International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Industrial Automation And Computing (ICIAC- 12th & 13th April 2014)

RESEARCH ARTICLE OPEN ACCESS

Secret Sharing Schemes: A Review

Miss. Reena S. Satpute*, Prof. Amit N. Thakare**
Department of Computer Science and Engineering, R.T.M.N.U. University, Wardha-442001
Email: reenasatpute@hotmail.com
Department of Computer Science and Engineering, R.T.M.N.U. University, Wardha-442001
Email: amu_thak@rediffmail.com)

ABSTRACT
The technique to hide a secret is needed in many situations. One might need to hide a password, an encryption Key, a secret recipe, and etc. Information can be secured with encryption, but the need to secure the secret key used for such encryption is important too. Consider, we encrypt our important files with one secret key and if that secret key is lost then all the important files will be inaccessible. Thus, secure and efficient key management mechanisms are required. One of them is secret sharing scheme (SSS) that allows to split the secret into several shares which will get distributed to all the participants. The secret can be recovered once these parties collaborate in some way. This survey paper will study these schemes and explain the need for the secret sharing and their security. Across the years, various schemes have been presented. This paper will review some of them varying from trivial schemes to threshold based ones.
Keywords **-** Secret splitting, Shamir's Secret Sharing Scheme, Threshold schemes

I. Introduction

The Secret Sharing Schemes (SSS) is one of the key management or establishment schemes invented separately in 1979 by both Shamir [1] and Blakey [8] as a solution to safeguard cryptographic keys. Secret sharing schemes are also used to protect other types of secrets, such as a secret recipe or a password to a bank vault, control access of nuclear weapons and others. We need these schemes because many cryptosystems that use a single master key have various vulnerabilities. For instance, if the master key is disclosed to the public by accident or by an attacker, this will compromise the entire system. Also, if the master key is lost, then all the other keys it protects become inaccessible. Additionally, if the owner of the master key turns out to be disloyal then all sensitive information will be leaked to the opponents [2].

In addition, these schemes are useful when we don't want to save the secret in a single place or when we don't trust a single person owning a certain secret. From these reasons comes the need for SSS. To see how SSS works in real life scenario consider a country that for various reasons does not want the access control of its nuclear weapon to be activated by a single person only[4]. Thus they can involve for example three participants, the President, Defense Minister and the Defense Ministry, where any two out of these three can gain control of the nuclear weapon.

II. Literature Survey

Since the inventions in late 1970s, secret sharing schemes have been thoroughly researched. Many different secret sharing schemes exist and thus secret sharing scheme can broadly categorized as follows:

1. Traditional Secret sharing scheme
2. Threshold Secret sharing scheme
3. Threshold Changeable Secret sharing scheme
4. Verifiable Secret sharing scheme

A Secret sharing is a technique for protecting sensitive data, such as cryptographic keys. It is used to distribute a secret value to a number of parts or shares that have to be combined together to access the original value. These shares can then be given to separate parties that protect them using standard means like memorize, store in a computer etc. Secret sharing is used in modern cryptography to lower the risks associated with compromised data. Sharing a secret spreads the risk of compromising the value across several parties [7].

1.1. Traditional Secret Sharing Scheme

Shamir [1] presented the first secret sharing method in1979. Secret sharing involves transmitting different shares in different channels. With a single share nobody can see the entire secret message. The general idea behind secret sharing is to distribute a secret to n different participants so that any k participants can reconstruct the secret, and any (k - 1) or less participants cannot reveal anything about the

secret. Such schemes are also known as (k, n) threshold-based scheme. For any secret sharing schemes it has the following two processes:

1.1.1. Distribution Process
This process input is the secret k that gets portioned into n number of shares S1, S2,...Sn that is privately delivered to the participants.

1.1.2. Reconstruction Process
It reconstructs the secret when a suitable set of shares is present using a certain algorithm.

1.2. Threshold Secret Sharing Scheme

These schemes are the first kind of schemes that were constructed individually by both Shamir who uses polynomial interpolation [1] and Blakley who uses finite geometry [8]. To share a secret we can split the secret and spread the pieces to all participants. In some schemes, reconstructing the secret needs combining all shares from participants, but this might not be practical since we might need the secret reconstructed by some of the participants and not all.

The reason is as follows:

Imagine if a country splits the access codes for its missiles among three officials and they found themselves in a dire need to access the missiles, but one of the officials is not present or he simply refuses to attack. Then, we need to have a different scheme where a subset of the participants can reconstruct the secret. These schemes are secure and do not require all n shares [4]. For example: Consider the Board of Directors of Defense ministry would like to protect missiles secret formula. The president of the company should be able to access the formula when needed, but in an emergency any 3 of the 12 board members would be able to unlock the secret formula together. This can be accomplished by a secret sharing scheme with k = 3 and n = 12, where 3 shares are given to the president, and 1 is given to each board member. These schemes are further classified depending in the size on the shares as:

1.2.1. Perfect Secret Sharing (PSS)
These schemes cannot allow the size of secret shares to become smaller than the size of the secret.
1.2.2. Ramp Secret Sharing (RSS)
These schemes achieve the goal of reducing the size of the shares, but at the cost of some degraded protection on the secret.

