An Improvement of the Design of Integrating Subliminal Channel with Access Control

Chin-Chen Chang and Chia-Chi Wu

Abstract—**Recently, Lee and Yang proposed a subliminal scheme which employs an access control in a hierarchy. In their scheme, chief users use a one-way hash function to compute their subordinates' secret keys with low computation efficiency. And we also find some drawbacks, which are potential loopholes of the security. In this paper, we will show that their scheme suffers inside malicious user attack. And, accordingly, we will present an improved scheme to enhance the security against this flaw.**

Index Terms—**Access control, digital signature, subliminal channel, user hierarchy**

I. INTRODUCTION

A subliminal channel is a secret channel, through which messages are delivered between a sender and an authorized receiver. Meanwhile, not any other users or interceptors will notice this secret communication, and therefore it is called "information hiding". It can be applied in espionage activity or secret communication. Simons first put forth the concept [17] of a subliminal channel and hid information [18] in DSA [13], and then many researches [5, 8, 10] made improvement on Simons's scheme [18] in terms of security and efficiency.

Access control is an information security mechanism, which can be implemented in a hierarchical organization or company. Higher level users can access all his/her subordinates' messages, while subordinates can not retrieve back their superiors' messages. Many researchers have made great effort on this topic recently. Any user can use his/her assigned secret key to compute the keys of all user classes in lower hierarchies, and thus give access privileges. Moreover, these schemes [1, 2, 21] prevent the possibility of users collaborating to compute a key of which they are not entitled. There were some related works on this topic. Tsai and Chang [19] designed a dynamic access control scheme, afterward Chang et al. [4] improved this scheme to implement in a partially ordered user hierarchy; some researches[3, 6] focused on weaknesses discussions of the access control schemes; and Hwang et al. [7] proposed an access control scheme with time constraint property, etc.

Recently, Lee and Yang proposed a subliminal scheme which employs an access control in a hierarchical group [11] such that a chief receiver needs not maintain many secret keys to get all his/her subordinates' messages. In their scheme, the chief users use one-way hash function such as MD5 [15] or SHA [13] to compute their subordinates' secret keys with low computation advantage. However, we still find some drawbacks, which can affect security of the scheme.

In this paper, we will show the drawbacks of Lee and Yang's scheme and propose an improved method to enhance security. The rest of this paper is organized as follows. In Section 2, we shall review Lee and Yang's scheme. Then, in Section 3, we present their drawbacks, followed with our improved scheme in Section 4. We discuss our scheme in terms of security and practicability in Section 5. Finally, a conclusive remark will be given in Section 6.

II. A REVIEW OF LEE AND YANG'S SCHEME

In this section, we shall briefly review Lee and Yang's scheme [11]. Basically, they combined the concepts of digital signature with an access control to design subliminal channels. Their scheme can be divided into four phases: initialization phase, signature generation phase, signature verification phase and subliminal message recovery phase. The detailed descriptions are given as follows.

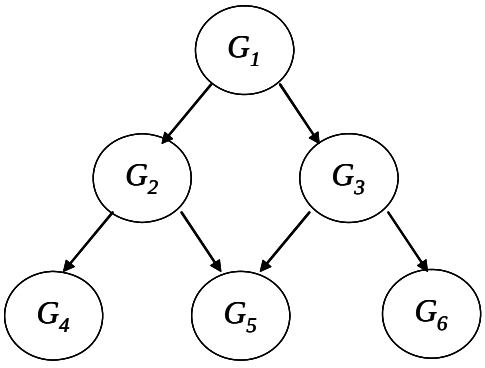

Fig. 1. An instance of user hierarchy

Manuscript received April 6, 2006.

Chin-Chen Chang is with the Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan, 40724, R.O.C. (corresponding author to provide phone: 886-4-24517250 ext. 3790; fax: 886-4-27066495; e-mail:ccc@cs.ccu.edu.tw) and with the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 621, Taiwan, R.O.C.

Chia-Chi Wu is with Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 621, Taiwan, R.O.C. (e-mail: wcc@cs.ccu.edu.tw).

Initialization phase

Assume that subliminal channel receivers organize a hierarchy form as Fig. 1. User G_1 can access any information kept by five users G_2, G_3, G_4, G_5, and G_6. On the other hand, users G_2, G_3, G_4, G_5, and G_6 are not permitted to access the information held by G_1. In this architecture, each user only holds one secret key and can use this secret key to compute other subordinates' secret keys and access their secret information. First, the sender G_s must generate and compute the following parameters:

p, q: two large primes, and $q|p$-1.

g_j: generators with order q in $GF(p)$, j=1,2,…,7.

