Secret Sharing Scheme for Collaborative Access System

Rashidah Kadir
Mohd Aizaini Maarof
Information Security Group
Faculty of Computer Science & Information System
Universiti Teknologi Malaysia
Skudai, 81310, Johor.
{ rashidah, maarofma} @fsksm.utm.my

Abstract- **This research investigate the concept of secret sharing scheme based on Shamir's secret sharing. The goal of this research is to implement secret sharing scheme for collaborative access system which are ideally suited to application in which a group of mutually suspicious individuals with conflicting interest must cooperate. In (q,n) secret sharing, a quorum, q of a group of n users are allowed to access the system by having the quorum reconstruct a secret(key), less than quorum can gain no information. Lost or stolen share still ensure the security of resources.**

Keywords: *Computer Supported Cooperative Work, Groupware. Access Control and Secret Sharing Scheme.*

I INTRODUCTION

Innovations of recent technology in computing, user interfaces and computer networking are enhancing the development of computer facilities that enable people to work together more efficiently and conveniently [7]. The field that deals with the development of such facilities is generally termed *Computer Supported Collaborative Work* (CSCW). The purpose of CSCW is to provide computer support that facilitates co-operation between users.

The increased attention on CSCW brings with it a need for security in the development of group applications. Much work has been done on the technological aspects of CSCW: the problems of how one actually provides computer support for co-operation [8]. However, the aspect of information security of CSCW technology has not received much attention, which encourages research on the security issues in CSCW [16].

The lack of security in general in CSCW has been raised by Teufal et *al.*[16]. This security deficiencies in CSCW system can be handled by incorporating security services, based on following security requirements [10]: Preventing unauthorised users accessing or participating in the CSCW system, ensuring against disclosure of information flow in the CSCW system and ensuring against disclosure of information stored in the CSCW system. In this paper we are proposing the implementation of secret sharing scheme for secure access control services for synchronous distributes collaborative system operating over the World Wide Web. The paper extend the work done by Maarof [10] by extending the External Security Layer (ESL) that provides a secure access control process for collaborative system. The used of World Wide Web (WWW) across the Internet has increased tremendously, both in terms of number of users and the amount of activity. It popularity provides uniform access to applications, its platform independence allows uniform user-interfaces for applications. It offers a great deal of potential for the developers of collaborative technologies, both as an enabling infrastructure and a platform for integration with existing end-user environments [1].

Secret sharing schemes are one of the most important primitives in distributed system and useful in any important action that requires the concurrence of several designated people to be initiated, also used in the management of cryptographic keys and multi-party secure protocols [3][4]. The secret sharing scheme implemented based on Shamir's Secret Sharing [13]. The goal of this research is to implement secret sharing scheme for collaborative access system which are ideally suited to application in which a group of mutually suspicious individuals with conflicting interest must cooperate. In (**q**,**n**) secret sharing, a quorum, **q** of a group of **n** users are allowed to access the system by having the quorum reconstruct a secret(key), less than quorum can gain no information.

II BACKGROUND

Shen and Dewan [15], Kanawati & Riveill [9], and Coulouris & Dollimore [5] in their research focus on access control issues for collaborative environments. Shen & Dewan [15] in their work stated that there has been much research done in computer applications for facilitating collaboration among multiple distributed users but there has been relatively little works done in

controlling access to the collaboration. Almost all available collaborative systems or groupware applications provide all collaborators or users with the same rights [9][15].

Secret Sharing Schemes

Secret sharing schemes were first introduced by Shamir [13] and Blakley [2] in 1979, and subsequently have been studied by numerous other authors and researcher. A secret sharing scheme is a system that is designed to protect a secret piece of information among a group of users in such a way that only certain subsets of users can jointly reconstruct the secret, whereas other subsets of users can ideally not obtain any information about the secret. The collection of subsets that can access the secret is called the access structure of the secret sharing scheme.

Shamir's Secret Sharing Scheme

In general (**q,n**) threshold scheme or secret sharing problem has the following charecteristic [13] :

1. A secret S is divided into n pieces, or shares;
2. Knowledge of quorum **q** or more allows S to be easily computed;
3. Knowledge of **q**-1 or less pieces reveals no information about S.

There are several useful properties of the secret sharing compared to mechanical locks and keys solution as :

- The size of each piece does not exceed the size of original data.
- When q is kept fixed, Si pieces can be dynamically deleted or added without effecting the other D.
- Si pieces are easy to change without changing the original data, S.
- Hierarchical access. Instead of giving one share to everyone, prioritize people according to authority [12].

