# 應用在分散式系統中有效率的使用者認證暨存取控制機制

# Efficient Access Control Scheme with User Authentication for Distributed Systems

李南逸　　何佩修
Narn-Yih Lee and Pei-Hsiu Ho

南台科技大學資訊管理研究所
Information Management Department
Southern Taiwan University of Technology
Tainan, Taiwan, Republic of China

摘　要

學者 Jan 和 Tseng 在 1998 年提出了兩個應用在分散式環境下的使用者認證和存取控制的機制。 然而 He、Wu 和 Lee 指出該機制是不安全的。本篇論文的目的是提出一個改進 Jan 和 Tseng 的第一個機制，並且解決 Lee 的論文中所提到的尚待解決的問題。本篇論文所提出之機制比 He 和 Wu 的第一個機制更有效率。

關鍵詞：密碼學、存取控制、使用者認證

**Abstract**

Jan and Tseng, in 1998, proposed two integrated schemes of user authentication and access control that provide a data protection system for distributed environments. However, He-Wu and Lee showed that both schemes are insecure, respectively. He-Wu and Lee also presented some improvements to withstand the proposed security flaws. The aim of the paper is to propose an improvement of Jan-Tseng's first scheme and solve the open problem in Lee's paper. The proposed scheme is also more efficient than He-Wu's first scheme.

**Keyword**：Cryptography、Cryptanalysis、Access control、User authentication

## 1. Introduction

In order to prevent the electronic data from being unauthorized access, some data protection mechanisms are required in the modern computer systems. Traditionally, access control schemes [1]-[3] and user authentication schemes [4]-[6] are proposed separately for data protection in a computer system. In 1992, Harn and Lin [7] first proposed a scheme for the integration of access control and user authentication. Then, Yen and Laih [8][9] improved the efficiency of the Harn-Lin scheme [7].

In 1998, Jan and Tseng [10] further extended the data protection systems for distributed computer systems. Two new integrated access control schemes with user authentication were proposed in [10]. The first scheme has dynamic property in that it provides an efficient updating

process for modification of access rights. The second scheme provides an efficient verification process on the servers for multiple access requests by a user at the same time. Unfortunately, He-Wu [11] and Lee [12] showed that both Jan-Tseng's schemes are insecure, respectively. In [11], He-Wu presented two simple corrections to withstand the proposed attacks. In [12], Lee also offered an efficient improvement of Jan-Tseng's second scheme to repair the security flaws. Meanwhile, Lee also announced an open problem in designing a scheme which can satisfy six considerations for user authentication and access control. The aim of the paper is to propose an improvement of Jan-Tseng's first scheme (JTF scheme in short). The proposed scheme is also more efficient that He-Wu's first scheme.

This paper will present an improved scheme which can achieve both user authentication and access control simultaneously. The security of the improved scheme is based on the difficulty of solving the discrete logarithm problem. The organization of this paper is as follows. We give a brief review of Jan-Tseng's first scheme in Section 2. Then, the improved scheme and the security analysis are given in Section 3 and Section 4, respectively. Finally, Section 5 concludes this paper.

## 2. Review of the JTF Scheme

This section reviews the JTF scheme [10]. The JTF scheme involves three parties of JTF scheme ：a *Central Authority* (*CA*), *Servers*, and *Users*. The *CA* is responsible for setting up the system parameters and assigning the access rights and the corresponding passwords for each user. The access rights and passwords are stored in a smart card. The smart card will send to the user secretly. Each *server* is responsible for user authentication and provides access services for the authorized users. But, it is noted that no secret information about the system or authorization data about the user is stored in the servers. Each *user* holds a smart card and may request different services from different servers.

### 2.1 The JTF Scheme

*Initialization phase*: The *CA* chooses a large prime number $p$ and an integer $g$, where $p$-1 has a large prime factor, $g$ is a primitive element of $GF(P)$. Assume there are $n$ access rights in the system. For each access rights, the *CA* chooses a secret $x_i$ randomly, where $1< x_i< p-1$, and $X=\{x_0,x_1,\ldots,x_{n-1}\}$. The *CA* computed public values $y_i = g^{x_i} \bmod p$, where $i$ =0, 1, 2 ..., $n$-1.

