ISSN 2319-524X

Analyzing Proactive Secret Sharing Schemes

Sonali Patil
Assistant Professor
Computer Dept. PCCOE, Pune
sonalimpatil@gmail.com

Nikita Rana
Student
Computer Dept. PCCOE, Pune
22.rananikita@gmail.com

Dhara Patel
Student
Computer Dept. PCCOE, Pune
dhara.patel205@gmail.com

Prajol Hodge
Student
Computer Dept. PCCOE, Pune
Prajolhodge24@gmail.com

Abstract: **There are circumstances where an action is required to be executed by a group of people. The idea of secret sharing is to divide a secret into pieces called shares, which are then distributed amongst users by the dealer. The shares provided to the participants are generally forever. But the need of the applications is to periodically renew the shares for the same secret to add more security. Also to add new participants enrolling feature is necessary and sometimes dis-enrollment is required to remove the dishonest participants. For example, to transfer money from a bank a manager and a clerk need to cooperate. A ballistic missile should only be launched if three officers authorize the action. Proactive secret sharing adds more security to all kind of such applications. The goal of the pro-active security scheme is to prevent the adversary from learning the secret or from destroying it. The intent of this paper is to provide an analysis of such proactive secret sharing schemes. The comparative study shows there is a need of better proactive secret sharing schemes.**

Keywords*: Secret Sharing, Network security, Extended Capabilities, Cryptography*

I. INTRODUCTION

In communications networks that require security, it is important that secrets be protected by more than one key. In commercial, medical and military systems security of sensitive information is essential and is of primary concern. Needless to say, it is also important for any information process to ensure data is not being tampered. To ensure the integrity and secrecy of the protected information encryption methods are one of the popular approaches. Public key encryption is a powerful mechanism for protecting the confidentiality of secure information. In those methods, secrets can be protected by more than one key. However, single-point-failure term is one of the critical problems faced in encryption techniques.

For example,

- The secret information cannot be recovered if the decryption key is lost.
- The encrypted content is corrupted during the transmission.
- Backup copies are created to protect cryptographic keys from loss or corruption.

The problem is, the greater the number of copies made, the greater the risk of security exposure, and smaller the number of copies made, the greater the chance that all of them are lost. To address these reliability problems, a secret sharing scheme (SSS) is a good alternative to remedy these types of vulnerabilities. Secret sharing schemes allows improving the level of protection without increasing the risk of exposure.

Secret Sharing is a scheme in which a secret is divided into pieces called shares, which are then distributed amongst users by the dealer. Only certain groups (authorized subsets of participants) can reconstruct the original secret. More formally a Secret Sharing Scheme (SSS) is a method whereby n pieces of information called shares or shadows are assigned to a secret key K in such a way that: i)The secret key can be reconstructed from certain authorized groups of shares and ii) The secret key cannot be reconstructed from unauthorized groups of shares. But in some circumstances, secret sharing need to be more flexible like provide proactive features such as to enroll and dis-enroll of shareholders, recover lost or corrupted shares and periodically renew shares.

The rest of the paper is organized as follows. In Section II some definitions are discussed. Section III covers proactive secret sharing schemes. In section IV performances of these schemes based on various parameters like ideal, perfect, enrollment, disenrollment, updation are analyzed. Finally in section V, we summarize this survey based on their comparative results.

II. SOME DEFINITIONS

Formal foundation of secret sharing was formulated using the information theory. Two important concepts were defined based on information rate: ideal and perfect schemes.

Information Rate: The information rate was studied by Stinson [1]. It is a measure of the amount of information that the participants need to keep secret in a secret sharing scheme. The information rate for a particular shareholder is the bit-size ratio (size of the shared secret) / (size of that user's share). The information rate for a secret sharing scheme itself is the minimum such rate over all participants [2] [3]. The efficiency of a secret sharing scheme is measured by its information rate.

Ideal Secret Sharing: Secret sharing schemes with information rate 1 are called ideal [4]. Scheme is ideal if share has the same length as secret. Ideal property can be thought as efficiency.

Perfect: A perfect threshold scheme is a threshold scheme in which knowing only (t - 1) or fewer shares reveal no information about Secret S whatsoever, in the information theoretic sense [2] [3].