Selberg [12] describes that in Shamir's original protocol, a Dealer, the person who knows the secret, creates a polynomial **f(x)** of the form:

$$f(x) = x^q + a_{q-1}x^{q-1} + \cdots + a_1 x + S \pmod p$$

where the coefficients $\mathbf{a_1 \ldots a_{q-1}}$ are chosen independently from [0, **p**). S is the secret and **p** is a large public prime.

The Dealer sends to each participant $\mathbf{C_1 \ldots C_n}$ **f(i)** (assume that the participants know their index). Hereafter, we will refer to **f(i)** as $\mathbf{C_i}$'s share **s** . When **q** participants desire to recompute the secret, they exchange their shares with each other. Once they have **q** shares , $\mathbf{s_1 \ldots s_q}$ they can create **q** equations. To find S , they need only solve for S and each $\mathbf{a_i}$ in the following system of equations:

$$\begin{aligned} f(s_1) &= s_1^q + a_{q-1}s_1^{q-1} + \cdots + a_1 s_1 + S \pmod p \\ f(s_2) &= s_2^q + a_{q-1}s_2^{q-1} + \cdots + a_1 s_2 + S \pmod p \\ &\vdots \\ f(s_q) &= s_q^q + a_{q-1}s_q^{q-1} + \cdots + a_1 s_q + S \pmod p \end{aligned}$$

where **p** and each $\mathbf{f(s_i)}$, $\mathbf{s_i}$ are known.

To solve for S and $\mathbf{a_1 \ldots a_{q-1}}$, all that is required is to solve for **q** unknowns with **q** equations in a modulo field. In matrix form (**u** = **Mv**, where **u** and **M** are known) this is:

$$\underbrace{\begin{bmatrix} f(s_1) \\ f(s_2) \\ \vdots \\ f(s_q) \end{bmatrix}}_{\text{known}} = \underbrace{\begin{bmatrix} s_1^q & s_1^{q-1} & \cdots & s_1 & 1 \\ s_2^q & s_2^{q-1} & \cdots & s_2 & 1 \\ & \vdots & & & \\ s_q^q & s_q^{q-1} & \cdots & s_q & 1 \end{bmatrix}}_{\text{known}} \underbrace{\begin{bmatrix} a_{q-1} \\ \vdots \\ a_1 \\ S \end{bmatrix}}_{\text{unknown}} \pmod p$$

All that is needed to solve for v (and thus S) is a simple matrix inversion modulo p and multiplication.

Proof of Correctness

A participant with **q** – 1(or less) shares can gain obsolutely no information about the secret.

Proof:Assuming that a participant does have shares, he can create the following:

$$\begin{aligned} f(s_1) &= s_1^q + a_{q-1}s_1^{q-1} + \cdots + a_1 s_1 + S \pmod p \\ f(s_2) &= s_2^q + a_{q-1}s_2^{q-1} + \cdots + a_1 s_2 + S \pmod p \\ &\vdots \\ f(s_{q-1}) &= s_{q-1}^q + a_{q-1}s_{q-1}^{q-1} + \cdots + a_1 s_{q-1} + S \pmod p \end{aligned}$$

To find , he has to solve for unknowns with only **q** – 1 equations. The best he can do is create an equation for with one degree of freedom, which gives no information about the actual value of S.

III RESULT AND DISSCUSION

Threshold(3,5) are chosen in the system development based on literature where there are many researchers [12][6] used this good combination. In general, the threshold depends on total number of participant involved in the collaborative system.

In this scheme the dealer selects at polynomial of degree (q-1) over f(x). The polynomial has the following form :

$$f(x) = x^3 + a_1x^2 + a_2x + S$$

where the coefficients a_i for i = 0,....k-1 are chosen randomly and uniformly from GF(x). The secret key is S = f(0). First the secret is split into five parts, with any three parts sufficient to reconstruct it. The reconstruct secret will be compared with the original before access permission is granted to users. The following example illustrate the secret reconstruction process:

Assuming that the secret S is 13 and the polynomial has created:

$$f(x) = x^3 + 11x^2 + 4x + S \pmod{17}$$

and has distributed the following point to node1, node2 and node3 :

node1 : (1,12) node2 : (2,5) node3 : (3,15)

Normal substitution would result in the following equations:

$$\begin{aligned} 12 &= 1 + a + b + S \pmod{17} \\ 5 &= 8 + 4a + 2b + S \pmod{17} \\ 15 &= 27 + 9a + 3b + S \pmod{17} \end{aligned}$$

which translates into the following matrix form :

$$\begin{bmatrix} 11 \\ 14 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 4 & 2 & 1 \\ 9 & 3 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ S \end{bmatrix} \pmod{17}$$

which results in [a, b, S] = [11,4,13] using Backward Substitution Method.

