A Password and Smart Card Based User Authentication Mechanism for Multi-Server Environments[§]

Chun-Ta Li[1], Cheng-Chi Lee[2,3,*], Hsing Mei[4] and Chia-Hao Yang[4]

[1]*Department of Information Management, Tainan University of Technology*
529 Zhongzheng Road, Tainan City 71002, TAIWAN (R.O.C.)
th0040@mail.tut.edu.tw

[2]*Department of Library and Information Science, Fun Jen Catholic University*
510 Jhongjheng Road, New Taipei City 24205, TAIWAN (R.O.C.)

[3]*Department of Photonics and Communication Engineering, Asia University*
500 Lioufeng Road, Taichung City 41354, TAIWAN (R.O.C.)
[*]*Corresponding author: cclee@mail.fju.edu.tw*

[4] *Department of Computer Science and Information Engineering, Fun Jen Catholic University, 510 Jhongjheng Road, New Taipei City 24205, TAIWAN (R.O.C.)*
mei@csie.tut.edu.tw

Abstract

Secure user authentication without repeating registration is one of the important issues in multi-server networks that needs to be adequately addressed. Recently, two-factor (smart card and password) based remote user authentication protocols have been widely introduced due to their low constructional cost and convenient usability for the authentication purpose. In 2011, Chang and Cheng proposed a smart card and password based remote login mechanism for multi-server environments. However, in this paper, we found that Chang-Cheng's mechanism suffers from susceptibility to security attacks. As a result, we introduced an improved version of smart card based password authentication mechanism in multi-server networks. Compared with other related protocols, performance analysis shows that our proposed mechanism is still cost-efficient for the real application in multi-server environments.

Keywords: *Information and network security, Multi-server networks; Password verification, Remote user authentication, Smart card*

1. Introduction

The more network communication technologies and application services are being developed, the more people can receive desired services through personal mobile devices anywhere and anytime [10, 15, 20, 25], such as online payment systems, applications of e-commerce service, e-learning, e-government, e-logistics and mobile commerce etc. Therefore, it is important to verify the validity of remote users in public environments before they can access the services provided by the remote service providing servers. To prevent illegal users' attempts of getting the serviceable resources

[§] Portions of this paper were presented at International Journal of Security and Its Applications, Vol. 6, No. 2, 2012 and at the 6th International Conference on Information Security and Assurance (ISA 2012), April 28-30, Shanghai, China, 2012.

maintained in remote servers, smart card based password authentication is the widely accepted and most adopted method in remote login environments [7, 8, 11, 13, 14, 16, 18, 19, 22]. For traditional remote login mechanisms, a user needs to register with different service providers and remember the various identities and passwords for ensuring higher security in multi-server environments. Therefore, in multi-server environments, single registration to a trusted registration center is the most important feature and any user can receive desired services from various service providers without repeating registration.

In 1994, a well-known Kerberos system [5] is proposed for a multi-server environment. In 2001, Li et al. proposed a neural network based password authentication scheme [9] for multi-server architecture. In 2004, Juang proposed an efficient multi-server password authentication and key agreement scheme [4]. Later Chang and Lee [1] demonstrated that Juang's scheme is not efficient and vulnerable to off-line dictionary attack. In 2004, Tsaur, Wu and Lee proposed a smart card and RSA-based password authentication scheme [24] in multi-server Internet services. Similarly, Tsaur et al.'s scheme is still not efficient due to its high computation and communication costs. In 2008, Tsai suggested a hash function based multi-server authentication scheme [23] without verification table. In 2009, Liao and Wang introduced a hash-based authentication scheme with user anonymity and mutual authentication in multi-server environments [21]. However, in the same year, Hsiang and Shih showed that Liao-Wang's scheme cannot resist insider attack, masquerade attack, server spoofing attack, registration center spoofing attack and they further proposed a dynamic identity based user authentication scheme [3] for multi-server environments. Unfortunately, in 2011, Lee, Lin and Chang [6] pointed out that Hsiang-Shih's authentication scheme is still not secure and cannot provide mutual authentication. Lee et al. found that Hsiang-Shih's scheme is vulnerable to masquerade attack and server spoofing attack, and is not easily reparable. Moreover, Lee et al. suggested a number of key concepts for securing communications in multi-server environments and security requirements include:

Without password/verification table. There is no need for maintaining any password or verification table in registration center.