H(•): a one-way hash function.

ID_i: the user G_i's identity, i=1,2,…,6.

x_i: the user G_i's secret key, i=1,2,…,6. If G_j has only one immediate predecessor G_i, $x_j=H(x_i,ID_j)$. Otherwise, the sender G_s randomly generates a secret key x_j for G_j.

x_s: the sender's secret key, $x_s \in Z_q^*$.

y_s: the sender's public key $y_s = \prod_{i=1}^{6} g_i^{-x_i} \cdot g_7^{-x_s} \bmod p$.

Because both G_2 and G_3 can derive the secret key of G_5, the sender G_s must compute two parameters and make them public as follows.

r_{k5}=H(x_k, ID_5)$\oplus x_5$, where k=2 and 3.

At last, the sender secretly sends x_1 to G_1, x_2 to G_2,…, x_6 to G_6.

Signature generation phase

Suppose that the sender wants to sign an obvious message m and hide subliminal messages $M_i \in Z_q^*$ into the signature. The sender first chooses a random integer $R \in Z_q^*$ and generates a signature (e, s_1, s_2,…, s_6, s_R) for m as follows.

$$e = H(\prod_{i=1}^{6} g_i^{M_i} \cdot g_7^{R} \bmod p \,\|\, m),$$

$$s_i = M_i + ex_i \bmod q,\ i = 1,2,...,6, \text{ and}$$

$$s_R = R + ex_s \bmod q.$$

Second, the sender delivers (m, e, s_1, s_2,…, s_6, s_R) to all of the receivers in the organization.

Signature verification phase

After receiving this message, each receiver can verify the signature via the equation:

$$e \stackrel{?}{=} H(\prod_{i=1}^{6} g_i^{s_i} \cdot g_7^{s_R} \cdot y_s^{e} \bmod p \,\|\, m).$$

If they are equal, the receiver can confirm the integrity of the signature.

Subliminal message recovery phase

As shown in Fig. 1, a higher level user can obtain his/her subordinates' subliminal messages. To recover subliminal messages, there are three steps. .

1. Getting his/her own message
   Each subliminal receiver can use his/her own secret key x_i to retrieve the subliminal message M_i through the equation:
   $M_i = s_i - ex_i \bmod q$. (1)
2. Getting his/her subordinates' subliminal messages
   The user G_i can compute his/her subordinates' secret key x_j via $x_j=H(x_i, ID_j)$, and then use x_j to compute subordinates' subliminal messages by Eq.(1).
3. Getting the subliminal message M_5
   Referring to G_2 and G_3, they first use their own secret key to calculate secret values $H(x_i, ID_5)$, i=2 or 3. Then, they derive G_5's secret key $x_5 = H(x_i, ID_5)\oplus r_{i5}$, i=2 or 3. As a result, G_2 and G_3 can retrieve M_5 by Eq.(1).

III. Drawbacks on Lee and Yang's Scheme

After we studied Lee and Yang's scheme in detail, we find that this scheme has two drawbacks, which may release inside malicious attacker critical information to break other's subliminal channel messages or secret keys. We explain these drawbacks as follows.

1. Subliminal Channel Messages Guessing Attack
   According to Lee and Yang's scheme, the sender must make (r_{25} , r_{35}) into public, and transmits (m, e, s_1, s_2,…, s_6, s_R) to all of the receivers via an open channel. Hence, we can ascertain that (m, e, s_1, s_2,…, s_6, s_R) and (r_{25} , r_{35}) can be obtained by all eligible receivers. The user G_2 can perform as follows to guess a subliminal channel message.
   (1) G_2 first computes x_5=H(x_2, ID_5)$\oplus r_{25}$, and then uses x_5 to compute H(x_3,ID_5) value via H(x_3,ID_5)= $x_5\oplus r_{35}$.
   (2) Assume that $x_3 < q$, and the user G_2 can rewrite Eq.(1) to get the following equation.
   $(s_3 - M_3) \cdot e^{-1} \bmod q = x_3$. (2)
   (3) With s_3 and $e^{-1} \in GF(q)$, G_2 is able to construct the following equation according to Eq.(2).
   H(x_3, ID_5)=H[(s_3-M_3) • e^{-1} mod q, ID_5]. (3)
   (4) Because M_3 is the only unknown number in Eq.(3) for G_2, he/she can use offline guessing to find M_3 value. G_2 can easily divide ranges of the prime q to perform parallel guessing computations; therefore, M_3 suffers off-line guessing attack by G_2 indeed. And M_2 also confronts the similar attack by G_3.
2. User Key Guessing Attack
   According to the above mentioned Item (1), we can infer that user G_2 can get H(x_3, ID_5). Similarly, G_3 can get H(x_2, ID_5), and G_5 can obtain H(x_2, ID_5) and H(x_3, ID_5). Since ID_5 is public, G_2 can do offline guessing of x_3 according to H(x_3, ID_5). Hence, G_3 can guess x_2 offline, and G_5 can guess x_2 and x_3. This will damage the security requirement of the hierarchical access control.

