Network Security(CSE350/550)

Assignment 3 : On-the-go verification of Driver's License

Contributors:

Paras Dhiman (2021482) || Aekansh Kathunia (2021127)

Questions and Answers:

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

Ans1:

- **Information Supplied by Driver to Police Officer:** When a driver is stopped for license verification, they provide their personal information such as name, date of birth, mobile number, and license number to the police officer. This information is essential for the verification process and helps establish the driver's identity.
- **Information Sought and Obtained by Police Officer from Server:** The police officer, upon receiving the driver's information, communicates with the transport authority server to obtain detailed information about the driver's license. This includes critical details such as the license number, expiry date, and other relevant information stored in the transport authority's database. By retrieving this data from the server, the police officer can verify the authenticity and validity of the driver's license in real-time.

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

Ans2:

The existence of a central server with comprehensive and accurate information on all drivers and licenses issued to them is paramount for the effective functioning of the system. Such a server acts as the authoritative source of information, serving as a centralized repository for storing and managing driver license data. Without a central server, it would be challenging to perform real-time license verifications and ensure consistency and accuracy across different verification processes.

3. In what way are digital signatures relevant?

Ans3:

Digital signatures play a crucial role in ensuring the authenticity and integrity of messages exchanged between different entities in the system, including the server, drivers, and police officers. By digitally signing messages using their private keys, parties can provide proof of the message's origin and ensure that it has not been altered or tampered with during transmission. Digital signatures help establish trust in the communication process and mitigate the risk of unauthorized access or manipulation of data.

4. Does one need to ensure that information is kept confidential? Or not altered during 2-way Communication?
Ans4:
Ensuring the confidentiality and integrity of information exchanged during two-way communication is imperative for maintaining the security of the system. Encryption techniques are employed to secure the transmission of sensitive information, such as OTPs, between the server and drivers. By encrypting data using robust encryption algorithms, the system prevents unauthorized access to confidential information and safeguards it from interception or eavesdropping. Additionally, digital signatures are used to verify the integrity of messages, ensuring that they have not been modified or tampered with during transit.

5. Which of these, viz. confidentiality, authentication, integrity and non-repudiation is/are relevant?
Ans5:
Several security concepts are relevant to the system's operation, including confidentiality, authentication, integrity, and non-repudiation. Confidentiality ensures that sensitive information remains protected from unauthorized access or disclosure, maintaining the privacy of personal data. Authentication mechanisms verify the identities of parties involved in the communication process, preventing unauthorized access and impersonation. Integrity mechanisms guarantee that data remains unchanged and unaltered during transmission, ensuring its reliability and trustworthiness. Non-repudiation mechanisms prevent parties from denying their actions or transactions, providing accountability and traceability for all communication activities.

Bonus Question:
Is date and time of communication important? If so how can that be obtained from a well-known server in a secure manner?
Ans:

the importance of date and time of communication, accurate date and time information is crucial for ensuring the timeliness, validity, and synchronization of license verifications. By obtaining this information from a well-known server in a secure manner, the system can establish a common reference point for timestamping communication events, preventing discrepancies or manipulation of timestamps. This ensures that the system operates based on accurate and synchronized time references, maintaining the integrity and reliability of communication processes.