User friendly. A legal user can freely choose and update his/her passwords any time without the help of registration center.

Mutual authentication and key agreement. After completing whole verification steps, the requirements of mutual authentication and key agreement should be achieved between the login user, the service provider and the registration center.

Single registration. A user does not need to remember numerous different identities and passwords when he/she accesses different remote service providing servers. Any user only registers himself/herself at the registration center once and he/she can access all the permitted services in multi-server environments.

Efficiency. The proposed authentication scheme must provide the requirements of low communication cost and computation complexity because the computation ability of the smart card is very limited.

Security. The proposed authentication scheme must be able to prevent various known security attacks such as password disclosure attack, insider and stolen-verifier attack, smart card lost attack, replay attack, and forgery attack etc.

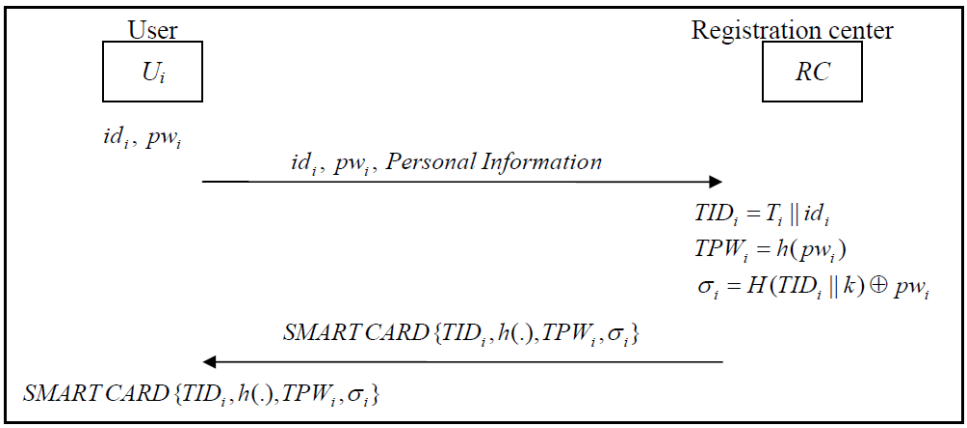

Figure 1. Registration Phase of Chang-Cheng's Authentication Mechanism

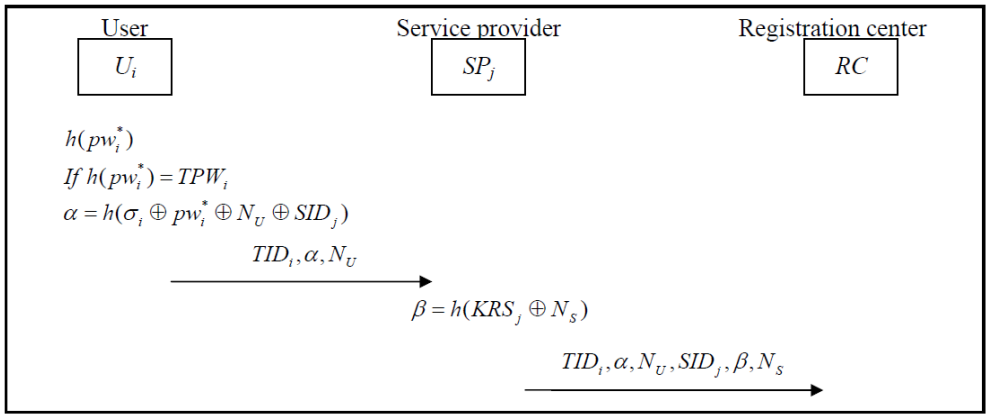

Figure 2. Login Phase of Chang-Cheng's Authentication Mechanism

In 2011, Chang and Cheng developed a nonce based remote login mechanism using smart cards [2]. Chang-Cheng's mechanism uses lightweight computations such as one-way hash function and exclusive OR operation for enhancing the system performance during multi-server authentication processes. The handshakes between U_i, SP_j and RC in Chang-Cheng's authentication mechanism are depicted in Figure 1, 2 and 3. However, we found that Chang-Cheng's login mechanism is insecure to some security attacks [12]. Chang-Cheng's mechanism has four weaknesses as follows.