Summary of above drawbacks, we find that H(x_2, ID_5) and H(x_3, ID_5) are very critical information that must be well protected. In Section 4, we propose an improved scheme to overcome these security drawbacks.

IV. Our Improved Scheme

In Lee and Yang's user hierarchy, each user G_i has two superiors at most. We let these two people negotiate their subordinate's secret key to protect the above mentioned hash

values against guessing attack.

In Initialization phase, we modify the generation procedure of x_5, and the sender does not need to compute and make public r_{k5}=H(x_k, ID_5)$\oplus x_5$, where k=2 and 3. First, the sender computes $x_5' = H(x_2, ID_5)$ and $x_5'' = H(x_3, ID_5)$. Second, the sender generates G_5's secret key $x_5 = g_7^{x_5' x_5''} \bmod p$. And the remainder processes are the same as Lee and Yang's scheme.

Signature generation phase and signature verification phase still execute the original processes.

In the subliminal message recovery phase (Item 3), if both G_2 and G_3 want to get G_5's subliminal message M_5, they must perform the following procedure to compute G_5's secret key x_5.

(1) G_2 computes $x_5' = H(x_2, ID_5)$

and $r_{25} = g_7^{x_5'} \bmod p$, and then sends r_{25} to G_3.

(2) G_3 computes $x_5'' = H(x_3, ID_5)$

and $r_{35} = g_7^{x_5''} \bmod p$, and sends r_{35} to G_2.

(3) G_2 computes $x_5 = r_{35}^{x_5'} \bmod p$.

(4) G_3 computes $x_5 = r_{25}^{x_5''} \bmod p$.

Therefore, both G_2 and G_3 can get x_5 so that they can retrieve M_5 by Eq.(1).

V. Security and Practicability Discussions

In this section, we analyze the advantages of our improved scheme in security and practicability.

1. Security

In our scheme, all hash values H(x_i, ID_j) are protected by the modular exponentiation. To find the hash value is to find the discrete logarithms of a number. Many published researches [9, 12, 14, 20] has proved that it is infeasible to solve this discrete logarithms problem in polynomial time. Contrarily, Rivest and Shamir's evaluated [16] that hash functions are about 10,000 times faster than the modular exponentiation. And therefore, Lee and Yang's scheme may easily confront off-line guessing attack. Consequently, our scheme is stronger than Lee and Yang's scheme in security.

2. Reducing the sender's burden

Assume that there are n levels in user hierarchy, and we induce that the sender will waste a large amount of storage space to store ((n-1) • (n-2)) publish parameters. However, in our improvement, the sender no more needs to maintain any bulletin board or publish parameters, which can reduce both the sender's storage space needed and service burden.

3. Distributing network flow

In Lee and Yang's scheme, each user G_i must get related public parameter to compute their subordinates' secret keys. Therefore, all network flow will concentrate on the sender's bulletin board. It is possible that the functionality of the bulletin board or result in network traffic jam will be affected.

In our improvement, G_2 and G_3 conduct message exchanging to negotiate their subordinate G_5's secret key. This performance can not only realize network flow distribution, but improve network efficiency as well.

VI. Conclusions

In this paper, we have proposed an improved version of Lee and Yang's scheme that will overcome the drawbacks of their original scheme. To realize the security of our improved scheme means to solve discrete logarithms problem. We have also demonstrated our scheme is practical in application that it can be applied in the high data security access control organization.

References

[1] C. C. Chang, R. J. Hwang, and T. C. Wu, "Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," *Information Systems*, Vol. 17, No. 3, 1992, pp. 243-247.

[2] C. C. Chang and D. J. Buehrer, "Access Control in a Hierarchy Using a One-Way Trap Door Function," *Computers and Mathematics with Applications*, Vol. 26, No. 5, 1993, pp. 71-76.

[3] C. C. Chang, S. W. Fan, H. T. Liaw, and M. Y. Chiou, "Cryptanalysis on an Access Control in a Hierarchy," *Computers and Mathematics with Applications*, Vol. 29, No. 4, Feb. 1995, pp. 69-72.