*Registration phase*: Assume that a user $u$ is to be grated $m$ access rights $y_{uj}$, $y_{uj} \in \{y_{u0}, y_{u1}, y_{u2}, ..., y_{u,n-1}\}$ , $0 \le j \le m-1$ , $m \le n$. For a user $u$, the *CA* randomly chooses a $pw_u$, for $1< pw_u<p-1$, $gcd(pw_u, p-1)=1$, and computes $ID_u = g^{pw_u} \bmod p$ . Then, the *CA* chooses an integer $k_u$, and computes $r_u = g^{k_u} \bmod p$ for $1< k_u <p-1$. The *CA* finds $m$ integers $S_{uj}$ to satisfy the following equation,

$ID_u \cdot x_{uj} + k_u \cdot y_{uj} = pw_u \cdot S_{uj} \bmod p-1$ , for $1<j<m-1$. Finally, the *CA* stores $pw_u$, $ID_u$, $r_u$, $y_{uj}$ and $S_{uj}$ to a smart card and delivers the smart card to the user $u$ secretly.

*Login phase*: If a user $u$ requests a service to some server for access right $y_{uj}$, then he/she attaches his/her smart card to a terminal. The smart card first randomly chooses an integer $R$, for $1 < R < p-1$, then computes $M=g^R \bmod p$, $H=h(M, T, ID_u)$, and $N = R + pw_u \cdot H \bmod(p-1)$. Here $h$ is an one way hash function [13] and $T$ is a time stamp. Finally, the smart card sends the message $L=\{ID_u, r_u, y_{uj}, S_{uj}, M, N, T\}$ to the server.

*Verification phase*: The server verified the access request $L$ for two steps.

**Step 1**：The server checks if $T'$-$T$ is less than the legal time interval for transmission delay, then the server receives the request. If it is else, the server rejects the request. Here, $T'$ is the time that the server receives the access request.

**Step 2**：The server computes $H=h(M,T,ID_u)$ and verifies whether the following equation holds or not,

$g^{N \cdot S_{uj}} ? = M^{S_{uj}} (y_{uj}^{ID_u} \cdot r_u^{y_{uj}})^H \bmod p$ .

If it is true, the server accepts the access request of the user $u$.

## 3. The Proposed Scheme

This section will present a cryptographic scheme to improve the security and efficiency of the JTF scheme.

The proposed scheme also involves three parties: a *Central Authority*, *Servers*, and *Users*. These three parties play the same roles as in the Section 2.

*Initialization phase*： System parameters $p$ and $g$ are selected by the *CA* as in the Section 2.1. Then, the *CA* chooses a secret $x_i$, $1< x_i <p-1$, and computes $y_i = g^{x_i} \bmod p$ , $0 \le i \le n-1$ . Let $Y=\{y_0,y_1,...,y_{n-1}\}$, and $X=\{x_0,x_1,...,x_{n-1}\}$.

*Registration phase*： Suppose that a user $u$ is to be granted $m$ access rights $y_{uj}$, $0 \le j \le m-1$ , $m \le n$ and $y_{uj} \in \{y_{u1}, y_{u2},..., y_{u,m-1}\}$. The *CA* chooses an integer $pw_u$, for $1< pw_u <p-1$, $gcd(pw_u,p-1)=1$, and computes $ID_u = g^{pw_u} \bmod p$ for the user $u$. Then, the *CA* chooses a random $k_u$, and computes $r_u = g^{k_u} \bmod p$, $1< k_u <p-1$. The *CA* finds $m$ integers $S_{uj}$ to satisfy the following equation $ID_u \cdot x_{uj} + r_u \cdot k_u \cdot y_{uj} = (pw_u + S_{uj}) \bmod p-1$, for $1 \le j \le m-1$. Finally, the *CA* stores $\{pw_u, ID_u, r_u, y_{uj}\}$ to a smart card and delivers it to the user secretly.

*Login phase*： If a user $u$ requests a service to some server for access right $y_{uj}$, the smart card executes the following operations.
First, the smart card chooses an integer $R$ randomly, for $1< R <p-1$, then computes $M=g^R \bmod p$, $H=h(M, T, ID_u)$, and $N = R + (pw_u + S_{uj}) \cdot H \bmod(p-1)$. Here, $h$ is an one way hash function and $T$ is used as a time stamp. The smart card finally sends the message $L=\{ID_u, r_u, y_{uj}, M, N, T\}$ to the server.

