Network Security A3

Soumya Mohapatra (2021103)
Harshit Pal (2021255)

Overview

1. The assignment required us to build an RSA based Certification Authority
2. Two Clients are provided which may communicate with each other until their certificates are valid.

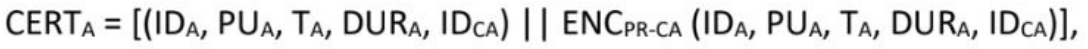
Assumptions:

1. Keys remain constant during the entire period and each node is aware of others key (Not a practical case, clients make their own key and enroll to CA)
2. Nodes port number are their ID.
3. C1 sends the messages C2 send replies

Certificate Format

Certificate Consists of the following:

1. Requestee ID (port no)
2. Requestee Public key
3. Time of issue
4. Duration
5. CA ID (port)
6. SHA256 hash (encrypted via CA private key)



$$CERT_A = [(ID_A, PU_A, T_A, DUR_A, ID_{CA}) \,||\, ENC_{PR\text{-}CA} (ID_A, PU_A, T_A, DUR_A, ID_{CA})],$$

System Overview for certificate retrieval and verification

1. The client requests for a certificate for a Node. Encrypts it request by CA public key
2. CA generates the certificate calculate the hash and encrypts it by its own private key. Since it is a asymmetric hash encryption the message send is non repudiable
3. CA sends the encrypted message to requester by encrypting it with Requesters public key.
4. Client decrpyts its message and hash using appropriate keys and compare the decrypted hash with client-side computed hash of the message. If the hashes are equal the message is valid.
5. The certificate remains valid till the duration after the issuing time.

System Specification

1. Keys are 8 digit long (these can be easily increased and kept short for readability purposes)
2. The system use block cipher for encryption uses N of the key as a reference of block size.
3. Encryption done on byte-wise.
4. SHA256 is used as hashing algorithm

Client-2-Client Communication specification

1. The Clients have each others keys until the certificates are valid. After which the keys are deleted.
2. To send message the sender first encrypts it with his private key (for verification) and then with receivers public key (for security).
3. Decryption happens by first decrypting by receiver private key and then sender's public key.