Copyright ⓒ 2013 KSII

An Extended Multi-Server-Based User Authentication and Key Agreement Scheme with User Anonymity

Chun-Ta Li[1], Cheng-Chi Lee[2,3], Chi-Yao Weng[4] and Chun-I Fan[4]
[1] Department of Information Management, Tainan University of Technology
529 Zhongzheng Road, Tainan City 71002, Taiwan
[2] Department of Library and Information Science, Fu Jen Catholic University
510 Jhongjheng Road, New Taipei City 24205, Taiwan
[3] Department of Photonics and Communication Engineering, Asia University
500 Lioufeng Road, Taichung City 41354, Taiwan
[4] Department of Computer Science and Engineering, National Sun Yat-sen University
70 Lienhai Road, Kaohsiung City 80424, Taiwan
[e-mail: th0040@mail.tut.edu.tw, cclee@mail.fju.edu.tw, cyweng@mail.cse.nsysu.edu.tw]
*Corresponding author: Cheng-Chi Lee

Received May 5, 2012; revised July 7, 2012; revised August 24, 2012; accepted September 3, 2012; published January 29, 2013

Abstract

With the explosive growth of computer networks, many remote service providing servers and multi-server network architecture are provided and it is extremely inconvenient for users to remember numerous different identities and passwords. Therefore, it is important to provide a mechanism for a remote user to use single identity and password to access multi-server network architecture without repetitive registration and various multi-server authentication schemes have been proposed in recent years. Recently, Tsaur et al. proposed an efficient and secure smart card based user authentication and key agreement scheme for multi-server environments. They claimed that their scheme satisfies all of the requirements needed for achieving secure password authentication in multi-server environments and gives the formal proof on the execution of the proposed authenticated key agreement scheme. However, we find that Tsaur et al.'s scheme is still vulnerable to impersonation attack and many logged-in users' attack. We propose an extended scheme that not only removes the aforementioned weaknesses on their scheme but also achieves user anonymity for hiding login user's real identity. Compared with other previous related schemes, our proposed scheme keeps the efficiency and security and is more suitable for the practical applications.

Keywords: Identity, key agreement, password, smart card, multi-server architecture, user anonymity, user authentication

This work was supported by the National Science Council of the Taiwan under grants NSC 101-2221-E-165-002, NSC 101-2221-E-030-018, NSC 100-2219-E-110-005, NSC 101-2219-E-110-003 and NSC 101-2219-E-110-005.

http://dx.doi.org/10.3837/tiis.2013.01.008

1. Introduction

Nowadays, numerous network resources and services have been developed and people can access desired services, exchange invaluable knowledge, and process office routine in multi-server environments. In order to protect remote servers from illegitimate access by unauthorized users, remote user authentication has been becoming extremely important and a two-factor (password and smart card) authentication is the most accepted and widely used mechanism due to its easy-implementation and low-cost advantages [3][6][7][8][9][10][13][17]. However, it is extremely inconvenient for users to remember numerous different identities and passwords when users adopt the single-server authentication scheme to access different remote servers. Therefore, single registration is an important issue and a user only needs to register once to access all remote servers in multi-server environments without repetitive registration. Moreover, a good multi-server authentication scheme should be applied in practice and meet the following security and functionality requirements:

1. Security requirements:
- Resistance to password disclosure and session key disclosure to any other users such as online/offline password guessing attacks and session key disclosure attacks.
- Resistance to maintenance problems in server side such as stolen-verifier attacks and insider compromised attacks.
- Resistance to various communication attacks such as replay attacks, man-in-the-middle attacks and impersonation attacks.
- Resistance to power analysis attacks even if a user's smart card is lost or someone steals his/her smart card.
- Resistance to many logged-in users' attacks even if a user's secret parameters are intentionally leaked to more than one non-registered users.

2. Functionality requirements:
- Allow users to freely choose his/her identity and passwords.
- Provision of mutual authentication between users and servers.
- Provision of low communication cost and computation complexity.
- Provision of session-key agreement with perfect forward/backward secrecy between users and servers.
- Provision of a fair session-key agreement mechanism and nobody has an unfair advantage in controlling the session key.
- Provision of service period management and a server can give each user different time limit of access control according to his/her payment.
- Provision of user anonymity and a user's true identity and location cannot be traced by any adversaries.

