Int. Computer Symposium, Dec. 15-17, 2004, Taipei, Taiwan.

Improvement on a Provable Secure Access Control using Smart Cards

Fuw-Yi Yang
Department of Applied Mathematics
National Chung Hsing University
E-mail:yangfy@ms7.hinet.net

Jinn-Ke Jan
Department of Computer Science
National Chung Hsing University
E-mail:jkjan@cs.nchu.edu.tw

Abstract—*An access control scheme integrating with user authentication is proposed. Though the scheme is provably secure in request messaging (authentication), there is a flaw in access control. This paper presents an attack on the access control system; and further, an improvement is proposed to remedy this flaw. Our improvement only increases the information size and the cost of computations during registration time, but these quantities are not increased during the login and verification phase.*

Keywords: access control, digital signature, user authentication.

1. Introduction

Access control is chiefly concerned with controlling access to the resources held by a system. Depending on the policies of the system, the central authority can grant or deny access to users. Traditionally, the operating system maintains some tables, *e.g.,* capability list or access control matrix, to perform access control [1].

Before granting access rights to a user, the system must have authenticated the user. Therefore, a user authentication scheme is required to achieve this goal. Many earlier schemes authenticated users based on a password table [2]. The password table records the user's account and password for each registered user. As a user wants to login the system, he must enter his account number and password. According to the content of the password table, the system can verify whether the login user is a legal one.

Authentication using a password table may cause problems. A user may deny having entered the system, because the user's password is stored inside the system and the user may argue that his password has been stolen. Therefore, the schemes that authenticate users by the pieces of secret data stored inside a smart card are explored. By keeping the personal data in the smart cards, rescues the system from maintaining the password table. Therefore, the mystery of the stolen password is no longer a problem.

The problem of stealing a password is also possible in the access control systems that are dependent on some stored tables. Thus, like the solution to the problem of a stolen password in the authentication scheme, storing the access control data in a smart card is a way to solve the problem described above.

A smart card that contains both the authentication data and the access control information inspires us to integrate the schemes of user authentication and access control into one module [3, 4, 5]. By storing these secret data in a smart card, the system is free to collect the tables of user authentication and access control. In addition, the integration benefits security, communication overheads, and computation cost, especially in the distributed computer networks.

However, the scheme in [5] has a drawback. Although the scheme is claimed to be secure, it is found only to be secure in digital signatures signed by cardholders. The scheme's access control leaks secret information about the integrated system. Collusion of some cardholders can reveal secret data of the system by implementing the leaked information.

1.1 Contributions

This paper proposes an attack on the scheme in [5]. After illustrating the cryptanalysis, an improvement to mend the information leakage is proposed. Guaranteeing the security, a formal proof is given to confirm that the improvement is secure against the adaptive chosen message attacks [6]. In this model of attack, it is assumed that an adversary has access to a signing oracle, which generates the signatures, *i.e.*, the access rights granted by the system. The adversary is allowed to collect the access rights by asking the signing oracle as he wishes, except the one that the adversary is forging. This level of security is sufficient to prevent the system from being attacked by the collusions of the smart card holders.

1.2 Organization

Section 2 reviews the scheme in [5], which is shown to be insecure in Section 3. An improvement is proposed in Section 4. Section 5 shows that the improvement is secure. Finally, Section 6 concludes the paper.

2. Review of the previous scheme

This section reviews the scheme in [5], which consists of three entities: a central authority (CA), servers, and users. For each registered user, the CA is responsible for storing the information of access rights and authentication to a smart card. Then the CA delivers the smart card to the user in a secure way. Each server stores resources and provides some access services. Although the server is responsible for user authentication and access control, it does not hold secret information about the access control system or authorization data about the users. By means of the smart card issued from the CA, each user can apply to the servers for some access services.

There are four phases in the implementation, *i.e.*, initialization phase, registration phase, login phase, and verification phase. The details are described as follows.

Initialization phase: The CA chooses and publishes a large prime number p such that $(p – 1)$ has a large prime factor q. Let g be an element of the set $Z_p^* = \{1, 2, …, (p – 1)\}$. The order of this element is q. A collision freeness hash function $h(.)$ maps arbitrary bits string to a bit string having fixed length k, *i.e.*, $h(.): \{0, 1\}^* \rightarrow \{0, 1\}^k$. Assume that the system includes n access rights. For each access right i, CA generates a secret number $x_i \in_R Z_q$, and uses it to compute $y_i = g^{x_i} \mod p$, where the symbol $a \in_R b$ denotes that the element a is chosen randomly from the set b. Therefore, the access rights managed by CA are essentially the two sets $X = \{x_i \mid x_i \in_R Z_q \}$ and $Y = \{y_i \mid y_i = g^{x_i} \mod p\}$, where $0 < i < (n + 1)$.