There are two modules in the development which based on Shamir's secret sharing scheme algorithm.

- The first is called the Dealer module, responsible in generating and distributing shares among the users(client) of collaborative system.

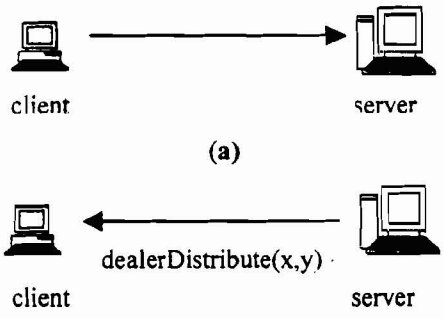

Figure 3.1 : Dealer process

Figure 3.1(a) shows the user request a share from Dealer(server) by sending his user ID. While the Combiner receive the request from users it will send a share consists two value, x and y(Figure 3.1(b). Shares are transferred as an object and stored in array(vector).

- The second is called the Combiner module that collects shares from the users and recompute or reconstruct the secret only for set of shares belonging to the access structure using matrix. The combiner takes shares from the participants (Figure 3.2(a)) and determines F(x) by Lagrangian interpolation. This always succeeds if the combiner has at least q different shares, but fails if the number of shares is less than q (Figure 3.2 (b)).

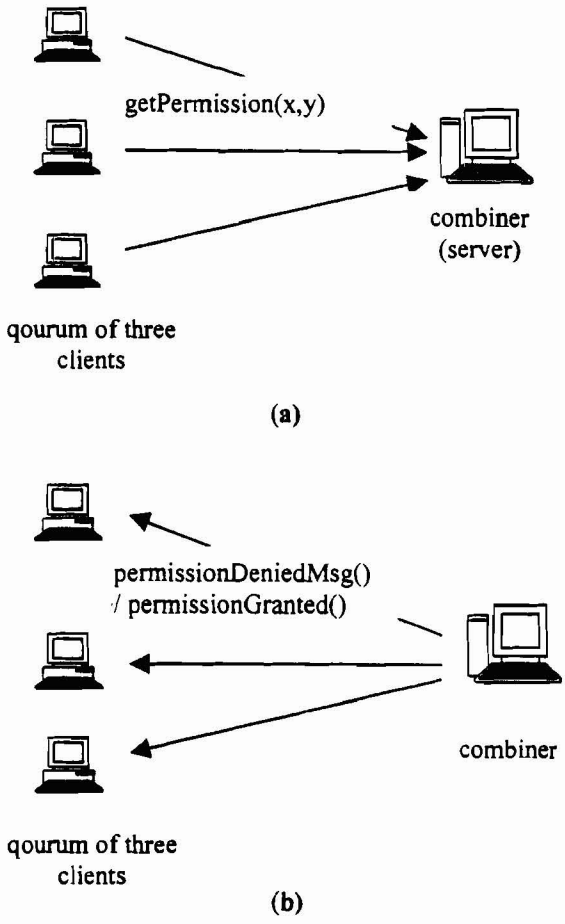

Figure 3.2 : Combiner process

Each participant holds their share of the same "weight". In other words, all participants are equal in their ability to recover secret and access the groupware. By implementing the secret sharing scheme as a access control mechanism make a groupware system more reliable and secure[12]. There are two level of authorisation checking. First, only authorised users can get a share which can be determine from the user ID. Second, reconstructing secret process can be a joint authorisation process.

Possibility for intruder get access into the system is small because they need to have three copies of shares in order to reconstruct the secret. So if one share are fall into intruder hand, resources and information of the system are still safe. Secret sharing scheme also make access control process flexible, with few different set of quorum can reconstruct the secret.

