SIL765 - PROGRAMMING ASSIGNMENT

PROJECT 3

Submitted By:
Mehak
2018MCS2143

PROBLEM STATEMENT

Project 3: This project has to do with verifying a document such as a “driver’s license”. (Truly this holds good for any “identity card” or any official document such as a passport or birth certificate.) Typically, and currently, a police officer looks at the physical driver’s license card and simply assumes that the license, together with the information it contains, was issued by the “transport authority”. Given that it is not so difficult to copy, alter or produce afresh a plastic card, how can one use technology to verify on the go the veracity of a driver license card, when shown to a police officer on the road or elsewhere.
(Recall: today cellular based access to Internet-connected servers from smart cell phones is readily available, almost all parts of India.)

Questions:
1. What is the information to be supplied by the driver to the police officer? And what information is sought and obtained from the transport authority?

2. Would you need a central server that has the correct and complete information on all drivers and the licenses issued to them?

3. Is date and time of communication important?

4. In what way are digital signatures relevant?

5. How does one ensure that information is not altered during the 2-way communication?

6. Which of these, viz. confidentiality, authentication, integrity and non-repudiation relevant?

INTRODUCTION

Suppose police wants to verify driver's license shown by him on the road. He will confirm the veracity from a central server by requesting the license id. He will check for :-

1. Expiry of license
2. Tampering of license
3. Replay attack by the server

For this purpose, digital signatures are used by the server to provide message integrity and authentication.

SYSTEM SPECIFICATION

Language used : Python

Assumptions

1. There is a central server having a repository of all the license documents of all the drivers.
2. Police has access to system used for verification of physical license.

PROCEDURE

The procedure used for the verification of license document by police is as following :

1. The police will query the system with the license id of the driver.
2. System will check for the expiry of the license.
3. If expired, it will report. Otherwise, it will proceed further.
4. System will send request to server with license id.

5. Server will respond with the license along with its digital signature.
6. System will verify the digital signature of server and stop if not verified.
7. Then system will check for the replay attack using timestamp.
8. If replay attack is found, it is reported.
9. Else system will match the license send by server and physical license. If not matched, it will report tampering otherwise system will report verified status of license.

IMPLEMENTATION

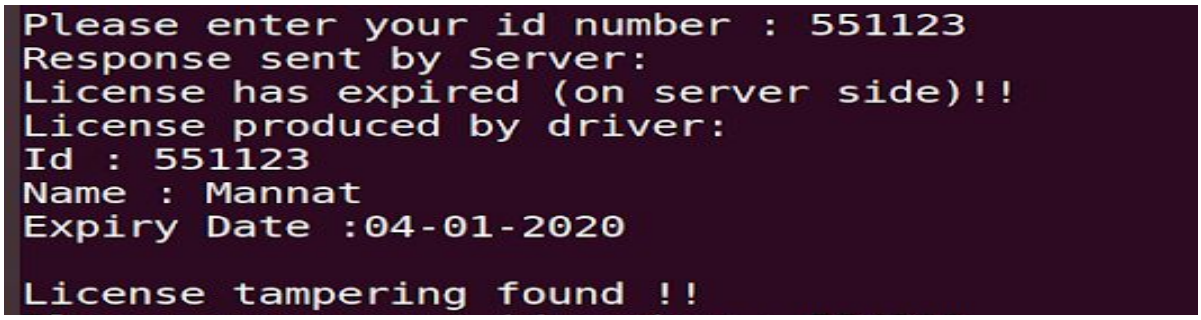
Case 1. License shown by driver is expired.

```
meh@meh-Len:~/Documents/nss/ass3$ python client.py
WELCOME TO ID VERIFICATION SYSTEM !!
Press q to quit.
Please enter your id number : 541232
License has expired !!
```

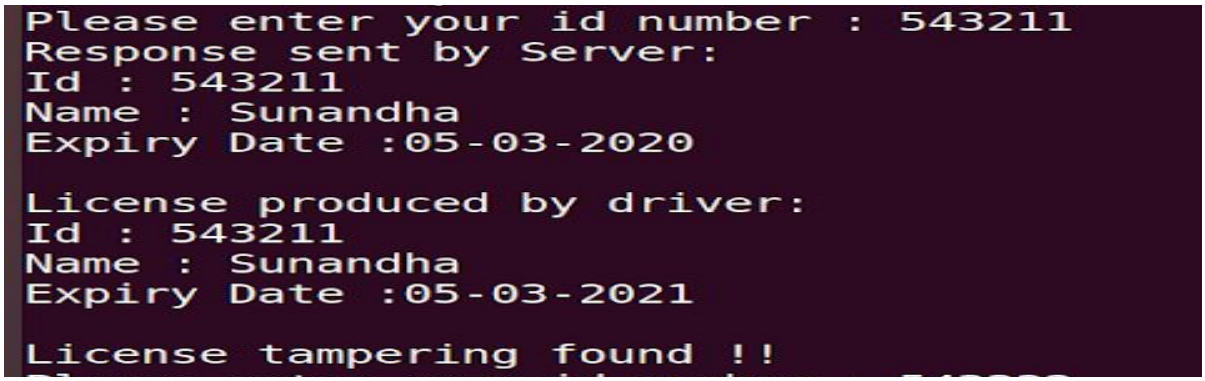
Case 2. License shown by driver is correct.

```
Please enter your id number : 543322
Response sent by Server:
Id : 543322
Name : Anant
Expiry Date :20-12-2020

License produced by driver:
Id : 543322
Name : Anant
Expiry Date :20-12-2020

License verified !!
```

Case 3. License is found expired at server end.



Case 4. License is found tampered.



Q1. What is the information to be supplied by the driver to the police officer? And what information is sought and obtained from the transport authority?

Ans. Driver needs to provide license to the police officer (taken as license id by system and used to collect license of that id). The police officer queries with license id and is provided with license with that id from transport authority.
Q2. Would you need a central server that has the correct and complete information on all drivers and the licenses issued to them?

Ans. Yes, we need a central server that has the correct and complete information on all drivers and the licenses issued to them. The police officer will ask the server for the license with a specific id of the driver.

Q3. Is date and time of communication important?

Ans. Yes, date and time of communication is important because replay attack with the previous message can take place.

Q4. In what way are digital signatures relevant?

Ans. Digital signatures are relevant for authentication and message integrity. When server responds with the license, digital signature of the license is also send along with the license. So that police officer can verify the integrity of the message.

Q5. How does one ensure that information is not altered during the 2-way communication?

Ans. One ensures that information is not altered during the 2-way communication using digital signatures. The server send the digital signature of the information encrypted with its private key along with the information. Then the receiver system will compute the hash of information and match it with the decrypted hash received from the server. If both are same, it implies that information is not altered.

Q6. Which of these, viz. confidentiality, authentication, integrity and non-repudiation relevant?

Ans. Confidentiality is not relevant as anyone can see the license it need not be kept secret. Authentication is not much relevant because anyone can have access to the license so the person asking for license need not be authenticated. However, authentication of the server is done using digital signatures. Message integrity is relevant here that is preserved using digital signatures. Non-repudiation is not relevant here because the transport authority cannot deny later about license issued because it is signed with their digital signatures and timestamp.