Up to now, many multi-server authentication schemes with smart card have been proposed in the literatures. In 2001, Li et al. proposed a user authentication scheme using neural networks and asymmetric key cryptosystems [5]. For enhancing the efficiency of Li et al.'s scheme, in 2003, Lin et al. proposed a multi-server authentication scheme [11] and the security of their scheme is based on discrete logarithm. In 2004, Juang proposed an efficient multi-server authentication scheme [2] based on lightweight one-way hashing function and

Copyright ⓒ 2013 KSII

symmetric key cryptosystem. However, in the same year, Chang and Lee [1] demonstrated that Juang's scheme is insecure and suffers from off-line dictionary attack. In 2008, Tsai proposed a multi-server authentication scheme [14] without maintaining a verifier table. However, Tsai's protocol suffers from impersonation attack and any attacker who intercepts a login message sent from a user can resubmit it to the server for gaining illegal access. In 2012, Tsaur et al. proposed an efficient and secure multi-server authentication scheme with key agreement to tackle these security problems [15] and provided a service period management for checking the service period of users. If a user's service period has expired, the server can delete his/her account and stop the service authority. However, through carefully analysis, we find that Tsaur et al.'s scheme is still vulnerable to impersonation attack and many logged-in users' attacks. Furthermore, all the above password authentication protocols for multi-server environment are based on static identity and user's login identity is changeless and sent in the form of plain-text via public channels. It gives the attacker an opportunity to intercept the login ID from the public channels, use it to trace the legal user and damage user privacy over public networks. Therefore, we consequently propose an extended multi-server authentication scheme to withstand aforementioned attacks and meanwhile achieve user anonymity.

The rest of the paper is organized as follows: Section 2 briefly reviews Tsaur et al.'s authentication scheme and shows a cryptanalysis of Tsaur et al.'s scheme in Section 3. Our extended scheme is proposed in Section 4. The security and performance analyzes of the proposed scheme are presented in Section 5 and Section 6. Finally, we draw our conclusions in Section 7.

2. Review of Tsaur et al.'s Scheme

Tsaur et al.'s scheme [15] contains two phases namely: registration phase and the log-in and session key agreement phase. The notations used throughout this paper are summarized in **Table 1** Tsaur et al.'s scheme involves three participants: the registration center (*RC*), the service providing server (S_j) and the user (U_i). *RC* is a trusted party and it is responsible for registration of U_i and S_j. When S_j register with *RC* use identity SID_j, *RC* computes the key $w_j = h(x||SID_j)$ shared between it and S_j. Then *RC* sends w_j to S_j via a secure channel. Detailed steps of two phases are described as follows.

2.1 Registration Phase

When a user U_i wants to get the service granted from S_j and the service period of S_j for U_i is E_T_{ij}. U_i must perform registration with *RC*. U_i chooses his/her identity UID_i and password PW_i and submits them to the registration center *RC* through a secure channel. Upon receiving the registration request, *RC* will perform the following steps:

Step 1: Compute U_i's secret information $v_i = h(x+1, UID_i)$ and $\mu_i = v_i \oplus h(PW_i)$.

Step 2: Compute the secret key $v_{ij} = h(v_i, SID_j)$ shared between U_i and S_j.

Step 3: Compute the authentication parameter $A_{ij} = E_{w_j \oplus E\_T_{ij}}(v_{ij})$ for U_i to log in S_j.

Step 4: Store (UID_i, μ_i, E_T_{ij}, A_{ij}) to the memory of a tamper-resistant smart card and issue it to U_i.

Table 1. Notation used in this paper

Notations	Description
U_i	The *i*th user
S_j	The *j*th server
RC	The registration center
UID_i	The identity of U_i
PW_i	The password of U_i
SID_j	The identity of S_j
x	The secret key of RC
w_j	The secret key shared between S_j and RC
E_T_{ij}	The service period of S_j for U_i
v_{ij}	The secret key shared between U_i and S_j
ru_k	A random number chosen by U_i's smart card for session key agreement
rs_k	A random number chosen by S_j for session key agreement
sk_k	The *k*th session key
$E_k(.)$	The encryption function with key *k*
$D_k(.)$	The decryption function with key *k*
$h(.)$	A collision free one-way hash function
$\oplus$	The bitwise exclusive-OR operation
$\|\|$	The message concatenation operation
T	A timestamp chosen by S_j
t_{now}	S_j's current date and time
ΔT	The endurable transmission delay from S_j to U_i

2.2 Log-In and Session Key Agreement Phase

In this phase, we assume that U_i wants to log in the server S_j and asks a service from S_j. U_i inserts his/her smart card to a card reader and inputs password PW_i. Then the smart card performs the following steps:

Step 1: The smart card computes $v_i = \mu_i \oplus h(PW_i)$, $v_{ij} = h(v_i, SID_j)$ and $E_{v_{ij}}(ru_k, h(UID_i))$ and transmits a log-in message $M_{ij} = \{E\_T_{ij}, A_{ij}, UID_i, E_{v_{ij}}(ru_k, h(UID_i))\}$ to S_j, where ru_k is a *k*th random number chosen by U_i and it is larger than 160 bits.