Smart card lost problems. In Chang-Cheng's mechanism, an adversary may use the secret information which is stored in user's smart card to launch off-line password guessing attack and impersonation attack.

Leak-of-verifier attack. In Chang-Cheng's mechanism, an adversary who possesses the smart card may derive service provider SP_j's secret $h(H(SID_j||k))$ for damaging the security of system in future, where SID_j is SP_j's identifier, $||$ is the string concatenation symbol, k is the private key of registration center, $h(.)$ is a public one-way hash function, and $H(.)$ is a private one-way hash function only known by RC.

Session key disclosure attack. In Chang-Cheng's mechanism, an adversary who possesses the service provider's secret $h(H(SID_j||k))$ may derive other users' previous and subsequent session keys.

Insider attack. In Chang-Cheng's mechanism, user registers to *RC* by presenting {id_i, pw_i, *Personal Information*} and the value of pw_i is revealed to *RC* so the insider of *RC* can know user's password with ease, where id_i is user's identifier and pw_i is transmitted in plaintext.

To overcome above-mentioned security flaws, we propose an improvement on Chang-Cheng's mechanism in this paper. To shorten the length of this paper, we omit the review of Chang-Cheng's login mechanism. Please refer to [2]. The rest of the paper is organized as follows. We propose our improvement on Chang-Cheng's mechanism in Section 2 and the security and performance analysis are presented in Section 3 and Section 4, respectively. Finally, we make our conclusions in Section 5.

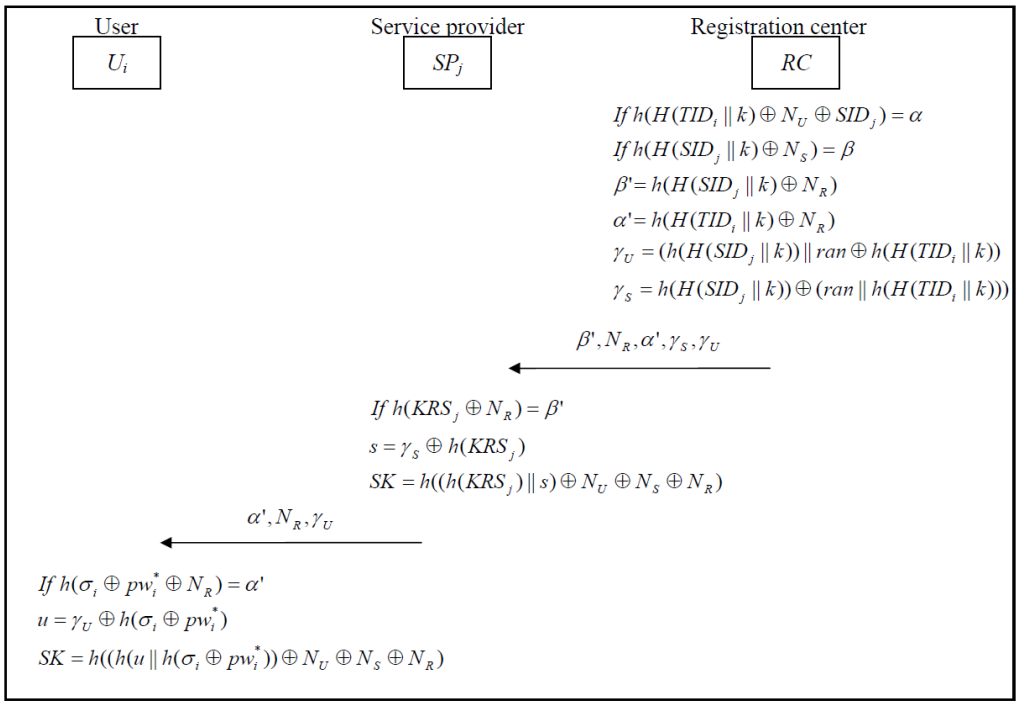

Figure 3. Authentication and Key Agreement Phase of Chang-Cheng's Authentication Mechanism