1. 3. Threshold Changeable Secret Sharing Scheme

Threshold Changeable secret sharing scheme was invented by the scientist Wang and Wong for changing thresholds in the absence of secure channels after the setup of threshold secret sharing schemes[4]. Initially, we construct a perfect (t, n) threshold scheme that is threshold changeable to t which is optimal with respect to the share size. But these threshold changeable schemes along with most previously known schemes turn out to be insecure under the collusion attack of players holding initial shares [9].

1.4. Verifiable Secret Sharing Scheme

This scheme was first introduced to overcome the problem of dishonest dealers. VSS schemes lets the participants verify that their shares are consistent, thus they can properly reconstruct the secret. To get a clear idea about how these schemes work, let us assume a dealer Trent sends shares to Alice, Bob, Carol and Dave. The only way they can be sure they have a valid share is to reconstruct the secret, but it may happen that Trent sent a bogus share to Bob or Bob received a bad share as a result of a communication error. VSS schemes allow these participants to validate their shares without the need to reconstruct the secret [5].

It is designed to resist an adversary who can corrupt the dealer and some of the participants.VSS requires an additional algorithm called verify that allows participants to verify their shares before any reconstructing attempts [6].

III. Comparison of Secret Sharing Schemes

Table1: Comparison table for Secret sharing scheme

Type	Sha-res	Represen-tation	Reconstr-uct	Pros
Traditional SSS	n	k=n	k=n	It is very effective for less number of participants
Threshold SSS	n	k, n	k out of n	It allows only few shares (threshold) to reconstruct the secret
Threshold Changeable SSS	n	t, n	t=t'	It allows to change the threshold in the absence of channel
Verifiable SSS	n	k, n	k, n	It is used as a solution to cheating problems

IV. Conclusion

Security is an important issue in any application. To provide the security, authentication plays very important role. Authentication is provided through the secret sharing schems. This review paper explains the methods based on the secret sharing schemes.

REFERENCES

[1] Mohammed Khasawne, Mohammad Malkawi, Omar Al-Jarrah, Thaier S.Hayajneh, A Biometric-Secure e-Voting System for Election Processes proceeding of IEEE Transaction, 5 International Symposium on Mechatronics and its Applications (ISMA08), Amman, Jordan, May 27-29, 2008

[2] Sanjay Saini and Dr. Joydip Dhar, An eavesdropping proof secure onlinevoting model proceeding of IEEE Transaction, International Conferenceon Computer Science and Software Engineering, 2008, pp. 704-708.

[3] Cesar R. K. Stradiotto, Angela I. Zotti, Claudia O. Bueno, Sonali P. M. Bedin, Hugo C. Hoeschl and Tania C. D. Bueno, Thiago P. S. Oliveira, Web 2.0 An Efficient and secure method for wireless sensor network proceeding of IEEE Transaction, 2010,pp. 1138-1142.

[4] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Babhuiya and Sukumar Nandi, Wireless sensor network System Powered By Sensor Security Using Steganography, proceeding of IEEE Transaction, Second International Conference on Emerging Applications of Information Technology, 2011,pp. 288-291.

[5] Chinniah Parkodi, Ramalingam Arumuganathan and Krishnasamy Vidya, Multi-authority Electronic Voting Scheme Based on Elliptic Curves, proceeding of IEEE Transaction, International Journal of Network Security, Vol.12, No.2, Mar. 2011, pp. 84-91.

[6] Haijun Pan, Edwin Hou, and Nirwan Ansari, E-NOTE: An E-voting System That Ensures Confidentiality and Voting Accuracy, in IEEE, ICC Communication and Information System Security Symposium, 2012,pp. 825-829.

[7] Anida Sarajlic, Narcis Behlilovic, Irma Sokolovic, A Modular Concept of E-voting System that Protects User Privacy Using Password Distributionproceeding of IEEE Transaction, 18th International Conference on System, Signal and Image Processing, IWSSIP, June 2011.

[8] Shamir and Blakey, An Anonymous and Efficient secret sharing Scheme, in proceeding of IEEE Transaction, 18th International Conference on e-Commerce in Developing Countries with focus on e-Security. April 2013.

[9] Honady Hussien and Hussien Aboelnager, Design of a Secured E-voting System, proceeding of IEEE Transaction, 2013.

[10] Adi Shamir, How to Share a Secret, in communications of ACM, Vol.22, no.11, 1979, pp. 612-613.