Step 2: After receiving M_{ij} from U_i, S_j validates the format of UID_i and the service period of E_T_{ij}. If they are not valid, S_j will terminate the service to U_i. Otherwise, S_j derives v_{ij} by computing $D_{w_j \oplus E\_T_{ij}}(A_{ij})$ and employs v_{ij} to reveal ru_k and $h(UID_i)$ by computing $D_{v_{ij}}(E_{v_{ij}}(ru_k, h(UID_i)))$. Then S_j will reject this log-in if the authentication tag $h(UID_i)$ is not valid; otherwise, S_j computes the *k*th session key $sk_k = h(rs_k, ru_k, v_{ij})$ and responses a message $E_{v_{ij}}(rs_k, ru_k, T)$ to U_i, where T is a current timestamp generated by S_j and rs_k is a *k*th random number chosen by S_j and it is larger than 160 bits.

Step 3: Upon receiving the response message from S_j, U_i's smart card reveals (rs_k, ru_k, T) by computing $D_{v_{ij}}(E_{v_{ij}}(rs_k, ru_k, T))$ and checks the validity of ru_k. If it holds, U_i's smart

Copyright ⓒ 2013 KSII

card computes the *k*th session key $sk_k = h(rs_k, ru_k, v_{ij})$ and sends $E_{sk_k}(T, sk_k)$ to S_j; otherwise, this connection will be terminated.

Step 4: Upon receiving $E_{sk_k}(T, sk_k)$ from U_i, S_j reveals (T, sk_k) by computing $D_{sk_k}(E_{sk_k}(T, sk_k))$ and checks if $t_{now} - T < \Delta T$. If it does not hold, S_j terminates this log-in; otherwise, S_j further checks the correctness of sk_k. If the session key is correct, both U_i and S_j can use sk_k for securing subsequent communications.

3. Cryptanalysis of Tsaur et al.'s Scheme

Although Tsaur et al. claimed that their protocol can resist many types of attacks and satisfy all the essential requirements for multi-server architecture authentication. Tsaur et al.'s scheme assumed that the credential is stored in the memory of a tamper-resistant smart card. However, many previous researchers have stated that the secret values stored in a smart card can be easily extracted by monitoring its power consumption [4][12]. Therefore, Tsaur et al.'s scheme may suffer from power analysis attacks and have some practical security pitfalls. The cryptanalysis of Tsaur et al.'s scheme has been made in this section and the detailed cryptanalysis is presented as follows.

3.1 Impersonation Attack

In Tsaur et al.'s scheme, we know that server S_j can derive v_{ij} from U_i's authentication parameter A_{ij} and the correct service period E_T_{ij}. Thus, their scheme does not need to maintain a verification table in the server side. However, we find that their scheme may suffer from impersonation attacks and a malicious privileged user U_a who possesses the smart card can easily impersonate other user U_i to login to the server S_j by performing the following steps:

Step 1: U_a extracted the stored values from his/her smart card by monitoring its power consumption [4][12]. As we know, the content of the smart card is $(UID_a, \mu_a, E\_T_{aj}, A_{aj})$.

Step 2: U_a computes $v_a = \mu_a \oplus h(PW_a)$ and $v_{aj} = h(v_a, SID_j)$ and chooses a *k*th random number ru_k.

Step 3: U_a employs U_i's identity UID_i to compute $E_{v_{aj}}(ru_k, h(UID_i))$.

Step 4: U_a uses his/her own authentication parameters E_T_{aj} and A_{aj} to impersonate U_i to make a valid log-in message $M_{aj} = \{E\_T_{aj}, A_{aj}, UID_i, E_{v_{aj}}(ru_k, h(UID_i))\}$ and sends M_{aj} to S_j.

As shown in above-mentioned steps, U_a's authentication parameters E_T_{aj}, A_{aj} and U_i's identity UID_i are legal, so the server S_j accepts the log-in request and Tsaur et al.'s scheme cannot resist the impersonation attack as they claimed.

3.2 Many Logged-In Users' Attack

Tsaur et al.'s scheme, the simultaneous access of a legitimate user's account in the *k*th server by multiple non-registered users using the same identity and password of the user and the server S_j is not aware of having caused problem. We assume that a registered user's smart card is massively duplicated and U_i's password PW_i is intentionally exposed to n non-registered attackers U_x, where $x = 1, 2, \ldots, n$. Then each one who has smart card and knows PW_i can login

to the server S_j at the same time by performing the following steps:

Step 1. Each U_x generates his/her random number ru_x and sends a valid log-in message $M_{ijx} = \{E\_T_{ij}, A_{ij}, UID_i, E_{v_{ij}}(ru_x, h(UID_i))\}$ to S_j, where $x = 1, 2, \ldots, n$.