2. The Proposed Mechanism

The proposed mechanism has five phases: registration, login, authentication and key agreement, password modification, and smart card revocation phase. *RC* is responsible for registration of SP_j and U_i. When SP_j register with *RC* use identifier SID_j, *RC* computes a secret key $KRS_j = H(SID_j||k)$ and shares it with SP_j. For ease of presentation, we employ some intuitive abbreviations and notations, which are listed in Table 1.

2.1. Registration Phase

When a user U_i wants to access the network services in multi-server system, U_i performs registration with *RC* and chooses his/her identity id_i and password pw_i. The details of the registration phase are described as follows.

Step 1: U_i computes $h(id_i||\ pw_i||r)$ and transmits the registration message $\{id_i, h(id_i||pw_i||r)$, *Personal Information*$\}$ to *RC* through a secure channel, where r is a random number chosen by U_i.

Step 2: *RC* checks U_i's registration information and credit. If it is not valid, *RC* rejects U_i's registration; otherwise, *RC* computes U_i's account number TID_i and stores it in the database, where $TID_i = T_i||id_i$ and T_i denotes the number of times a user U_i registers by *RC*. Note that T_i is stored in U_i's account database on the registration center *RC* and the value of T_i is used to revoke a smart card in case of lost or stolen of smart card. In addition, $T_i = 0$ if U_i is a new registration user, otherwise, *RC* sets value $T_i = 1$ and changes T_i in U_i's account database if U_i is re-registering in *RC*.

Step 3: *RC* computes $\sigma_i = H(TID_i||k) \oplus h(id_i||pw_i||r)$, saves $(\sigma_i, h(TID_i), h(.), T_i)$ into U_i's smart card and issues it to U_i.

Step 4: U_i saves r into the smart card and U_i does not need to remember r after finishing this phase.

The handshake between U_i and *RC* is depicted in Figure 4.

Table 1. Notations

Symbol	Description
U_i	User
SP_j	Service provider, where j = 1, 2, …, n and n is numbers of all service providing servers
RC	Registration center
id_i	The identity of U_i
pw_i	The password of U_i
SID_j	The identifier of SP_j
k	The secret key maintained by *RC*
$h(.)$	A public one-way hash function
$H(.)$	A private one-way hash function only known by *RC*
KRS_j	A secret key is shared with *RC* and SP_j, where $KRS_j = H(SID_j||k)$
SK	Session key
T_i	The number of times U_i registers by *RC*
$\oplus$	XOR operation
$\|\|$	String concatenation operation

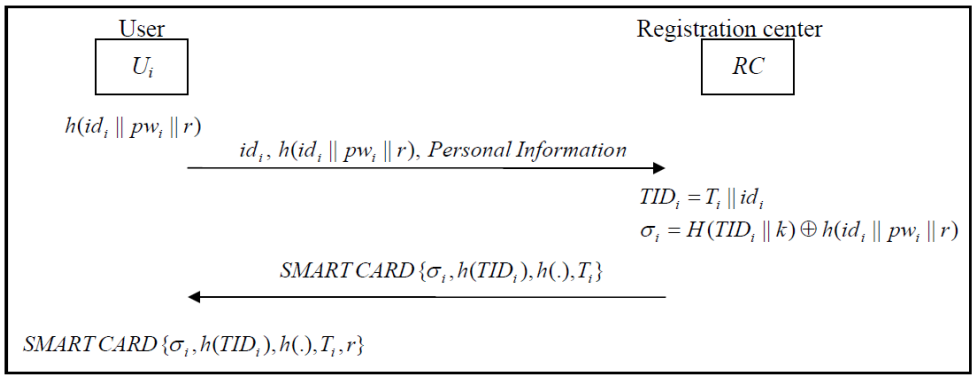

Figure 4. Registration Phase of the Proposed Mechanism

2.2. Login Phase

In this phase, we assume U_i wants to ask a service from SP_j and inserts his/her smart card to an input device. Then, U_i enters identity id_i, password pw_i and SID_j and the smart card performs the following steps:

Step 1: The smart card computes $TID_i' = T_i \| id_i$ and $h(id_i \| pw_i \| r)$ and checks whether $h(TID_i') = h(TID_i)$, where T_i and r are retrieved from the smart card. If it is not match, this phase is terminated by the smart card; otherwise, the smart card transmits $\{TID_i, \alpha_1, \alpha_2\}$ to SP_j via a public channel, where N_U is a nonce, $\alpha_1 = \sigma_i \oplus h(id_i \| pw_i \| r) \oplus N_U$ and $\alpha_2 = h((TID_i \| SID_j) \oplus N_U)$.

Step 2: SP_j generates a nonce N_S, computes $\beta_1 = KRS_j \oplus N_S$ and transmits $\{TID_i, \alpha_1, \alpha_2, SID_j, \beta_1, \beta_2\}$ to RC via a public channel, where $\beta_2 = h((SID_j \| TID_i) \oplus N_S)$.

The handshake between U_i, SP_j and RC is depicted in Figure 5.

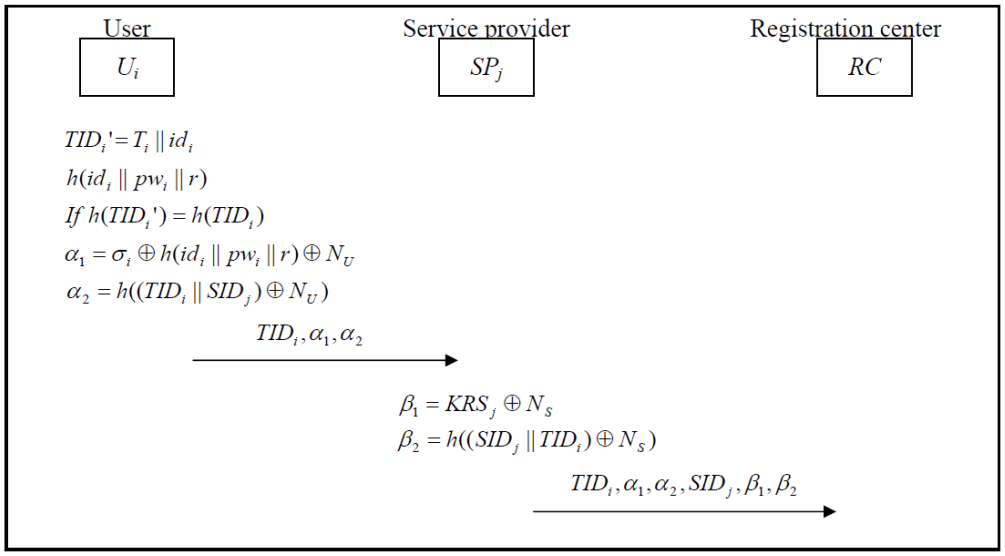

Figure 5. Login Phase of the Proposed Mechanism

2.3. Authentication and Key Agreement Phase

After receiving the message from SP_j, RC, SP_j and U_i perform the following steps to achieve mutual authentication and key agreement between them.

Step 1: RC checks the validity of TID_i and SID_j. If they are not valid, RC rejects this login request; otherwise, RC computes $N_U' = \alpha_1 \oplus h((TID_i||k)$. Then, RC verifies the freshness of N_U' and the validity of $h((TID_i||SID_j) \oplus N_U') = \alpha_2$. If either one is not valid, RC terminates this connection; otherwise, U_i is authenticated by RC.

