MODIFIED "CHANG-HWANG-WU ACCESS CONTROL SCHEME" *

Min-Shiang Hwang [†, ‡], Chin-Chen Chang [¶]
and
Wei-Pang Yang [§]

Department of Computer and Information Science [†, §]
National Chiao Tung University
Hsinchu, Taiwan 300, R.O.C.

Institute of Computer Science and Information Engineering [¶]
National Chung Cheng University
Chiayi, Taiwan 621, R.O.C.

Directorate General of Telecommunication Laboratories [‡]
Ministry of Transportation and Communications
Chung-Li, Taiwan 320, R.O.C.

November 13, 2004

Abstract

This letter presents that some security classes in Chang-Hwang-Wu's access control scheme can collaborate to derive the secret key of their immediate ancestor in some cases. We also give some slight modifications on the proposed scheme to enhance the security levels.

Indexing terms: Cryptography, Security.

Introduction: In [Chang, Hwang, Wu 1992], the authors proposed an efficient cryptographic key assignment scheme for solving the access control problem in a partially ordered hierarchy. Basically, the scheme is based on Newton's interpolating method and a predefined one-way function. The scheme not only reduces the amount of the storage required for storing public parameters, but also is simple and efficient in generating and derivating keys. However, some security classes can collaborate to derive the secret key of their immediate ancestor in some cases. We also give some modifications to slightly modify that subject scheme so that the security will be greatly

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC82-0408-E-009-161, and by the Telecommunication Laboratories. Taiwan, R.O.C., under contracts no.: TL-NSC-82-5206.

†

‡

¶

§

†

§

¶

‡

improved.

The weakness of the proposed scheme: In the subject paper, the authors assumed that there is a trusted third party in the system that is responsible for generating and distributing keys. They assigned each security class C_{ij} an associated distinct pairs (a_{ij}, b_{ij}) as the public parameter. Assume that the security class C_i has d immediate successors $C_{i1}, C_{i2}, \cdots, C_{id}$. The security class C_i, using Newton's interpolation method, constructs an interpolating polynomial $H_i(X)$ of degree d by interpolating on the points $(0, K_i)$, (a_{i1}, b_{i1}), (a_{i2}, b_{i2}), $\cdots$, (a_{id}, b_{id}) over $GF(P)$. Let $H_i(X) = (K_i + \sum_j c_{ij}X^j) \bmod P$, where c_{ij} is an integer between 0 and $P-1$. The secret key K_{ij} of C_{ij} is calculated by $K_{ij} = f(c_{ij}) \bmod P$, for $j = 1, 2, \cdots, d$, where c_{ij} is the coefficient of the term X^j in $H_i(X)$.

The key derivation is quite similar to the key generation. Using Newton's interpolation method, they reconstruct the interpolating polynomial $H_i(X) = (K_i + \sum_j c_{ij}X^j) \bmod P$ by interpolating on the points $(0, K_i)$, (a_{i1}, b_{i1}), (a_{i2}, b_{i2}), $\cdots$, (a_{id}, b_{id}). The secret key of C_{ij} is thus obtained from $K_{ij} = f(c_{ij}) \bmod P$, where c_{ij} is the coefficient of the term X^j in $H_i(X)$.

In the proposed scheme, the pairs of public parameters (a_{ij}, b_{ij})'s, the prime number P and the predefined one-way function f are known to all security classes in the hierarchy. The security class C_i only keeps its own secret key K_i secretly.

Now we will show that the weakness in security of the above scheme. Let $C_{i1}, C_{i2}, \cdots, C_{id}$ be d immediate successors of the security class C_i. Since the points (a_{i1}, b_{i1}), (a_{i2}, b_{i2}), $\cdots$, (a_{id}, b_{id}) for $C_{i1}, C_{i2}, \cdots, C_{id}$, respectively, are known to each security class, we can construct an interpolating polynomial $H_i(X) = (K_i + \sum_j c_{ij} X^j) \bmod P$ with one unknown point $(0, K_i)$ and d known points (a_{i1}, b_{i1}), (a_{i2}, b_{i2}), $\cdots$, (a_{id}, b_{id}), based on the Newton's interpolation method [Knuth 1969]. The formula is as follows.

$$H_i(X) = (K_i + g_1(K_i)X + g_2(K_i)X^2 + \cdots + g_d(K_i)X^d) \bmod P, \tag{1}$$

where $g_j(K_i)$ can be represented as a linear polynomial with one unknown variable K_i. (i.e., $g_j(K_i) = g_1 K_i + g_0$, g_1, g_0 are two integers.) Now suppose f is a one-way function of degree d. Then the coefficient $g_j(K_i)$ in (1) is substituted to the function f. Consequently, we have

$$\begin{aligned} f(g_j(K_i)) &= K_j, \\ &= (e_{jd} K_i^d + e_{j(d-1)} K_i^{d-1} + \cdots + \\ &\qquad \cdots + e_{j1} K_i + e_{j0}) \bmod P, \text{ for } j = 1, 2, \cdots, d. \end{aligned}$$

Since we have d equations and d variables, by Gauss's eliminating method [Noble, Danial 1977], thus when d immediate successors of the security class C_i collude, the secret key K_i of C_i is revealed. In fact, only one security class is needed for breaking the scheme when the one-way function is in Quadratic Residue modulo (i.e., $f(X) = g_2 X^2 + g_1 X + g_0 \bmod P$.) [Schroeder 1985]. Therefore, when the one-way function is a polynomial of degree d, they need

$d-1$ immediate successors for conspiracy attack.

Modifications and Discussions: From the above statements and example, we see that $d-1$ security classes can collaborating attack the one-way function of degree d. We now give two modifications for withstanding this attack.

Modification 1: Each security class has his own private one-way function. This means that the one-way function f_i has to be kept secretly by the security class C_i and the third party.

Modification 2: Choose a one-way function of degree $d+2$ where d is a maximal number of immediate successors of each security class in the whole system.

Although Modification 1 can prevent conspiracy attack, it wastes a large amount of storage space to store these one-way functions. As to Modification 2, it not only keeps the advantage of the proposed scheme but also enhances the security.

References

[1] CHANG, C. C., HWANG, R. J., and WU, T. C.: 'Cryptographic key assignment scheme for access control in a hierarchy', *Information Systems,* 1992, **17(3)**, pp. 243-247

[2] KNUTH, D. E.: 'The art of computer programming, Vol.2: seminumberical algorithm' (MA:Addision-Wesley, 1980)

[3] NOBLE, B. and DANIAL, J. W.: 'Applied linear algebra, 2'nd edition' (Prentice-Hall, 1977)

[4] SCHROEDER, M. R.: 'Number theory in science and communication, 2'nd edition' (Springer-Verlag, 1985)