Step 2. After receiving all the log-in messages $M_{ij1} = \{E\_T_{ij}, A_{ij}, UID_i, E_{v_{ij}}(ru_1, h(UID_i))\}$, $M_{ij2} = \{E\_T_{ij}, A_{ij}, UID_i, E_{v_{ij}}(ru_2, h(UID_i))\}$, …, $M_{ijn} = \{E\_T_{ij}, A_{ij}, UID_i, E_{v_{ij}}(ru_n, h(UID_i))\}$ from $U_1, U_2, \ldots, U_n$, S_j gets the same identity UID_i with different random numbers $ru_1, ru_2, \ldots, ru_n$. Finally, S_j allows all of $U_1, U_2, \ldots, U_n$ to login and accesses U_i's account simultaneously.

4. Our Extended Scheme

In this section, we propose an extended scheme to overcome the security weaknesses of Tsaur et al.'s scheme. Note that our extended scheme does not need to assume that the secret values are stored in the memory of a tamper-resistant smart card. In other words, we assumed in the existence of power analysis attacks and any attacker may maliciously extract the stored values from a smart card by monitoring its power consumption. The extended scheme can prevent impersonation attacks and provide secure services by storing a write protected file in the servers. In addition, the extended scheme guarantees user anonymity by hiding user's true identity during log-in and session key agreement phase. Our extended scheme consists of two phases namely: registration phase and the log-in and session key agreement phase. Fig. 1 is the work flow of the extended scheme and each of two phases is discussed below.

4.1 Registration Phase

When a user U_i wants to get the service granted from S_j, U_i has to submit his/her identity UID_i and PW_i to RC. This phase is extremely similar to Tsaur et al.'s scheme and the major difference is that the authentication parameter, A_{ij}, generated by registration center RC is changed as follows: $A_{ij} = E_{w_j \oplus E\_T_{ij}}(UID_i, v_{ij})$. Note that we integrated user's identity UID_i into the authentication parameter A_{ij}. Moreover, RC submits U_i's identity UID_i and service period E_T_{ij} to S_j and S_j maintains the identity table as depicted in **Table 2**, where the *Status-bit* indicates the status of the user, i.e., when U_i is logged-in to S_j the *Status-bit* is set to one, otherwise it is set to zero. Note that only S_j has authority to modify the stored values of the identity table. Finally, RC stores $(\mu_i, E\_T_{ij}, A_{ij})$ to the memory of a smart card and issue it to U_i.