Step 2: RC computes $N_S' = \beta_1 \oplus h((SID_j||k)$ and verifies the freshness of N_S' and the validity of $h((SID_j||TID_i) \oplus N_S') = \beta_2$. If either one is not valid, RC terminates this connection; otherwise, SP_j is authenticated by RC.

Step 3: RC generates a nonce N_R, computes $\alpha' = h(N_U') \oplus N_S' \oplus N_R$, $\gamma_U = h((TID_i||k) \oplus SK)$, $\beta' = h(N_S') \oplus N_U' \oplus N_R$ and $\gamma_S = h((SID_j||k) \oplus SK)$ and sends $\{\alpha', \gamma_U, \beta', \gamma_S\}$ to SP_j via a public channel, where SK is a common session key and it is constructed by computing $SK = h(N_U' \oplus N_S' \oplus N_R)$.

Step 4: After receiving the response message from RC, SP_j computes $\beta'' = \beta' \oplus h(N_S)$ and $SK_S = h(\beta'' \oplus N_S)$ and verifies whether $h(H(SID_j||k) \oplus SK_S) = \gamma_S$, where $SK_S = SK$ and it is shared between SP_j, U_i and RC. If it is not valid, SP_j terminates this phase; otherwise, RC and U_i are authenticated by SP_j and transmits $\{\alpha', \gamma_U\}$ to U_i via a public channel.

Step 5: After receiving the message from SP_j, the smart card computes $\alpha'' = \alpha' \oplus h(N_U)$ and $SK_U = h(\alpha'' \oplus N_U)$ and verifies whether $h(H(TID_i||k) \oplus SK_U) = \gamma_U$. If it is not valid, U_i terminates this phase; otherwise, RC and SP_j are authenticated by U_i, where $SK_U = SK = SK_S$ and it is shared between U_i, SP_j and RC.

The handshake between U_i, SP_j and RC is depicted in Figure 6.

2.4. Password Modification Phase

When U_i wants to change his/her original password pw_i to a new password pw_i^{new}, U_i must insert the smart card into input device and enter id_i and pw_i. Then, the smart card retrieves T_i to compute $TID_i' = T_i||id_i$ and checks whether $h(TID_i') = h(TID_i)$. If it does not hold, the smart card terminates this modification procedure; otherwise, U_i is asked to input a new password pw_i^{new} and a new random number r^{new} and the smart card computes $\sigma_i^{new} = H(TID_i||k) \oplus h(id_i||pw_i||r) \oplus h(id_i||pw_i^{new}||r^{new})$ and replaces σ_i and r with σ_i^{new} and r^{new}.

2.5. Smart Card Revocation Phase

In case of stolen or lost of smart card, U_i can request RC for its revocation. First, RC updates the value of T_i and the value of T_i is incremented by one. Finally, U_i can re-register to RC without changing his/her original identity id_i.

