PROJECT PROPOSAL - CSE 664

1. Team Members :

- Arti Gupta (50170010)
- Aditya Nalge (50207629)

2. Topic :

Encryption System Implementing Threshold Cryptographic Protocols.

3. Project Description :

i. Security Objectives -

- Confidentiality.
- Authorization & Authentication of users involved.
- Non-repudiation.
- Data Integrity.
- Availability gets compromised since no user will be able to access the data until a threshold number of users access it together. However this adds additional layers of security.

ii. Plan for realizing the security objectives -

The basic concept of Threshold Cryptosystems is that multiple users 'U' can together share a common a secret say 'S'. However, none of the users U can learn anything about the secret S until a predefined threshold number of users i.e. 'T' are present. Even if T - 1 users work together, they cannot receive any information about the secret 'S'.

Thus, threshold cryptosystems are used when you want to distribute a single secret amongst multiple parties such that only all the party members together or only when a threshold number of party members are present that the secret can be recomputed. The concept of threshold is necessary because it acts as a backup in a scenario wherein a party members key is lost and as a result other party members can still retrieve the secret. It also provides security since even if a single party member's key is compromised, no information of the secret is revealed.

The two main encryption algorithms that can be used to implement Threshold Cryptosystems are:

- El Gamal - Used for public key cryptography and is an asymmetric key encryption algorithm.
- RSA - A public key encryption algorithm containing different private and public keys.

We plan to realize the various security objectives of our system using Cryptographic techniques. Confidentiality can be maintained by preventing unauthorized users from accessing the information. Non-repudiation can be implemented using digital signatures. Authorization and Authentication can be ensured by using a system which involves every user having a unique id and password to access the system. Data integrity can be verified using Hash functions and needs to be verified periodically.

iii. Expected Outcomes -

At the end of this project, we expect to have created a system which fundamentally is based on Threshold Cryptographic Protocols. The objective is to use a cipher technique by which a common public key can be used by multiple users to encrypt data. However, the key to decrypt the data would be different. Each user would hold a part of the secret and any number of users below the threshold cannot learn anything about the secret individually or by working together. The secret can be deciphered only when a threshold number of users decrypt it together.

4. References :

[1] Cornell - Threshold Cryptosystems - http://www.cs.cornell.edu/courses/cs754/2001fa/307.PDF

[2] https://www.dcl.hpi.uni-potsdam.de/teaching/cloudsec/presentations/threshold-cryptography.pdf

[3] https://en.wikipedia.org/wiki/ElGamal_encryption

[4] https://en.wikipedia.org/wiki/RSA_(cryptosystem)