Table 2. The identity table of S_j after finishing the registration phase

User identity	Service period	*Status-bit*
⋮	⋮	⋮
UID_i	E_T_{ij}	0/1
⋮	⋮	⋮

Copyright ⓒ 2013 KSII

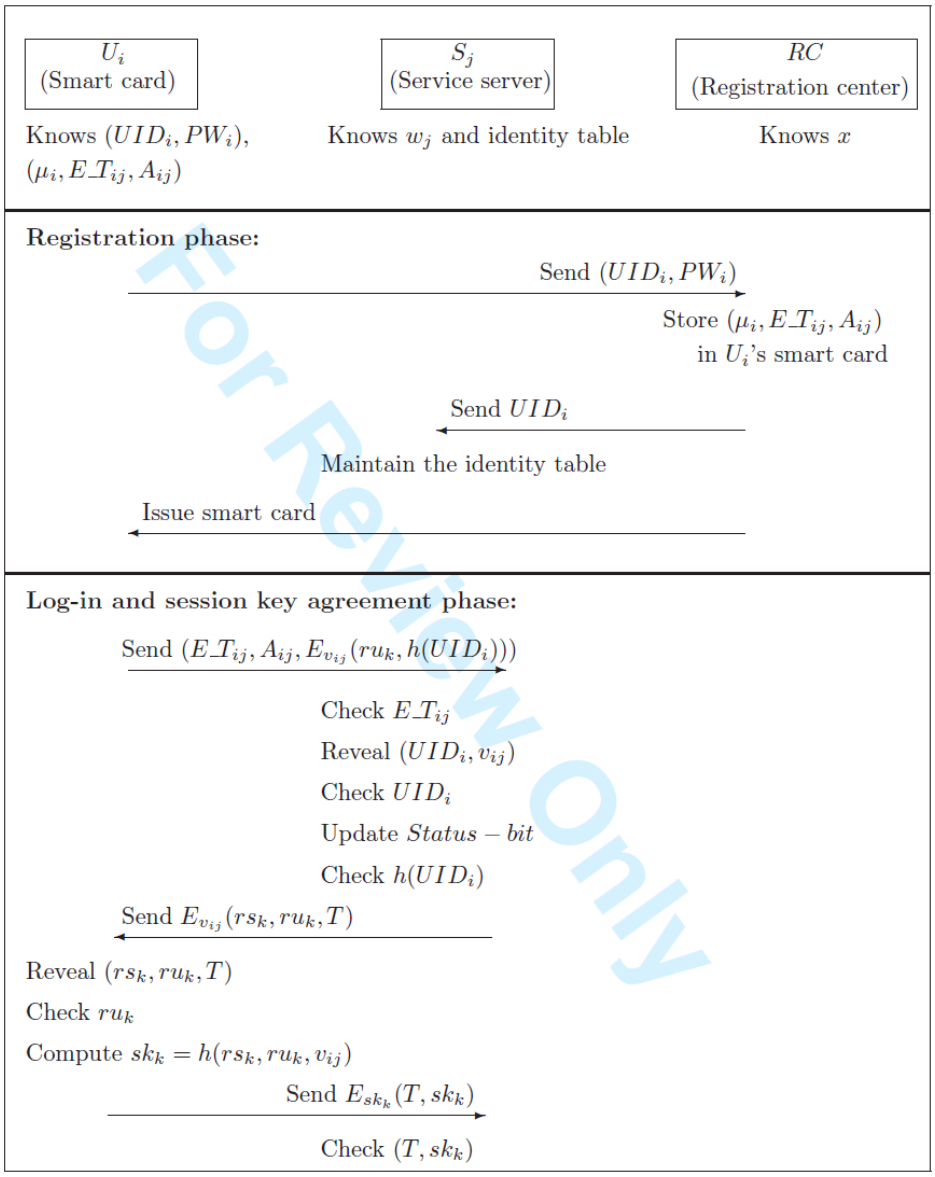

Fig. 1. The extended scheme

For Review Only

4.2 Log-In and Session Key Agreement Phase

In this phase, we assume that U_i wants to log in the server S_j and asks a service from S_j. U_i inserts his/her smart card into the terminal and inputs UID_i and PW_i. Then the smart card performs the following steps:

Step 1: The smart card computes $v_i = \mu_i \oplus h(PW_i)$, $v_{ij} = h(v_i, SID_j)$ and $E_{v_{ij}}(ru_k, h(UID_i))$ and transmits a login message $M_{ij} = \{E\_T_{ij}, A_{ij}, E_{v_{ij}}(ru_k, h(UID_i))\}$ to S_j, where ru_k is a kth random number chosen by U_i and it is larger than 160 bits.

Step 2: After receiving M_{ij} from U_i, S_j validates the service period of E_T_{ij}. If it is not valid, S_j will terminate the service to U_i. Otherwise, S_j derives UID_i and v_{ij} by computing $D_{w_j \oplus E\_T_{ij}}(A_{ij})$ and validate the format of UID_i. If it is valid, the *Status-bit* is set to one and S_j employs v_{ij} to reveal ru_k and $h(UID_i)$ by computing $D_{v_{ij}}(E_{v_{ij}}(ru_k, h(UID_i)))$. Then S_j will accept this log-in if the authentication tag $h(UID_i)$ is valid. Moreover, S_j computes the kth session key $sk_k = h(rs_k, ru_k, v_{ij})$ and responses a message $E_{v_{ij}}(rs_k, ru_k, T)$ to U_i, where T is a current timestamp generated by S_j and rs_k is a kth random number chosen by S_j and it is larger than 160 bits.

Step 3 and Step 4: These two steps are the same as Tsaur et al.'s scheme.

5. Security Analysis

In this section, we analysis the security of our extended scheme and several features of the proposed scheme are discussed as follows. Prior to demonstration of preventing possible attacks, some assumptions of security are given.

Assumption 1. U_i's identity and password are well-protected by the user and securely sent to *RC* in the registration phase.
Assumption 2. There is a secure channel between each server S_j and the control server *RC* in the registration phase.
Assumption 3. During the log-in and session key agreement phase, the attacker U_a has control over the communication channels between U_i and S_j such as eavesdropping, intercepting, inserting and deleting any transmitted messages in these public channels.
Assumption 4. In case of U_i's smart card is stolen by an attacker, the malicious attacker can extract the stored values from someone's smart card by monitoring its power consumption.
Assumption 5. The bit length of (x, ru_k, rs_k) are large enough and these values are high entropy secret key and random numbers.
Assumption 6. Every symmetric key cryptosystem is secure to prevent secret information from cracking and any encrypted message cannot be revealed without having the secret key shared between the sender and receiver.

Using the above security assumptions, we provide proof of the correctness of our extended scheme and evaluate its security with respect to its robustness in the presence of the security requirements presented in Section 1.