Registration phase: Assume that CA wants to grant a set of m access rights to user u. Let Y_u denote this set of authorized access rights, then $Y_u \subseteq Y$ and $Y_u = \{y_{uj} \mid y_{uj} \in Y\}$, where $0 < j < (m + 1)$. The CA and user execute cooperatively the following steps to complete the registration phase.

Step 1. User u selects a number $x_u \in_R Z_q$ as his private key. Then, the corresponding public key is $ID_u = g^{x_u} \mod p$. The user stores x_u to a smart card and registers ID_u in the access control system.

Step 2. CA picks an integer $k_u \in_R Z_q$, and computes $r_u = g^{k_u} \mod p$. If $r_u = 0 \mod q$ repeats Step 2 again.

Step 3. CA computes the quantities S_{uj} from the linear congruence equation

$$S_{uj} = h(r_u, ID_u)\, k_u + r_u\, x_{uj} \mod q, \tag{1}$$

where $j = 1, …, m$.

Step 4. CA stores ID_u, r_u, S_{uj}, and y_{uj} to the smart card. The smart card then contains x_u, ID_u, r_u, S_{uj}, and y_{uj} $(j = 1, …, m)$. This card enables user u (user ID_u) to issue a request message for obtaining the service $y_{uj} \in Y_u$.

Login phase: User u attaches his smart card to a terminal and conducts the following steps, whenever he wants to enter the service y_{uj} at time T.

Step 1. Chooses an integer $k \in_R Z_q$ and computes the quantities $r = g^k \mod p$, $H = h(r, T, ID_u, r_u, S_{uj}, y_{uj})$, $s = (k\, H + x_u\, r) \mod q$. If $r = 0 \mod q$, repeats this step again.

Step 2. Constructs the message $L = \{r, s, T, ID_u, r_u, S_{uj}, y_{uj}\}$ and sends it to the server.

Verification phase: In fact, L contains two signatures: (ID_u, r_u, S_{uj}) and $((T, ID_u, r_u, S_{uj}, y_{uj}), r, s)$. The first signature is a certificate issued by CA to certify the identity of user u. The second one is signed by user u on the message $(T, ID_u, r_u, S_{uj}, y_{uj})$ in order to acquire the service of y_{uj}. Therefore, the verification phase consists of two procedures to check whether these two signatures are valid.

The server does the following computations to conclude the verification process. Assume that the request message L arrived at time T'.

Step 1. Checks whether $(T' - T)$ is less than the legal transmission time. If not, rejects the request.

Step 2. Uses the equation $g^{S_{uj}} = r_u^{h(r_u, ID_u)}\, y_{uj}^{r_u} \mod p$ to confirm that (ID_u, r_u, S_{uj}) is a valid certificate.

Step 3. Calculates $H = h(r, T, ID_u, r_u, S_{uj}, y_{uj})$.

Step 4. The equation $g^s = r^H\, ID_u^r \mod p$ is used to prove that the second signature is signed by user u. Accepts user u as legal and grants the service y_{uj} to him, if both equations are valid, but otherwise denies the services to user u.

3. Cryptanalysis of the scheme reviewed

Although the scheme in [5] has rigorous treatment on the security of a request message, it is found that it does not discuss the security on the access control. This section proposes an attack on the access control.

From the initialization phase, it is found that for each service y_i, the secret parameter x_i is the same for all users. Assume that user u has been granted the services y_a and y_b. Hence (2), (3), and (4) are obtained.

$$S_{ua} = h(r_u, ID_u)\, k_u + r_u\, x_a \mod q, \tag{2}$$
$$S_{ub} = h(r_u, ID_u)\, k_u + r_u\, x_b \mod q, \tag{3}$$
$$x_a – x_b = (S_{ua} – S_{ub}) / r_u \mod q. \tag{4}$$

By intercepting the request messages $L_{ua} = \{r', s', T', ID_u, r_u, S_{ua}, y_{ua}\}$ and $L_{ub} = \{r'', s'', T'', ID_u, r_u, S_{ub}, y_{ub}\}$, any one can calculate the quantity $(x_a – x_b)$ using (4). Assume that another user v has obtained the service y_a. Then user v can calculate the quantity S_{vb} in the following way:

$$x_a – x_b = (S_{ua} – S_{ub}) / r_u = (S_{va} – S_{vb}) / r_v \mod q,$$
$$S_{vb} = S_{va} - r_v\, (S_{ua} – S_{ub}) / r_u \mod q. \tag{5}$$

By (5), user v successfully calculates the quantity of S_{vb}, which is the CA's signature on the service y_b and the identity ID_v. Using the same method, if user u colludes with user v, user u can transfer all services granted by CA to user v. This result violates the security of access control.

