A Novel Key Management Scheme for Dynamic Access Control in a Hierarchy

Shiang-Feng Tzeng[1], Cheng-Chi Lee[2], Tzu-Chun Lin[3]
(Corresponding author: C. C. Lee)

Department of Library and Information Science, Fu Jen Catholic University[2]
510 Jhongjheng Road, Taipei 24205, Taiwan, R.O.C. (Email: cclee@blue.lins.fju.edu.tw)
Department of Applied Mathematics, Feng Chia University[3]
100 Wenhwa Rd, Seatwen, Taichung, Taiwan, R.O.C.
Department of Information Management, Chaoyang University of Technology[1]
168 Gifeng E. Rd., Wufeng Taichung County, Taiwan, R.O.C.
(Received Jan. 12, 2010; revised and accepted Mar. 9, 2010)

Abstract

Shen and Chen proposed a novel key management scheme for dynamic access control in a hierarchy. In this article, the authors shall present an improved version of Shen and Chen's scheme to reduce the computational time required for key generation and derivation.

Keywords: Access control, cryptography, data security, key management.

1 Introduction

In 1983, Akl and Taylor [1] first proposed a solution to the control of the access to information items among a group of users in a hierarchy. In general, the key management in a hierarchy can be achieved by dividing the users and their own information items into a number of disjoint sets of security classes [2, 5, 6, 11, 12, 13, 16, 17, 18]. Let $SC_1, SC_2, \cdots, SC_n$ be n disjoint security classes. Assume that " <= " is a partially ordered binary relation applied to the set $SC = \{SC_1, SC_2, \cdots, SC_n\}$, where $SC_j <= SC_i$ means that the users in the security class SC_i have a security clearance higher than or equal to those in the security class SC_j. On the one hand, users in the security class SC_i can obtain the secret keys in SC_j and access the information items of the users in SC_j, while the users in SC_j cannot access the information items of the users in SC_i. So far, many schemes have been proposed to solve the problem of access control in a hierarchy [3, 7, 8, 9, 10, 14, 15].

Recently, Shen and Chen [14] proposed a novel key management scheme for dynamic access control in a partially order user hierarchy. Their scheme is based on both the Diffie-Hellman public key system [4] and the polynomial interpolation method. The key generation phase and the key derivation phase of Shen and Chen's scheme are simple. Furthermore, their scheme supports dynamical addition and deletion of security classes and relationships. Besides, any user can choose her/his own secret key at will for convenience and can freely change her/his secret key for some security reasons. Shen and Chen stated that their scheme could shorten the computational time for key management. However, to enhance the efficiency, in the paper, we shall present an improved version of Shen and Chen's scheme.

2 Overview of the Shen-Chen Scheme

There are three phases in the Shen-Chen Scheme: the relationship building, the key generation, and the key derivation phases [14]. Their scheme is aimed at solving the dynamic key management problem in a user hierarchy by introducing the Diffie-Hellman public key system and the polynomial interpolation method. The relationship-building phase is completed by the central authority (CA), whose main role is to construct a public relationship list that includes each security class in the hierarchy. The relationship list is used to check whether the user's key derivation is needed or not. Only CA owns the capability to modify the contents of the relationship list.

The key generation phase is completed by CA, whose main aim here is to create secret as well as public information for each security class. After the key generation phase, CA assigns four parameters to each security class SC_i, denoted as Q_i, H_i, b_i and SK_i. Here, Q_i is public information. The other parameters (H_i, b_i, SK_i) are secret information owned by SC_i. The parameters are defined as follows:

- p is a large random prime number such that $p = 2p' + 1$, where p' is also a large prime integer number.
- b_i, $i = 1, 2, \cdots, n$, are random positive integers such that $1 <= b_i <= p$.
- SK_i, $i = 1, 2, \cdots, n$, are secret keys that satisfy $GCD(SK_i, p-1) = 1$.
- $H_i(x)$ are polynomial interpolations for SC_i at points $(j||(g^{SK_i} \bmod p),\ b_j)$'s for all $SC_j <= SC_i$, where "||" is a bit concatenation operator.
- $Q_i = SK_i^{1/b_i} \bmod p$, where $b_i \times b_i^{-1} = 1 \bmod (p-1)$.