III. PROACTIVE SECRET SHARING SCHEMES: LITERATURE SURVEY CRUX

Proactive Secret Sharing:

The Secret Sharing scheme assumes long-lived shares; however the protection provided by this scheme may be insufficient. The security in a system that is exposed to attacks and break-ins might become exhausted; several faults might occur such as Secrets can be revealed, Shares can gradually be corrupted / compromised, Hardware failure or damage, for example reboot, power failures etc.The goal of the pro-active security scheme is to prevent the adversary from learning the secret or from destroying it, in particular any group of t non-faulty shareholders should be able to reconstruct the secret whenever it is necessary.Proactive secret sharing scheme (PSSS) was introduced to improve security through periodic executions. With no PSSS, using an (t, n)-threshold secret sharing scheme, SSS can tolerate up to t-1 compromised shares. Given enough time, a hacker may be able to compromise enough shares (t or more) to gain the secret. PSSS is a scheme that allows generating new set of shares for the same secret from the old shares without reconstructing the secret. Using PSSS, all the shares are refreshed so that old shares become useless. Thus, an adversary has to gather at least t shares between two executions of PSSS. The secret remains confidential if fewer than t shares were compromised from the start of one PSSS to the end of the next PSSS. The goal of the pro-active security scheme is to prevent the adversary from learning the secret or from destroying it, In particular any group of t non-faulty shareholders should be able to reconstruct the secret whenever it is necessary.

The term pro-active refers to the fact that it's not necessary for a breach of security to occur before secrets are refreshed, the refreshment is done periodically (and hence, proactively).

The core properties of pro-active secret sharing:

- To renew existing shares without changing the secret, so that previous exposures of shares will not damage the secret (old shares will become useless).
- To recover lost or corrupted shares without compromising the secrecy of the shares.
- Reconstruction of Lost / Corrupted Shares

Pro-active Model requirement

- An adversary can reveal at most t-1 shares in any time period (where t-1<n/2. this guarantees the existence of t honest shareholders at any given time). This time period should be synchronized with the share-renewal protocol.
- Authenticated broadcast channel.
- Authenticated and secret communication channels between each two participants.
- Synchronization: the servers (shareholders) can access a common global clock so that the protocol can be applied in a certain time period.
- Shares can be erased: every honest server (shareholder) can erase its shares in a manner that no attacker can gain access to erased data.

Active & Passive attacks

A secret sharing system is still quite vulnerable when a dynamic adversary determines to break into the system before the lifetime of the secret expires. Ben-Or et al. [5] discussed a general theory for the distributed fault tolerance systems and presented some possible solutions to avoid such attacks. Among many different classifications of adversary attacks, one of the most notable ones is to classify the attacks as:

- Passive adversary attacks
- Active adversary attacks.

Where passive adversary attacks are primarily resulting in spoofing data without modification or corruption to the data. In contrast to the passive adversary attacks, the active

ISSN 2319-524X

adversary attacks are much more malicious wherein the adversaries can persistently attempt to infiltrate a system, and/or to damage or destroy data already stored in the system. We are briefly describing some PSSS below:

A) Shamir's Secret Sharing Scheme

A PSSS based on Shamir [6] secret sharing scheme is explained in [1]. Shamir [6] developed the idea of a (k, n) threshold-based secret sharing technique ($k \leq n$). The technique is to construct a polynomial function of order ($k - 1$) as,

$$f(x) = d_0 + d_1 x + d_2 x^2 + \ldots + d_{k-1} x^{k-1} \pmod{p},$$

where the value d_0 is the secret and p is a prime number. The secret shares are the pairs of values (xi, yi) where yi = f(xi), $1 \leq i \leq n$ and $0 < x1 < x2 \ldots < xn \leq p - 1$. The polynomial function f(x) is destroyed after each server Pi possesses a pair of values (xi, yi) so that no single server knows what the secret value d_0 is. In fact, no groups of ($k - 1$) or fewer secret shares can be used to discover the secret d_0. On the other hand, when k or more secret shares are available, we can set up at least k equations yi = f(xi) with k unknown parameters di's. The unique solution d_0 can be solved. Also, a Lagrange interpolation formula [6] is commonly used to solve the secret value d_0 as the following formula

$$d_0 = \sum_{i=0}^{k} \left(\prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{-x_j}{x_i - x_j} \right) y_i \pmod{p}$$

where (xi, yj) are any k shares for $1 \leq i \leq k$. Shamir's SSS is regarded as a perfect SSS because knowing ($k - 1$) linear equations cannot expose any information about the secret.

We assume an initial stage where a secret *s* is encoded into *n* shares using Shamir's secret sharing scheme. Each participant holds his/her share *f(i)* for some *t-1* degree polynomial *f(x).* After the initialization, at the beginning of each time period, all honest servers/shareholders trigger an update phase in which the servers perform a share renewal protocol.

Each *i'th* shareholder receives the following shares: $P_1(i), \ldots, P_n(i)$ (including his own made share $P_i(i)$) and computes his/her new share by adding his old share- *f(i)* to the sum of the new *n* shares. Mathematically speaking:

$$h(i) = f(i) + \sum_{c=1}^{n} P_c(i)$$

B) Herzberg's [7] Proactive Secret Sharing scheme

Herzberg [7] proposed the PSS scheme based on the Shamir SSS to address the problem of passive and active attacks. This method periodically renews the shares (without reconstructing the secret) so that it prevents an adversary from gaining the knowledge of the secret before it expires. To counter active adversary attacks, Herzberg et al. combined the ideas of the VSS technique to prevent dishonest participants (or compromised participants by active adversaries) from refusing to change the shares during the renew process, or introduce invalid secret shares.

