Improvement of Yen-Laih Dynamic Access Control Scheme with User Authentication

Tzong-Chen Wu
Department of Information Management,
National Taiwan University of Science and Technology,
43, Section 4, Keelung Road, Taipei, Taiwan 106,
R.O.C.
E-mail: tcwu@cs.ntust.edu.tw

Wei-Hua He
Department of Information Management,
National Taiwan University of Science and Technology,
43, Section 4, Keelung Road, Taipei, Taiwan 106,
R.O.C.
E-mail: D8509004@mail.ntust.edu.tw

Abstract

The authors show that Yen and Laih's dynamic access control scheme with user authentication does not achieve the security requirements as they claimed. That is, any legitimate user can successfully fool the system to act as another legitimate user and take over all access privileges granted by that user. The authors also present an improvement that can eliminate the security flaw inherent in the original Yen-Laih scheme.

Keywords: *dynamic access control, user authentication*

1. Introduction

In 1992, Harn and Lin [2] first proposed a dynamic access control scheme with combination of user authentication that provides security solutions to insertion of a new user/file, deletion of an old user/file, and grant/revocation of access privileges. The security of the Harn-Lin scheme is based on the well-known factorization problem and the RSA cryptosystem [3]. Lately, Yen and Laih [4] proposed another dynamic access control scheme based on the well-know discrete logarithm problem and the ElGamal cryptosystem [1] to resolve the same problems defined in the Harn-Lin scheme. The Yen-Laih scheme preserves the same advantages and characteristics of the Harn-Lin scheme. Hence, both these two schemes are applicable to counter the threats of unauthorized users to access files and to prevent a legitimate user to from performing unauthorized operations in the file protection system. By examining the Yen-Laih scheme deeply, we find that there exists some security flaw within it. That is, any legitimate user can successfully fool the system to act as another legitimate user and take over all access privileges granted by that user. In this letter, we first show the security flaw of the Yen-Laih scheme. We then present an improvement that can eliminate the security flaw inherent in the original Yen-Laih scheme. The improvement is as efficient as the original scheme, since it only requires a slight effort for calculating the adopted one-way hash function during the registration and the verification phases. Besides, the improvement can achieve the security administration functions (such as the password updating process and batch access request verification) that are provided by the original Yen-Laih scheme in effective.

2. Review of the Yen-Laih scheme

The Yen-Laih scheme is described in the following. Initially, the system selects a large prime p, a generator g over GF(p), two integers $S_1 \in Z_p$ and $S_2 \in Z_{p-1}^*$, and a one-way hash function h. Note that S_1, S_2 and h are kept secretly by the system. Let SF_i be the set of files that are authorized to the user U_i, $ID_i \in Z_{p-1}^*$ be the identity of U_i, and $r_{i,j}$ be the highest access privilege to F_j for U_i. During the registration phase, the system computes an associated parameter $t_i = \prod_{F_j \in SF_i} h(F_j \| r_{i,j})$ for SF_i and a password $PW_i = g^{k_i} \bmod p$ for U_i, where

$$k_i = (1 - t_i \cdot S_1) \cdot (ID_i \cdot S_2)^{-1} \bmod (p-1) \quad (1)$$

Each U_i possesses t_i, $r_{i,j}$ (for each $F_j \in SF_i$) and PW_i after the registration phase.

Suppose that a legitimate user U_i wants to access to the file F_j with privilege r. First of all, U_i makes a request message $\{ID_i, PW_i, t_i, F_j, r_{i,j}, r\}$ and sends it to the system. Upon receiving U_i's request, the system first checks if ID_i is legitimate and then determines if $h(F_j \| r_{i,j}) | t_i$ and $r \le r_{i,j}$. After the above checks, the system checks the following equality:

$$g = (PW_i)^{ID_i \cdot S_2} \cdot g^{t_i \cdot S_1} \bmod p \quad (2)$$

If equation 2 holds, then U_i is authenticated and his/her access request to F_j with privilege r is granted.