4. Improvement in the reviewed scheme

From (2) and (3), it can be seen that CA uses the same random number k_u to issue signatures on every service granted to user u. The unknown variable k_u can thus be canceled out as shown in (4). The cancellation of k_u leaks information, *i.e.*, the differences between the secret keys x_a and x_b. Therefore, modifying the signing equation is required, which is used in the registration phase, so that the unknown variable k_u cannot be eliminated.

The improved version of registration phase, login phase, and verification phase are described below.

Improved registration phase: Let $Y_u = \{y_{uj} \mid y_{uj} \in Y, 1 \leq j \leq m\}$ denote the set of services that will be granted to user u. User u and CA execute the following steps together to finish the improved registration phase.

Step 1. This step is the same as Step 1 for the registration phase shown in Section 2, *i.e.*, user u chooses $x_u \in_R Z_q$ as his private key. The corresponding public key is $ID_u = g^{x_u} \; mod \; p$.

Step 2. For each $y_j \in Y_u$, CA picks an integer $k_{uj} \in_R Z_q$, and computes $r_{uj}= g^{k_{uj}} \; mod \; p$. If $r_{uj} = 0 \; mod \; q$ repeats this step. Therefore, CA has calculated the set $R_u = \{ r_{uj} \mid k_{uj} \in_R Z_q, r_{uj}= g^{k_{uj}} \; mod \; p, r_{uj} \neq 0 \; mod \; q$, and $1 \leq j \leq m\}$.

Step 3. Solving for S_{uj} in the linear congruence equation (6), we obtain the set of signatures for the set of access rights Y_u, *i.e.*, $S_u = \{ s_{uj} \mid s_{uj}$ satisfies (6), $y_{uj} \in Y_u$, and $1 \leq j \leq m\}$.

$$s_{uj} = h(r_{uj}, ID_u)\, k_{uj} + r_{uj}\, x_{uj} \; mod \; q \qquad (6)$$

Step 4. CA stores ID_u, R_u, S_u, and Y_u to the smart card. The smart card then contains x_u, ID_u, r_{uj}, s_{uj}, and y_{uj} $(j = 1,..., m)$. This card enables user u to issue the request message for obtaining the service $y_{uj} \in Y_u$.

Improved login phase: Assume that at time T, user u requires the service y_{uj}. He inserts his smart card to a card reader and constructs the request message L_{uj}. Essentially, the request message is a signature of user u on the public key ID_u and the desired service y_{uj}. The following steps describe the details of the signing procedure.

Step 1. Selects an integer $k \in_R Z_q$, and computes the quantities $r = g^k \; mod \; p$, $H = h(r, T, ID_u, r_{uj}, s_{uj}, y_{uj})$, $s = (k\,H + x_u\, r) \; mod \; q$. If $r = 0 \; mod \; q$, repeats this step.

Step 2. Constructs the request message $L_{uj} = \{r, s, T, ID_u, r_{uj}, s_{uj}, y_{uj}\}$ and sends it to the server.

Improved verification phase: On receiving the request message L_{uj}, the server will verify two signatures: (ID_u, r_{uj}, s_{uj}) and $((T, ID_u, r_{uj}, s_{uj}, y_{uj}), r, s)$. The first signature is issued from CA using the private key x_{uj}, and the second one is a signature signed by user u. A detailed description of the verification is given below. Assume that the request message L arrived at time T'.

Step 1. Reject the request if $(T' - T)$ is greater than the legal transmission time.

Step 2. Use the equation $g^{s_{uj}} = r_{uj}^{h(r_{uj}, ID_u)} \, y_{uj}^{r_{uj}} \; mod \; p$ to confirm that (ID_u, r_{uj}, s_{uj}) is a valid certificate to the public key ID_u.

Step 3. Calculate the quantity of message digest $H = h(r, T, ID_u, r_{uj}, s_{uj}, y_{uj})$.

Step 4. Verify the second signature by the equation $g^s = r^H \, ID_u^r \; mod \; p$. Grants the service y_{uj} to user u, if he passes Step 1 to Step 4. Otherwise, denies services to user u.