To periodically update shares is an effective way to protect a secret from being revealed by adversary attacks. Herzberg et al. developed a PSS technique for the Shamir's method. After the initialisation of Shamir's SSS, at the beginning of every time period, all 'honest' servers can trigger an update phase in which the servers perform a share renewal protocol. The shares computed in period t are denoted by using the superscript t, i.e., (xi, $f^t(x_i)$), t = 0, 1, ... We know that the secret d0 at time ($t - 1$) is

$$d0 = f^{(t-1)}(0).$$

The algorithm is to construct a new ($k - 1$) random polynomial function at each updating phase as,

$$\delta(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} \pmod{p}, \qquad (1)$$

where $\delta(0) = 0$ so that $f^t(0) = f^{t-1}(0) + \delta(0) = d_0 + 0 = d_0$.

Since the δ(x) function does not have a constant term, consequently, any group of k or more servers can still compute d_0 by contributing their new shares. However, a combination of k shares using past and present shares cannot be used to reconstruct the secret. As a result, the secret is protected from being revealed by the passive adversaries.

C) Proactive Secret Sharing Scheme using matrix projection

Lie Bai [8] proposed a secrete sharing scheme for images. Lie Bai and Zou [9] proposed a secret sharing scheme which supports proactive secret sharing with enrollment, disenrollment, periodically renewal of shares. There is no need to expose the secret and other shares while providing a new share to new enrolled shareholder. Also he introduced a new, secure and distributed proactive secrete sharing scheme using the matrix projection method. This scheme is different than Hertzberg's scheme. After the shares are updated, any k shares of past and present shares cannot be used to reveal the secret matrix. This method looks after the protection against the passive attacks.

IV. PERFORMANCE ANALYSIS OF SCHEMES

Few secret sharing schemes are considered for comparative study based on some parameters. The following table summarizes that:

Parameters / Schemes	Ideal	Perfect	Computational Complexity	Functionality				
				Enrollment	Disenrollment	Reconstruction of Lost/ Corrupted Shares	Updation	
							Active	passive
Shamir	Yes	Yes	Less	Yes	Yes	No	No	Yes
Herzberg	Yes	No	Less	Yes	Yes	No	No	Yes
Lie Bai	Yes	Yes	More	Yes	Yes	Yes	No	Yes

Table I. Comparison of secret sharing schemes on the basis extended capabilities.

V. CONCLUSION

In this paper we have tried to analyze proactive secret sharing schemes and their mapping with suitable applications. Proactive secret sharing schemes with these pro-activeness draw our attention, and we are also eager to know their specific implementation methods. Also the performances of existing proactive secret sharing schemes is evaluated on some parameters like complexity measure, perfect, ideal, flexible, enrollment, disenrollment, updating share. Table I. Comparison of secret sharing schemes on the basis extended capabilities. There is a need to add extended capabilities like proactive secret sharing in applications. The scheme should more secure and efficient. This should be performed without, of course, any information-leak or any secret change. Unfortunately, in a normal proactive secret sharing, new members can't enroll the system according to the need of actual circumstance because the normal proactive secret sharing has no this ability.

VI. REFERENCES

[1] D. R. Stinson, "Cryptography: Theory and Practice", CRC Press, Boca Raton 1995.

[2] Menezes, A., P. Van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996, pp. 524-528

[3] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," vol. IT-29, no. 1, pp. 35–41, Jan. 1983.

[4] P. Paillier, "On ideal non-perfect secret sharing schemes," in Security Protocols Workshop, 1997, pp. 207–216.

[5] Ben-Or, M., Goldwasser, S. and Wigderson, A. (1988) 'Completeness theorems for non-cryptographic faulttolerant distributed computation', *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, 2–4 May, Chicago, Illinois, pp.1–10.

[6] Shamir, A., "How to Share a Secret", Communications of the ACM, vol.22, no.11, 1979.

[7] Herzberg, A., Jarecki, S., Krawczyk, H. and Yung, M. (1995) 'Proactive secret sharing or: how to cope with perpetual leakage', in Don Coppersmith (Ed.): *Advances in Cryptology – Crypto '95*, August, Santa Barbara, CA, pp.339–352.

[8]Lie Bai ,"A Reliable (*k*, *n*) Image Secret Sharing Scheme", 2006

[9] Bai, L. and Zou, X. (2009) „A Proactive Secret Sharing Scheme in matrix projection method", Int. J. Security and Networks, Vol. 4, No. 4, pp.201–209.

[10] Zhengjun Cao, Olivier Markowitch, "Two Optimum Secret Sharing Schemes Revisited", International Seminar on Future Information Technology and Management Engineering, 2008 IEEE, p. 157-160.