[4] C. C. Chang, I. C. Lin, and H. M. Tsai, "A Dynamic Mechanism for Determining Relationships in a Partially Ordered User Hierarchy," *International Journal of High Performance Computing and Networking*, Vol. 3, No. 5/6. 2005, pp. 378-384.

[5] Y. F. Chang, C. C. Chang, and H. F. Huang, "Digital Signature with Message Recovery Using Self-certified Public Keys without Trustworthy System Authority," *Applied Mathematics and Computation*, Vol. 161, No. 1, 2005, pp. 211-227.

[6] M. S. Hwang, C. C. Chang, and W. P. Yang, "Modified Chang-Hwang-Wu Access Control Scheme," *IEE Electronics Letters*, Vol. 29, No. 24, Nov. 1993, pp. 2095-2096.

[7] H. F. Hwang, and C. C. Chang, "A New Cryptographic Key Assignment Scheme with Time-Constraint Access Control in a Hierarchy," *Computer Standards and Interfaces*, Vol. 26, No. 3, 2004, pp. 159-166.

[8] J. K. Jan, Y. M. Tseng, "New Digital Signature with Subliminal Channels Based on the Discrete Logarithm Problem," *Proceedings of the 1999 International Workshops on Parallel Processing*, 1999, pp. 198-203.

[9] B. A. LaMacchia and A. M. Odlyzko, "Computation of Discrete Logarithms in Prime Fields," *Design, Codes, and Cryptography*, Vol. 1, 1991, pp. 46-62

[10] N. Y. Lee and D.R. Lin, "Robust Digital Signature Scheme with the Subliminal Channels," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E86-A, No. 1, 2003, pp. 187-188.

[11] N. Y. Lee and S. Y. Yang, " The Design of Integrating Subliminal Channel with Access Control," *Applied Mathematics and Computation*, Vol. 171, No. 1, pp. 573-580, Dec. 2005.

[12] K. S. McCurley, "The Discrete Logarithm Problem," *Cryptography and Computational Number Theory, Proceedings of the Symposium on Applied Mathematics*, American Mathematics Society, 1990, pp.49-74.

[13] National Institute of Standards and Technology, NIST FIPS PUB 186, "Digital Signature Standard," U. S. Department of Commerce, May 1994.

[14] A. Odlyzko, "Discrete Logarithms in Finite Fields and Their Cryptographic Significance," *Advance in Cryptology: Proceedings of EUROCRYPT 84*, Springer-Verlag, 1985, pp.224-314.

[15] R. Rivest, "The MD5 Message Digest Algorithm," RFC 1321, 1992.

[16] R. Rivest and A. Shamir, “PayWord and MicroMint: Two Simple Micropayment Schemes,” May 1996. Available at http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps
[17] G. J. Simons, “The Prisoner’s Channel and the Subliminal Channel,” *Advance in Cryptology: Proceedings of CRYPT 83*, Springer-Verlag, 1984, pp.51-67.
[18] G. J. Simons, “Subliminal Communication Is Easy Using the DSA,” *Advance in Cryptology: Proceedings of EUROCRYPT 93*, Springer-Verlag, 1994, pp.218-232.
[19] H. M. Tsai and C. C. Chang, “A Cryptographic Implementation for Dynamic Access Control in a User Hierarchy,” *Computers and Security*, Vol. 14, No. 2, 1995, pp. 159-166.
[20] A. L. Wells Jr., “A Polynomial Form for Logarithms Modulo a Prime,” *IEEE Transactions on Information Theory*, Nov. 1984, pp. 845-846.
[21] T. C. Wu, and C. C. Chang, “Cryptographic Key Assignment Scheme for Hierarchical Access Control,” *International Journal of Computer Systems Science and Engineering*, Vol. 16, No. 1, 2001, pp. 25-28.

Chin-Chen Chang received his BS degree in applied mathematics in 1977 and his MS degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. During the academic years of 1980-1983, he was on the faculty of the Department of Computer Engineering at the National Chiao Tung University. From 1983-1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan.From 1989 to 2004, he has worked as a professor in the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. Since 2005, he has worked as a professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. Dr. Chang is a Fellow of IEEE, a Fellow of IEE and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, and the Phi Tau Phi Society of the Republic of China. His research interests include computer cryptography, data engineering, and image compression.

Chia-Chi Wu was born on December 9, 1967 in Taoyuan, Taiwan, Republic of China (R.O.C.). He received the B.S. in Information Management from National Defense Management College, Taipei, Taiwan, Republic of China, in 1991; the M.S. in Information Management from National Defense Management College, Taiwan, in 1999. He is currently pursuing his Ph.D. degree in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan. His current research interests include electronic commerce, information security, cryptography, and mobile communications.