Theorem 5.1. *The extended scheme is secured against replay and impersonation attack while ensuring the data integrity of the parties that have participated in a login session over multi-server networks; including U_i and S_j.*

Proof. An attacker U_a may intercept the authentication message M_{ij} and replay the forged authentication message M_{ij}' modified from M_{ij}. Therefore, U_a must change the random number ru_k as ru_k' and compute the corresponding $M_{ij}' = Ev_{ij}(ru_k', h(UID_i))$. However, in the proposed scheme, U_a is unable to compute a valid M_{ij}' without knowing the encryption key v_{ij} and identity UID_i. On the other hand, U_a may intercept the authentication message M_{ij} and try to masquerade as U_i by replaying M_{ij} without modifying any M_{ij}'s content. However, U_a is unable to calculate a valid response $E_{sk_k}(T, sk_k)$ to S_j without knowing the secret key v_{ij}. Therefore,

Copyright ⓒ 2013 KSII

the extended scheme can prevent the replay attacks.

For impersonation attack, the attacker U_a may try to forge a valid log-in message $(E\_T_{ij}, A_{ij}, E_{v_{ij}}(ru_k, h(UID_i)))$ to impersonate as a legitimate user using the previously eavesdropped messages. However, in the proposed scheme, it is intractable for U_a to obtain the secret key $v_{ij} = h(v_i, SID_j)$ because the secret $\mu_i = v_i \oplus h(PW_i)$ is stored in U_i's smart card, only the user who knows the identity UID_i and password PW_i and owns the smart card can get the secret key v_{ij}. As a result, if a random number ru_k' is selected by U_a, U_a still cannot generate a valid $Ev_{ij}(ru_k', h(UID_i))$ to S_j without knowing v_{ij} and UID_i.

Theorem 5.2. *The extended scheme is secured against smart card lost problem.*

Proof. The smart card lost problem is an inherent limitation of user authentication scheme. We found that the best solution is to prohibit the guesstimate chance of the malicious off-line password guessing attack and the secret values stored on the smart card are $(\mu_i, E\_T_{ij}, A_{ij})$ in our extended scheme. We assume that the secret values extracted from user's smart card, it still can not help an attacker U_a to derive or update the user's password without knowing the user's UID_i and PW_i. Moreover, since x is unknown to U_a, he/she cannot calculate $v_i = h(x + 1, UID_i)$ and cannot perform the impersonation attack using the stolen or lost smart card.

Theorem 5.3. *The extended scheme is secured against off-line password guessing and session key disclosure attacks.*

Proof. In the log-in and session key agreement phase of our extended scheme, when a user's identity and password are keyed in, his/her smart card will generate the authentication message M_{ij} and send it to the server S_j. Note that M_{ij} does not contain any information about user's password. Therefore, a malicious server S_j or any external attacker cannot successfully guess user's password from M_{ij} by an off-line manner.

For session key disclosure attack, we assume that kth session key $sk_k = h(rs_k, ru_k, v_{ij})$ is known by an attacker U_a and U_a may try to use it to derive the previous session keys $sk_x = h(rs_x, ru_x, v_{ij})$, where x = 1, 2, …, k-1. However, rs_x and ru_x are random numbers which are different in previous k-1 sessions and v_{ij} is well-protected by U_i and S_j. Therefore, U_a cannot derive the previous session keys sk_x and the proposed scheme can resist the session key disclosure attacks.

Theorem 5.4. *The extended scheme is secured against stolen-verifier and many logged-in users' attacks.*

Proof. The stolen-verifier attacks means that an attacker U_a steals the verifier table from the server and launches an impersonation attack. Thus, U_a can masquerade as a legitimate user U_i to login server. In the proposed scheme, the server maintains an identity table and this table stores all privileged users' identity. Even so, it does not help U_a to make a valid authentication parameter $A_{ij} = E_{w_j \oplus E\_T_{ij}}(UID_i, v_{ij})$ without knowing w_j and the identity table is only used to prevent many logged-in users' attack. So the stolen-verifier attack is prevented in our extended

scheme. In the extended scheme, we assume that the user's secret parameters $(E\_T_{ij}, A_{ij}, v_{ij}, UID_i)$ are leaked to more than one non-registered users. However, the server S_j maintained a status-bit in its identity table and no one allowed to login S_j at the same time out of all who know the valid secret parameters $(E\_T_{ij}, A_{ij}, v_{ij}, UID_i)$. Based on the identity table, we can say that our extended scheme can prevent the many logged-in users' attack.

