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. Validity of license

For this purpose, digital signatures are used 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 police id, license id and hash of license encrypted with server's public key.
5. Server will decrypt the message, compare the hash sent with the hash of license at server end.

IMPLEMENTATION

```
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 !!
```

```
meh@meh-Len:~/Downloads/2018MCS2143$ python client.py
WELCOME TO ID VERIFICATION SYSTEM !!
Press q to quit.
----Keys generated successfully----
Please enter your id number : 541233
Response sent by Server:
License tampered as no license found !!
Please enter your id number : 551123
Response sent by Server:
License tampered!!
Please enter your id number : 541321
Id number not found!!
Please enter a valid id number.

Please enter your id number : 543211
Response sent by Server:
License tampered!!
Please enter your id number : 541232
License has expired !!
Please enter your id number : 543322
Response sent by Server:
License verified successfully!!
Please enter your id number : q
```

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 status of verification 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. Police officer sends hash of the license which is encrypted by server's public key which preserves integrity of message also. Hence digital signatures are not much relevant here.

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 suitable encryption. Since the communication is encrypted there is no way of alteration of messages. Also the system will send request with a license id and hash

of license to the server. Then the server will compute the hash of information and match it with the hash received. 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 relevant as anyone should not see the license information as it contains some personal details that needs to be be kept secret. Authentication is also relevant as both the server and police officer needs to be authenticated which is done by encryption. Message integrity is relevant here that is preserved using digital signatures and encryption. Non-repudiation is also relevant here because the transport authority cannot deny later about license issued because it is signed with their digital signatures and timestamp.