*Verification phase*： The access request $L$ is verified by the server as follows.
**Step 1**：The server checks $(T'-T)$ is less than the legal time interval and $y_{uj} \in Y$ . If not, the server rejects the request.
**Step 2**： The server computes $H=h(M,T, ID_u)$ and verifies whether the following equation holds or not.

$$g^N \stackrel{?}{=} M(y_{uj}{}^{ID_u} \cdot r_u{}^{r_u \cdot y_{uj}})^H \bmod p$$

If it is true, the server accepts the request of the user $u$. The correctness of the above equation can be verified as follows.

$$\begin{aligned} & M(y_{uj}{}^{ID_u} \cdot r_u{}^{r_u \cdot y_{uj}})^H \bmod p \\ &= M(g^{x_{uj} \cdot ID_u} \cdot g^{k_u \cdot r_u \cdot y_{uj}})^H \bmod p \\ &= M(g^{x_{uj} \cdot ID_u + k_u \cdot r_u \cdot y_{uj}})^H \bmod p \\ &= g^R \cdot g^{(pw_u + S_{uj}) \cdot H} \bmod p \\ &= g^{R+(pw_u + S_{uj}) \cdot H} \bmod p \\ &= g^N \bmod p \end{aligned}$$

# 4 Discussions and Analysis

## 4.1 Security analysis

In this section, we will show that the improved scheme is secure and can withstand the attacks in [11] and [12].

(1) The secret key $x_i$ of the *CA* can not be derived.
To derive $x_i$ from the corresponding $y_i = g^{x_i} \bmod p$ , the intruder must solve the discrete logarithm problem. If a user $u$ wants to derive *CA*'s secret key $x_{uj}$, he/she may use the equation $ID_u \cdot x_{uj} + r_u \cdot k_u \cdot y_{uj} = (pw_u + S_{uj}) \bmod p-1$ , to reveal $x_{uj}$. But, $pw_u$ is protected by the smart card, the user $u$ can not retrieve it. Besides, $k_u$ is a number chosen by the *CA*. To get $k_u$ from $r_u = g^{k_u} \bmod p$ , it is equivalent to solve discrete logarithm problem. Thus, to reveal $x_{uj}$ is very difficult.

(2) An intruder can not retrieve $pw_u$ from the intercepted message $L=\{ID_u, r_u, y_{uj}, M, N, T\}$.
An intruder wants to retrieve $pw_u$ from $N = R + (pw_u + S_{uj}) \cdot H \bmod(p-1)$, he/she has to find $R$ first. But, to find $R$ from $M=g^R \bmod p$ is equivalent to solve the discrete logarithm problem.

(3) The replay attack will fail.
If an intruder replays a previously intercepted message $L=\{ID_u, r_u, y_{uj}, M, N, T\}$ to a server at the time $T'$ and the server received the message $L$ at

the time $T''$. $T''$-$T$ will be larger than the legal time interval, so the server will reject the request. If the intruder replaces the time $T$ with $T'$, the equation $H=h(M,T',r_u)$ will not hold.

(4) He-Wu's attacks can not work on the proposed scheme.
According to the attack 1 in [11], the intruder has to find an $s'_{uj}$ from the equation

$$s'_{uj} = s_{uj} \cdot (h(ID_u, M, T))^{-1} \cdot h(ID_u, M, T') \mod(p-1).$$

But the parameter $s_{uj}$ is not used in the proposed scheme. So, the He-Wu's attack 1 will not work in the proposed scheme. According to the attack 2 in [11], the intruder has to find a $r'_u$ to satisfy the equation

$$r'^{\,r'_u \cdot y_{uj}}_u = (g^N \cdot M^{-1})^{H^{-1}} \cdot y_{uj}^{-ID_u} \bmod p.$$

However, the intruder is hard to do it without knowing the discrete logarithm of $y_{uj}$. So, the He-Wu's attack 2 fails in the proposed scheme.