Theorem 5.5. *The extended scheme ensures anonymous interactions between the user U_i and the server S_j and no outsiders can ascribe any session to a particular user during the log-in and session key agreement phase.*

Proof. In the registration phase of the proposed scheme, U_i's identity UID_i and a secure channel between U_i and the registration center RC are used for protecting the U_i's real identity from disclosure. In the log-in and session key agreement phase, U_i sends the authentication message M_{ij} for its authentication to the server S_j. Note that U_i 's real identity UID_i is encrypted into A_{ij} and it has never transmitted in plaintext over public channels. Therefore, the attacker cannot distinguish different sessions corresponding to a certain user without knowing w_j. Since U_i's real identity UID_i is well-protected for each session when U_i logins to S_j. Therefore, the user anonymity is provided in our proposed scheme.

6. Performance Analysis

In this section, we compare the computational primitives involved in registration and log-in and session key agreement phases of the extended scheme with other previous multi-server authentication schemes [2][14][15] and tabulate the results in **Table 3** Obviously, RC has no need to participate in the user authentication process in our scheme and Tsaur et al.'s scheme [15], and therefore the total computations are lower than Juang's scheme [2]. In addition, Tsai's scheme [14] adopts only 12 computations of one-way hash function to construct a multi-server authentication scheme. Unfortunately, in 2009, Wang et al. [16] indicated that Tsai's scheme cannot resist the server spoofing and the impersonation attacks.

Table 3. Performance comparisons among our extended scheme and other related schemes for multi-server authentication

Compared schemes → **Executive computations ↓**	**The extended scheme**	**Tsaur** [15] **(2012)**	**Tsai** [14] **(2008)**	**Juang** [2] **(2004)**
Computation of user registration	3H + 1S	3H + 1S	2H	1H
Computation of server registration	1H	1H	1H	1H
Computation of user authentication	4H + 3S	4H + 3S	5H	3H + 3S
Computation of server authentication	2H + 4S	2H + 4S	3H	3H + 4S
Computation of *RC* authentication	—	—	1H	1H + 2S
Total computations	10H + 8S	10H + 8S	12H	9H + 9S

H: Time complexity for one-way hash function;
S: Time complexity for symmetric key cryptosystem;
—: No computations.

Copyright ⓒ 2013 KSII

7. Conclusion

This paper proposed a new user anonymously authentication scheme with key agreement for multi-server environments that not only can prevent the deficiencies of Tsaur et al.'s scheme, but also can provide efficiency and security for remote services in multi-server authentication systems. Compared with other previous multi-server authentication schemes, our extended scheme has the following main advantages: (1) It provides secure user anonymity during log-in and session key agreement phase; (2) It provides a service period management for deleting users' accounts once users are stopped the service authority; (3) It does not need to maintain the password verification table stored at the server side; (4) It provides mutual authentication and session key agreement between login user and remote server; (5) It prevents impersonation attacks and many logged-in users' attacks. As a result, the proposed scheme is more suitable for remote services in multi-server environments due to its acceptable computation cost and high level security.

References

[1] C. C. Chang and J. S. Lee, "An efficient and secure multi-server password authentication scheme using smart cards," in *Proc. of 3th International Conference on Cyberworlds*, pp. 417-422, 2004. Article (CrossRef Link)

[2] W. Juang, "Efficient multi-server password authenticated key agreement using smart cards," *IEEE Transactions on Consumer Eletronics*, vol. 50, no. 1, pp. 251-255, 2004. Article (CrossRef Link)

[3] M. S. Hwang, S. K. Chong and T. Y. Chen, "Dos-resistant ID-based password authentication scheme using smart cards," *Journal of Systems and Software*, vol. 83, no. 1, pp. 163-172, 2010. Article (CrossRef Link)

[4] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," *Advances in Cryptology*, pp. 388-397, 1999. http://www.cryptography.com/public/pdf/DPA.pdf

[5] L. H. Li, I. C. Lin and M. S. Hwang, "A remote password authentication scheme for multi-server architecture using neural networks," *IEEE Transactions on Neural Network*, vol. 12, no. 6, pp. 1498-1504, 2001. Article (CrossRef Link)

[6] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1-5, 2010. Article (CrossRef Link)

[7] C. T. Li, C. C. Lee, L. J. Wang and C. J. Liu, "A secure billing service with two-factor user authentication in wireless sensor networks," *International Journal of Innovative Computing, Information and Control*, vol. 7, no. 8, pp. 4821-4831, 2011. http://www.ijicic.org/ijicic-10-03005.pdf

[8] C. T. Li, "Secure smart card based password authentication scheme with user anonymity," *Information Technology and Control*, vol. 40, no. 2, pp. 157-162, 2011. Article (CrossRef Link)