In the key derivation phase of the Shen-Chen scheme, the secret key of the security class SC_j can be derived by the security class SC_i if $SC_j <= SC_i$. SC_i can use the secret key SK_i and the secret information H_i owned by her/himself to obtain the secret key of SC_j. SC_i can obtain b_j by computing $H_i(j||(g^{SK_i} \bmod p))$. Since $SK_j = Q_j^{b_j} \bmod p$, SC_i can thus derive the secret key SK_j.

3 The Improved Scheme

Shen and Chen used the discrete logarithms and polynomial interpolations to hide the secret key SK_i. Our improved scheme is the same as Shen and Chen's scheme except that we use the one-way hash function and the execute-or operation of discrete logarithms.

To save more computational time, we built up an improved scheme which is a revised version of Shen and Chen's scheme. The revised scheme works as follows.

1) Randomly choose a positive integer b_i of SC_i.
2) Select a random integer as the secret key SK_i for SC_i.
3) Calculate $H_i(x)$ at point $(h(j, SK_i), b_j)$'s for all $SC_j <= SC_i$.
4) Calculate $Q_i = SK_i \oplus b_i$.

By way of the above steps, each security class SC_i, $i = 1, 2, \cdots, n$, has four parameters: (Q_i, $H_i(x)$, b_i, SK_i). Q_i is a public parameter, $H_i(x)$, b_i and SK_i are secret parameters. By using the secret key SK_i, SC_i can derive her/his successor's secret key SK_j. From the secret key SK_j, SC_i can decrypt the information owned by SC_j. The key derivation phase to obtain the secret key SK_j is as follows.

$$b_j = H_i(h(j, SK_i)). \quad (1)$$

By using b_j and the execute-or operation, SC_i can receive the secret key SK_j as follows.

$$SK_j = Q_j \oplus b_j. \quad (2)$$

Let's compare the computational complexity of the key generation phase of our scheme with that of Shen and Chen's scheme. Our revised scheme does not need the exponentiation and modular inverse computation. The computational time needed by the key generation phase of our novel revised scheme is thus found to be less than that of the Shen-Chen scheme.

Next, let's compare the computational time of the key derivation phase of our scheme with that of the Shen-Chen scheme. Our scheme requires only a single one-way hash function to do Equation (1) and one execute-or operation for Equation (2). However, Shen and Chen's scheme requires two exponential computations, as stated in Section 2. Thus the computational time of the key derivation phase of our new extended scheme is found to be less than that of the Shen-Chen scheme.

The security of the secret key of SC_i in our scheme is lies in the interpolating polynomial $H_i(x)$ and the execute-or operation $SK_j = Q_j \oplus b_j$. Since $H_i(x)$ and b_j are secret information and a dishonest user only has the public information Q_j and j, she/he cannot obtain the secret key SK_i and $H_i(x)$. In addition, two or more users at a lower level security classes SC_j cannot collaborate to get a higher security class SC_i's secret key SK_i.

Our scheme can also perform dynamic key management, such as adding/deleting classes, adding/deleting relationships and changing secret keys, which is similar to the Shen-Chen scheme. The modified scheme not only preserves all the advantages of Shen and Chen's scheme but also shortens the computational time for key generation and key derivation.

4 Conclusion

In this article, we have presented a revised scheme which is a slight modification of the Shen-Chen scheme to reduce the computational time. The improved scheme can also perform dynamical access control the same way the Shen-Chen scheme does.

Acknowledgments

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC98-2221-E-468-002. The authors are grateful to the anonymous reviewers for valuable comments.

References

[1] S. G. Akl and P. D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," *ACM Transactions on Computer Systems*, vol. 1, pp. 239–248, 1983.