Key management is the set of techniques and procedures supporting the establishment and maintenance of keying relationship between authorised parties [11]. In secret sharing scheme, moderator generate the secret (key) and distribute the shares among the users. Each user has her/his own share which is used to reconstruct the secret with another two users. After secret reconstruction process, combiner will compare the secret with an original secret before an access permission is granted to the users. If the number of users is less than three, they have to wait for other users to fulfill the secret reconstruction requirement. Meanwhile, if the number of users is greater than the number of quorum, user is allowed to reconstruct the secret directly with any two users who had already granted an access.

IV CONCLUSION

Future work on collaborative access system and secret sharing scheme concentrates in overcoming the constraints and limitations[12]. They are :

- *Hierarchical access.* Instead of giving one share to every groupware users, another logical approach in deploying secret sharing scheme is to rank the access according to authority. In a business for example, we can give the CEO q shares, for each member of the board q/2 shares and for each manager q/3 shares. Thus rather than requiring q users to convene, all that is necessary is to gather users whom together have q shares .
- *Share encryption.* If anything happen during the transmission between client and server, intruder cannot get an original value of share.
- *Smart card.* To store the quorum complement with Authentication Protocol.

The implementation of the secret sharing scheme as a access control mechanism make a groupware system more reliable and secure. Possibility for intruder get access into the system is small because they need to have three copies of shares in order to reconstruct the secret. So if one share are fall into intruder hand, resources and information of the system are still safe.

As a conclusion the implementation of the secret sharing scheme into the collaborative system extend the current technology of the groupware by enhancing the access control process.

REFERENCES

[1] Bentley, R., Horstmann, T., Sikkel, K., and Trevor, J. (1995), "Supporting Collaborative Information Sharing with the World Wide Web: The BSCW Shared Workspace System", *4th International WWW Conference*, Boston, MS, U.S.A, December 1995.

[2] Blakley, G.R. (1979). "Safeguarding cryptographic keys." AFIPS Conference Proceedings, 48, 313-317.

[3] Blundo, C., De Santis, A., and Vaccaro, U. (1996), "Randomness in Distribution Protocols", Information and Computation, 131(2):111-139.

[4] Capocelli, R. M., De Santis, A., Gargano, L., and Vaccaro, U. (1993), "On the size of shares for secret sharing schemes", Journal of Cryptology, 6(3):157-167.

[5] Couloris, G. & Dollimore, J. (1994). "Security Model for Cooperative Work." Technical Report 674, Department of Computer Science, Queen Mary and Westfield College.

[6] CST, CST(Crypto Systems Toolkit Developer's Guide) (1999). "Shamir's Secret Sharing in CST." at http://www.baltimore.com.product

[7] Eltoweissy, M. Y (1993), "A framework for data sharing in computer-supported co-operative environments", Ph.D., Old Dominion University, U.S.A.

[8] Foley, S. N., and Jacob, J. (1995), "Specifying Security for CSCW Systems", *Eight IEEE Computer Security Foundations Workshop*, June 13-15, 1995, IEEE Computer Science Press, pp. 136-45.

[9] Kanawati, R. and Reveill, M. (1995). "Access Control Model for Groupware Applications." HCI'95 People and Computer, G. Allen, J. Wilkkinson et P, Wright (ed), 66-71 (Adjunt Proceeding), School of Computing and Mathematics, University of Huddersfield-UK.

[10] Maarof, M. A. (2000), " Integrating Security Into Computer Supported Cooperative Work", Ph.D Thesis, Aston University, United Kingdom.

[11] Menezes, A. J., van Oorschot, P. C. and Vanstone, Scott A. (1997). Handbook of Applied Cryptography, London : CRC Press.

[12] Rashidah Kadir(2000), "Secret Sharing Scheme for Collaborative Access System" M. Sc. Computer Science, Universiti Teknologi Malaysia, Malaysia.

[13] Selberg, E. W. (1994), "How to Stop a Cheater: Secret Sharing with Dishonest Participation", Thesis for Senior Honors Research Program, School of Computer Science, Carnegie Mellon University.

[14] Shamir, A. (1979), "How to Share a Secret", Comm. ACM, Vol. 22, Num. 11.

[15] Shen, H. H. and Dewan, P (1992), " Access Control for Collaborative Environments", Proceeding of ACM CSCW '92, pp. 51-58.

[16] Teufal, S., Eloff, J. H. P., Bauknecht, K., and Karagiannis, D. (1995), "Information Security Concepts in Computer Supported Cooperative Work", Norman Revell and A. Min Tjoa (ed.), In *Proceedings of 6th International Conference on Database and Expert System Application*, September 1995, Berlin Springer Verlag, pp. 621-631.