3. Attack on the Yen-Laih scheme

Let U_a and U_i be two legitimate users. Consider the scenario that U_a attempts to act as U_i and fool the system to grant the access to $F_j \in SF_a$ with privilege r, such that the system will believe that the access to F_j is granted by U_i, not by U_a. For example, U_a may act as U_i to "delete" F_j so that he/she can unload the responsibility on U_i. From equation 2, it can be seen that if U_a (without knowing S_1 and S_2) can compute a valid password PW_i^* satisfying $(PW_i^*)^{ID_i} = (PW_a)^{ID_a} \pmod p$, then he/she can make a valid request message $\{ID_i, PW_i^*, t_a, F_j, r_{a,j}, r\}$ that will pass all checks in the

verification phase. U_a can successfully proceed such attack by computing

$$w = ID_a \cdot ID_i^{-1} \bmod (p-1) \quad (3)$$

$$PW_i^* = (PW_a)^w \bmod p \quad (4)$$

From equations 1 and 3, we have

$$k_a = (1 - t_a \cdot S_1) \cdot (w \cdot ID_i \cdot S_2)^{-1} \bmod (p-1)$$

That is,

$$k_a \cdot w \cdot ID_i \cdot S_2 + t_a \cdot S_1 = 1 \bmod (p-1) \quad (5)$$

Raising both sides of equation 5 to exponents with the base g and substituting equation 4 into the result, it yields that

$$\begin{aligned} g &= g^{k_a \cdot w \cdot ID_i \cdot S_2 + t_a \cdot S_1} \\ &= (g^{k_a})^{w \cdot ID_i \cdot S_2} \cdot g^{t_a \cdot S_1} \\ &= ((PW_a)^w)^{ID_i \cdot S_2} \cdot g^{t_a \cdot S_1} \\ &= (PW_i^*)^{ID_i \cdot S_2} \cdot g^{t_a \cdot S_1} \pmod p \end{aligned}$$

Therefore, the request message $\{ID_i, PW_i^*, t_a, F_j, r_{a,j}, r\}$ will pass all checks in the verification phase, and hence, U_a can act as U_i to grant the access privilege r to F_j without being detected by the system.

4. Our Improvement

From the above analysis, we can easily eliminate the security flaw of the Yen-Laih scheme by replacing equations 1 and 2 with 1* and 2*, respectively:

$$k_i = (1 - h(t_i \| ID_i) \cdot S_1) \cdot S_2^{-1} \bmod (p-1) \quad (1^*)$$

$$g = (PW_i)^{S_2} \cdot g^{h(t_i \| ID_i) \cdot S_1} \bmod p \quad (2^*)$$

Now, let us give an informal proof to show that the improvement can withstand the attack stated above. Reconsider the scenario of the impersonation attack against the Yen-Laih scheme. From equation 2*, it can be seen that if the attacker U_a can either find a PW_i^* satisfying $g = (PW_i^*)^{S_2} \cdot g^{h(t_a \| ID_i) \cdot S_1} \pmod p$ or find a t_i^* satisfying $g = (PW_a)^{S_2} \cdot g^{h(t_i^* \| ID_i) \cdot S_1} \pmod p$ and $h(F_j \| r_{a,j}) \| t_i^*$, then he/she can act as U_i to grant the access privilege r to F_j without being detected by the system. This implies that the success of these two approaches depend on the disclosure of S_1 and S_2. However, S_1 and S_2 are protected by the intractability of computing discrete logarithm over GF(p) [1]. The encouraged reader can verify that our improvement can achieve the security administration functions (such as the password updating process and batch access request verification) provided by the original scheme in effective.

Reference

[1] ElGamal T., "A public key cryptosystem and signature scheme based on discrete logarithm", *IEEE Transactions on Information Theory*, Vol. IT-31, No. 4, pp. 469-472, 1985.

[2] Harn, L. and Lin, H. Y., "Integration of user authentication and access control", *IEE Proceedings Computers and Digital Techniques*, Vol. 139, No. 2, pp. 139-143, 1992.

[3] Rivest R. L., Shamir, A. and Adleman L., "A method for obtaining digital signatures and public-key cryptosystem", *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[4] Yen S. M. and Laih C. S., "The design of dynamic access control scheme with user authentication", *Computers and Mathematics with Applications*, Vol. 25, No. 7, pp. 27-32, 1993.