(5) Lee's attacks can not work on the proposed scheme.
According to the attack 1 in [11], an intruder first chooses a random number $N'$ and computes $M'=g^{N'} \bmod p$, $H'=h(M',T',ID_u)$. Then, the intruder has to find a $r'_u$ to satisfy the equation

$$r'_u = y_{uj}^{-ID_u \cdot r_u^{-1} \cdot y_{uj}^{-1}} \bmod p.$$

Without the knowledge of $x_{uj}$, the intruder is very difficult fo find the $r'_u$. According to the attack 2 in [11], the intruder first choose two numbers $r'_u$ and $N'$ and compute

$$M' = g^{N'} \cdot [y_{uj}^{ID_u} \cdot r'^{\,r'_u \cdot y_{uj}}_u]^{-1} \bmod p \ , \quad H'=h(M', T', ID_u),$$

and let $s_{uj}=H'$. But, the parameter $s_{uj}$ is not used in the verification equation of the newly proposed scheme. Thus, Lee's attack 2 can not work.

### 4.2 Discussions

In order to design a practical access control scheme with user authentication in a distributed computer system, the criteria which Jan-Tseng proposed in [10] are crucial.

The JTF scheme, He-Wu's first scheme and our scheme comply with the criteria C1-C5, but not C6. Note that our scheme is securer than the JTF scheme. Moreover, our scheme is more efficient than He-Wu's first scheme in signature verification process. The performance analysis of the JTF scheme, He-Wu's first scheme and our scheme in the number of modular exponentiations is listed in the Table 1.

**Table 1.** The number of modular exponentiations required in the schemes.

| | **JTF scheme** | **He-Wu's scheme** | **Our scheme** |
|---|---|---|---|
| Login phase | 1 | 1 | 1 |
| Verification phase | 4 | 4 | 3 |

## 5 Conclusions

We have presented an improvement of the Jan-Tseng's first scheme. It provides an efficient updating process for the modification of the access rights. The security of the proposed scheme is based on the discrete logarithms problem. The proposed scheme is secure from the Lee and He-Wu's attacks and more efficient than the original Jan-Tseng and He-Wu's first scheme.

### References


[1] J.K. Jan, "A Single Key Access Control Scheme in Information Protection System", *Inf. Sci.*, Vol. 50, pp.1-11, 1990.

[2] J.K. Jan, C.C. Chang and S.J. Wang, "A New Dynamic Key-Lock-Pair Access Control Scheme", *Comput. Security*, Vol. 10, No. 2, pp.129-139, 1991.

[3] C.S. Laih, L. Harn and J.Y. Lee, "On the Design of Single-Key-Lock Mechanism Based on Newton's Interpolating Polynomials", *IEEE Trans.*, Vol. SE-10, No. 2, pp.185-191, 1984.

[4] C.C. Chang, S.M. Tsu, and C.Y. Chen, "Remote Scheme for Password Authentication Based on Theory of Quadratic Residues", *Comput. Commun.*, Vol. 18, No. 12, pp.932-946, 1995.

[5] D.E. Denning, "Cryptography and Data Security", *Addison-Wesley*, Reading, 1982.

[6] T.Y.C. Woo and S.S. Lam, “Authentication for Distributed Systems”, *IEEE Comput.*, Vol. 25, pp.39-52, 1992.
[7] L. Harn and H.Y. Lin, “Integration of User Authentication and Access Control”, *IEE Proc.-Comput. Digit. Tech.*, Vol. 139, No. 2, pp.139-143, 1992.
[8] S.M. Yen and C.S. Laih, “Analysis and Improvement of an Access Control Scheme with User Authentication”, *IEE Proc.-Comput. Digit. Tech.*, Vol. 141, No. 5, pp.271-273, 1994.
[9] S.M. Yen and C.S. Laih, “The Design of Dynamic Access Control Scheme with User Authentication”, *Comput. Math. Appl.*, Vol. 25, No. 7, pp.27-32, 1993.
[10] J.K. Jan and Y.M. Tseng, “Two Integrated Schemes of User Authentication and Access Control in a Distributed Computer Network”, *IEE Proc.-Comput. Digit Tech.*, Vol. 145, No. 6, 1998, pp. 419-424.
[11] W.-H. He and T.-C. Wu, “Security of the Jan-Tseng Integrated Scheme for User Au thentication and Access Control”, *IEE Proc.-Comput. Digit. Tech*, Vol. 147, No. 5, 2000, pp.365-368.
[12] N.Y. Lee, “Cryptanalysis and Improvement of Two Access Control Schemes with User Authentication in a Distributed Computer Network”, *IEICE Trans. Inf. and Sys.*, Vol E85-D, NO.2, 2002, pp.386-391.
[13] NIST, Secure Hash Standard. FIPS (Federal Information Processing Standards) publication 180, 1993.