[9] C. T. Li and C. C. Lee, "A robust remote user authentication scheme using smart card," *Information Technology and Control*, vol. 40, no. 3, pp. 236-245, 2011. Article (CrossRef Link)

[10] C. T. Li and C. C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for wireless communications," *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 35-44, 2012. Article (CrossRef Link)

[11] I. C. Lin, M. S. Hwang and L. H. Li, "A new remote user authentication scheme for multi-server architecture," *Future Generation Computer Systems*, vol. 19, no. 1, pp. 13-22, 2003. Article (CrossRef Link)

[12] T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541-552, 2002. Article (CrossRef Link)

[13] R. Ramasamy and A. P. Muniyandi, "An efficient password authentication scheme for smart card," *International Journal of Network Security*, vol. 14, no. 3, pp. 180-186, 2012.

[14] J. L. Tsai, "Efficient multi-server authentication scheme based on one-way hash function without verification table," *Computers & Security*, vol. 27, no. 3-4, pp. 115-121, 2008. Article (CrossRef Link)
[15] W. J. Tsaur, J. H. Li and W. B. Lee, "An efficient and secure multi-server authentication scheme with key agreement," *Journal of Systems and Software*, vol. 85, no. 4, pp. 876-882, 2012. Article (CrossRef Link)
[16] R. Wang, W. Juan and C. Lei, "User authentication scheme with privacy-preservation for multi-server environment," *IEEE Communications Letters*, vol. 13, no. 2, pp. 157-159, 2009. Article (CrossRef Link)
[17] L. Yang, J. F. Ma and Q. Jiang, "Mutual authentication scheme with smart cards and password under trusted computing," *International Journal of Network Security*, vol. 14, no. 3, pp. 156-163, 2012.

Chun-Ta Li received the Ph.D. degree in Computer Science and Engineering from National Chung Hsing University, Taiwan, R.O.C., in 2008. He is currently an assistance professor of the Department of Information Management, Tainan University of Technology, Taiwan, R.O.C. Dr. Li received the 2011 IJICIC Most Cited Paper Award from International Journal of Innovative Computing, Information and Control. Dr. Li is a member of IEEE, a member of Chinese Information Security Association (CCISA), a member of Future Technology Research Association International (FTRA), a member of IFIP WG 11.3, a member of Machine Intelligence Research Labs (MIR Labs), and an editorial board member of International Journal of Network Security (IJNS). His research interests include information security, wireless sensor networks, mobile computing, and security protocols for ad hoc networks. Dr. Li had published more than 50 international journal and international conference papers on the above research fields.

Cheng-Chi Lee received the BSc and MSc in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 1999 and in 2001, respectively. He researched in Computer and Information Science from National Chiao Tung University (NCTU), Taiwan, China, from 2001 to 2003. He received the PhD 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 was 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. From 2010, he is now an assistant professor of Library and Information Science, Fu Jen Catholic University. His current research interests include information security, cryptography, and mobile communications. Dr Lee had published more than 70+ articles on the aforementioned research fields in international journals.

Chi-Yao Weng received the M.S. degree in Computer Science from Nation Pingtung University of Education, Pingtung, Taiwan, in 2007, and Ph. D degree in Computer Science from National Tsing Hua University, Hsinchu, Taiwan, in 2011. He is currently a postdoctoral researcher in Computer Science and Engineering from National Sun Yat-Sen University, Kaohsiung, Taiwan. His current research interests include data hiding, image watermarking, images processing, digital right management, information forensics, and information security.

Copyright ⓒ 2013 KSII

Chun-I Fan was born in Tainan, Taiwan. He received his M.S. degree in computer science and information engineering from National Chiao Tung University, Taiwan, in 1993, and the Ph.D. degree in electrical engineering at National Taiwan University in 1998. From 1999 to 2003, he was an associate researcher and project leader of Telecommunication Laboratories, Chunghwa Telecom Co., Ltd, Taiwan. In 2003, he joined the faculty of the department of computer science and engineering, National Sun Yat-sen University, Kaohsiung, Taiwan, and has been a full professor since 2010. He won the Dragon Ph.D. Thesis Award from Acer Foundation, Best Ph.D. Thesis Award from Institute of Information & Computing Machinery in 1999, Best Student Paper Awards in National Conference on Information Security 1998 and 2007, Best Master Thesis Award from Taiwan Association for Web Intelligence Consortium in 2011, Outstanding Master Dissertation Award from Taiwan Institute of Electrical and Electronic Engineering in 2011, and Master Thesis Award from Chinese Cryptology and Information Security Association in 2012. He also was the editor-in-chief of Information Security Newsletter and is an Executive Director of Chinese Cryptology and Information Security Association. His current research interests include applied cryptology, cryptographic protocols, information and communication security, and he has published over 100 technical papers.