[2] Chin-Chen Chang, Iuon-Chang Lin, and Chia-Te Liao, "An access control system with time-constraint

using support vector machines," *International Journal of Network Security*, vol. 2, no. 2, pp. 150–159, 2006.
[3] T. S. Chen and Y. F. Chung, "Hierarchical access control based on chinese remainder theorem and symmetric algorithm," *Computers & Security*, vol. 21, no. 6, pp. 565–570, 2002.
[4] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644–654, 1976.
[5] Debasis Giri and P. D. Srivastava, "An asymmetric cryptographic key assignment scheme for access control in tree structural hierarchies," *International Journal of Network Security*, vol. 4, no. 3, pp. 348–354, 2007.
[6] Debasis Giri and P. D. Srivastava, "A cryptographic key assignment scheme for access control in poset ordered hierarchies with enhanced security," *International Journal of Network Security*, vol. 7, no. 2, pp. 223–234, 2008.
[7] M. S. Hwang, "Extension of CHW cryptographic key assignment scheme in a hierarchy," *IEE Proceedings Computers and Digital Techniques*, vol. 146, no. 4, pp. 219, 1999.
[8] M. S. Hwang, "An asymmetric cryptographic scheme for a totally-ordered hierarchy," *International Journal of Computer Mathematics*, vol. 73, pp. 463–468, 2000.
[9] M. S. Hwang, "Cryptanalysis of YCN key assignment scheme in a hierarchy," *Information Processing Letters*, vol. 73, no. 3, pp. 97–101, 2000.
[10] M. S. Hwang, C. C. Chang and W.-P. Yang, "Modified Chang-Hwang-Wu access control scheme," *IEE Electronics Letters*, vol. 29, pp. 2095–2096, 1993.
[11] Hristo Koshutanski, "A survey on distributed access control systems for web business processes," *International Journal of Network Security*, vol. 9, no. 1, pp. 61–69, 2009.
[12] Deholo Nali, Carlisle Adams, and Ali Miri, "Using threshold attribute-based encryption for practical biometric-based access control," *International Journal of Network Security*, vol. 1, no. 3, pp. 173–182, 2005.
[13] Leon Pan, "A web-based multilayer access control model for multimedia applications in MPEG-7," *International Journal of Network Security*, vol. 4, no. 2, pp. 155–165, 2007.
[14] V. R. L. Shen and T. S. Chen, "A novel key management scheme based on discrete logarithms and polynomial interpolations," *Computers & Security*, vol. 21, no. 2, pp. 164–171, 2002.
[15] V. R. L. Shen, T. S. Chen and F. Lai, "Novel cryptographic key assignment scheme for dynamic access control in a hierarchy," *Transactions on Fundamentals*, vol. E80-A, no. 10, pp. 2035–2037, 1997.
[16] Manpreet Singh and Manjeet S. Patterh, "Formal specification of common criteria based access control policy model," *International Journal of Network Security*, vol. 11, no. 3, pp. 112–121, 2010.
[17] Nicolas Sklavos and Odysseas Koufopavlou, "Access Control in Networks Hierarchy: Implementation of Key Management Protocol," *International Journal of Network Security*, vol. 1, no. 2, pp. 103–109, 2005.
[18] Qiong Zhang, Yuke Wang, and Jason P. Jue, "A Key Management Scheme for Hierarchical Access Control in Group Communication," *International Journal of Network Security*, vol. 7, no. 3, pp. 323–334, 2008.

Shiang-Feng Tzeng received the B.S. degree in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2001 and the M.S. degree in Information Management in 2003 from CYUT. His current research interests include applied cryptography and data security.

Cheng-Chi Lee received the B.S. and M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 1999 and in 2001. He researched in Computer and Information Science from National Chiao Tung University (NCTU), Taiwan, Republic of China, from 2001 to 2003. He received the Ph.D. in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. He was a Lecturer of Computer and Communication, Asia University, from 2004 to 2007. From 2007, he is an assistant professor of Photonics and Communication Engineering, Asia University. From 2009, he is an Editorial Board member of International Journal of Network Security and International Journal of Secure Digital Information Age. His current research interests include information security, cryptography, and mobile communications. Dr. Lee had published over 60+ articles on the above research fields in international journals.

Tzu-Chun Lin is an assistant professor in the Department of Applied Mathematics of Feng Chia University in Taiwan, R.O.C. She received her PhD in Mathematics from GLottingen University in Germany. Her current research interests include Invariant Theory of Finite Groups and Elliptic Curve Cryptography.