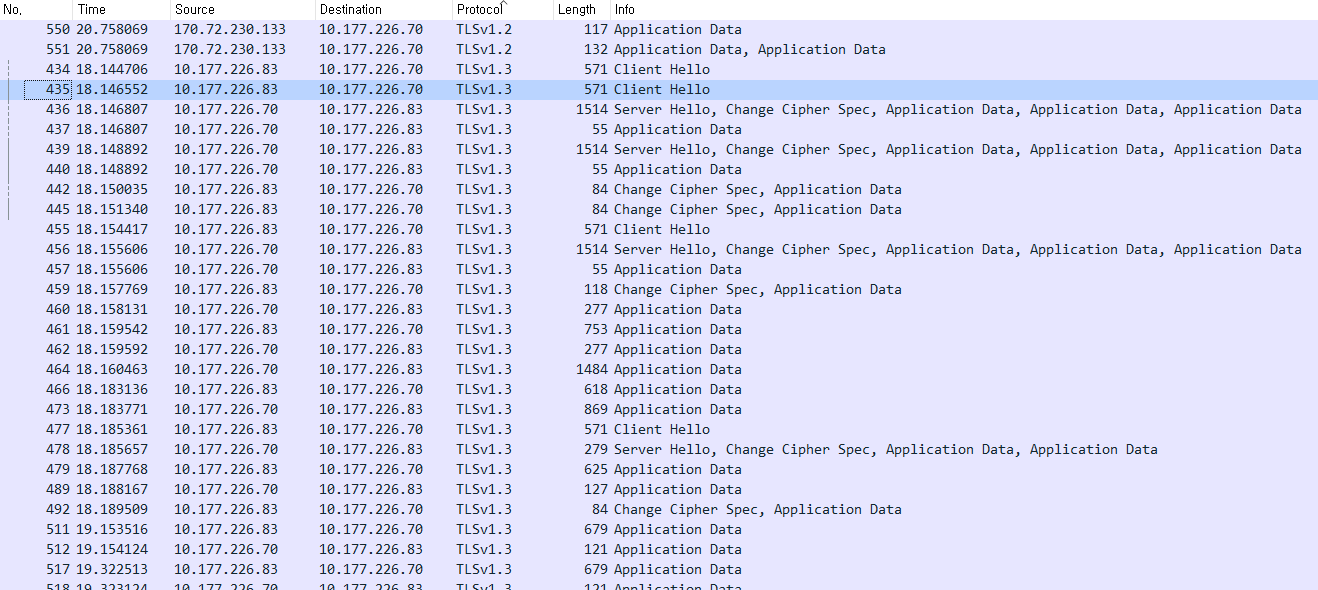
# 10. Security Evaluation

## 10-1. Dependency Check



## 10-2. TLS Validation

Wireshark



## 10-3. Static Analysis

Sonarcloud