5. Analysis of security

The security of the request message has been proven to be secure against the adaptive chosen message attack in the reviewed scheme. In this section, an attempt to prove that the access control system has the same strength of security. Every user in the system has obtained a set of signatures issued by CA using the secret keys of services. Lemma 1 will show that the quantities of signatures s_{ua}, s_{ub}, s_{va}, and s_{vb} are independent of each other. Thus, the security of the access control system is reduced to the security of digital signatures. Since the digital signatures used in the improved registration phase has been proven to be secure against the adaptive chosen message attack in the schemes [5, 7-8], it is proven that the improved access control has this strength of security.

Lemma 1. Assume that user u has obtained signatures s_{ua} and s_{ub}, and user v has received signatures s_{va} and s_{vb}. These signatures are mutually independent, if they are calculated according to (6) in the improved registration phase.

Proof. The four signing equations are listed below.

$$s_{ua} = h(r_{ua}, ID_u)\, k_{ua} + r_{ua}\, x_a \; mod \; q \qquad (7)$$
$$s_{ub} = h(r_{ub}, ID_u)\, k_{ub} + r_{ub}\, x_b \; mod \; q \qquad (8)$$
$$s_{va} = h(r_{va}, ID_v)\, k_{va} + r_{va}\, x_a \; mod \; q \qquad (9)$$
$$s_{vb} = h(r_{vb}, ID_v)\, k_{vb} + r_{vb}\, x_b \; mod \; q \qquad (10)$$

The four numbers k_{ua}, k_{ub}, k_{va}, and k_{vb} are selected randomly from Z_q, therefore, they are mutually independent. Consequently, s_{ua}, s_{ub}, s_{va}, and s_{vb} are also mutually independent. □

Lemma 2. The signatures issued to users are mutually independent with overwhelming probability.

Proof. Assume that there are n users and each user has no more m access rights. Hence, Lemma 1 holds true, if $m\, n << q$. □

Lemma 3. The security of the access control system can be reduced to the security of digital signatures.

Proof. Assume that the check on the differences between timestamp T' and T (Step 1) is sufficient to safeguard the improved scheme from replay attack (A three moves identification protocol could be used, when in doubt about the security of using timestamp.). The security of the request message (Step 3 and 4) has been proven in scheme [5]. Therefore, the security of the access control system is reduced to verifying the certificates in Step 2.

A valid certificate (ID_u, r_{uj}, s_{uj}) is a necessary condition for the server granting service y_j to user u. However, to forge a valid certificate is to forge a signature s_{uj}. Thus, we have proven this lemma. □

Theorem 4. The access control system is secure against the adaptive chosen message attack.

Proof. The digital signatures generated by (6) have been proven to be secure against the adaptive chosen message attack [5, 7-8]. Hence, Theorem 4 is proven, by Lemma 3. □

6. Conclusions

It has been shown that the users in the reviewed scheme can deduce the differences between private keys. With this information, users are able to counterfeit certificates so as to intrude into the access control system. An improvement to remedy this flaw is proposed. The improvement is proven to be secure under the adaptive chosen message attack. Thus, the improvement is not only to mend a flaw, but also to protect the scheme from other undetected flaws.

References

1. A. Silberschatz, P. B. Galvin, and G. Gagne, “Operating Systems Concepts,” Sixth Edition. John Wiley & Sons, 2001.
2. L. Lamport, “Password authentication with insecure communication,” *Communications of ACM*, Vol. 24, pp. 770-772, 1981.
3. L. Harn and H. N. Lin, ”Integration of user authentication and access control,” *IEE Proceedings-E*, 139, (2), pp. 139-143, 1992.
4. N. Y. Lee, ”Integrating access control with user authentication using smart cards,” *IEEE Transactions on Consumer Electronics*, 46, (4), pp. 943-948, 2000.
5. F. Y. Yang and J. K. Jan, ”A provable access control using smart cards”, *IEEE Transactions on Consumer Electronics*, 49, (4), pp. 1223-1226, 2003.
6. S. Goldwasser, S. Micali, and R. Rivest, “A digital signature scheme secure against adaptive chosen-message attacks,” *SIAM journal of computing*, Vol. 17, No. 2, pp. 281-308, 1988.
7. D. Pointcheval and J. Stern, “Security proofs for signature schemes,” *Advances in Cryptology-EUROCRYPT’96*, LNCS 1070, pp. 387-398, 1996.
8. D. Pointcheval and J. Stern, “Security arguments for digital signatures and blind signatures,” *Journal of Cryptology*, Vol. 13, N0. 3, pp. 361-396, 2000.