(CS 890BN) PROJECT PROPOSAL

TOPIC : - THRESHOLD SECRET SHARE CRYPTOGRAPHY

Submitted By : Amal Majeed
200415928
Date : 21/09/2019

The aim of this project is to study the implementation of SSS (Shamir Secret Sharing Scheme) Algorithm proposed by Adi Shamir in his ACM publication *'How to share a secret'* [3] for a "multi-factor authentication" scheme as incorporated in the work by Vishnu Venukumar and Vinod Pathari [1] where the authors try to overcome the security hurdle of "shoulder surfing" in a public "Point of Sale(PoS) Terminal" secret password entry scenario. In their paper [1] , the authors describe "Multi-Factor authentication" as a form of "strong authentication which uses more than one information from a secret password , RFID , fingerprint etc" . One advantage of a "multi-factor authentication" is that even if one or more levels of the secrecy is compromised , depending on the complexity/ depth of the scheme, the stolen key information might not still be adequate to unlock the secret information, which is the main reason why several online services such as internet banking and email services employ multi-factor authentication. The key idea of implementation in the 'Multi-factor authentication by threshold cryptography" [1] was taken from Adi Shamir's [2][1] idea of dividing a secret data into 'n' distinct pieces called "shares" , or "secret shares" and distribute it among 'n' trusted sources and with any of the threshold 't' number of "shares" of the data the original piece of secret information can be retrieved back by Lagrange polynomial interpolation [4] , where 't' <= 'n' .

However, with a rising number of bot programs on the internet it is highly possible that a plaintext transfer of "shares" can compromise the security of the system to attacks from bots that can sniff out the transmission. This project aims to figure out the possibilities of adding on CAPTCHA or other forms of bot resistant secret transfer media which can reduce the vulnerabilities that computer bots can exploit in the system.

References

1. Venukumar, Vishnu., Pathari, Vinod. *'Multi-Factor Authentication using Threshold Cryptography'* , 2016 Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 21-24, 2016, Jaipur, India
2. *'Shamir's Secret Sharing'* Wiki (link:https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing)
3. Shamir, Adi (1979), *'How to share a secret'*, *Communications of the ACM*, **22** (11): 612–613, (link : https://doi.org/10.1145%2F359168.359176)
4. *'Lagrange Polynomial'* Wiki (link : https://en.wikipedia.org/wiki/Lagrange_polynomial)