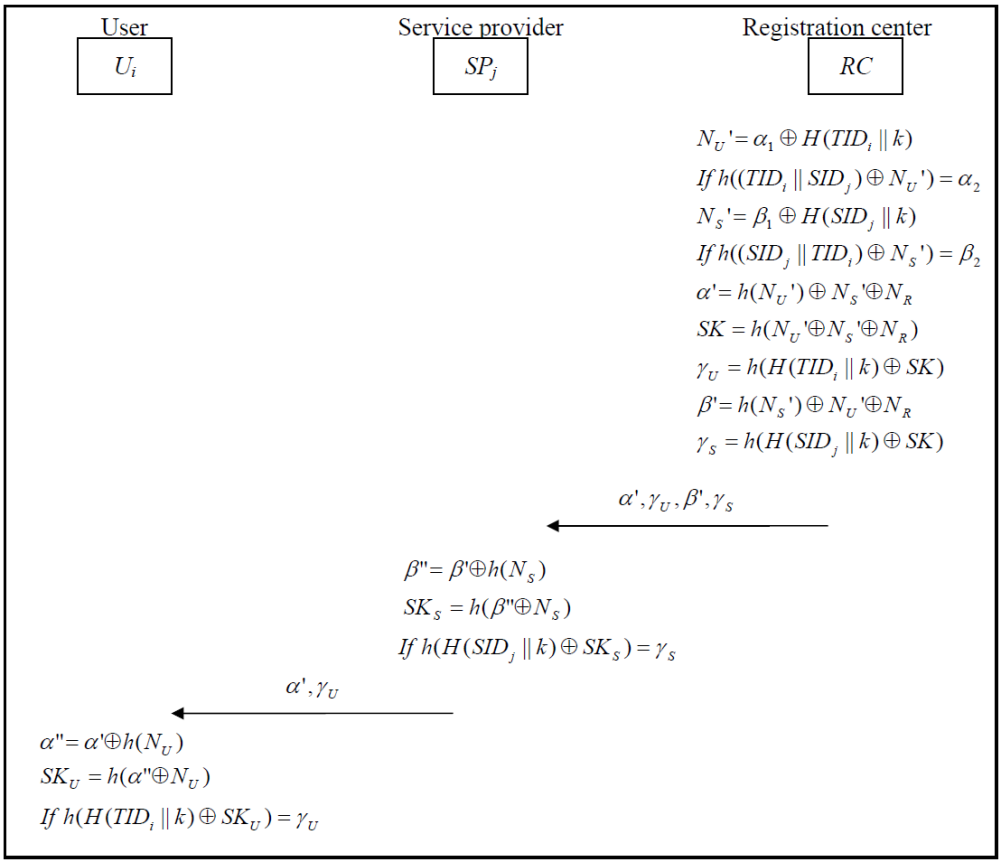

Figure 6. Authentication and Key Agreement Phase of the Proposed Mechanism

3. Security Analysis

In this section, we show that the proposed mechanism is secure and has several security properties as follows:

Resist insider and stolen-verifier attack: In our mechanism, a legal user U_i registers to *RC* by presenting $h(id_i||pw_i||r)$ instead of pw_i. Note that the random number r is not revealed to *RC* so the insider of *RC* cannot obtain U_i's pw_i by performing off-line guessing attack on $h(id_i||pw_i||r)$. Also, the proposed mechanism does not need to maintain the verifier table in the registration center side and can prevent the insider and stolen-verifier attacks.

Resist off-line password guessing and smart card lost attacks: We assume that an adversary can eavesdrop all transmitted messages $\{TID_i, \alpha_1, \alpha_2\}$, $\{TID_i, \alpha_1, \alpha_2, SID_j, \beta_1, \beta_2\}$, $\{\alpha', \gamma_U, \beta', \gamma_S\}$ between U_i, SP_j and *RC*, and $(\sigma_i, h(TID_i), h(.), T_i, r)$, which are stored in U_i's smart card. The adversary may launch an off-line password guessing attack in the proposed mechanism. In order to derive U_i's password or login into the multi-server system by using the stolen or lost smart card, the adversary guesses a trial identity id_i' and password pw_i' and computes $\sigma_i \oplus h(id_i'||pw_i'||r)$. However, without knowing $H(TID_i||k)$ and N_U, the adversary cannot verify if $\alpha_1 = \sigma_i \oplus h(id_i'||pw_i'||r) \oplus N_U$ holds or not, since the adversary is unable to compute $H(TID_i||k)$ from σ_i due to the protection of one-way hash function. As a result, our proposed mechanism can withstand o®-line password guessing and smart card lost attacks.

Resist replay attack: In Step 1 and 2 of login phase of the proposed mechanism, two random nonces N_U and N_S are generated by U_i and SP_j, respectively, which make all login messages dynamic and valid for that session only. Thus, the proposed mechanism can resist replay attacks by using random nonces in different sessions.

Resist forgery attack: For this attack, we assume that an adversary can get (σ_i, $h(TID_i)$, $h(.)$, T_i, r), which are stored in U_i's smart card. The adversary may select a service provider SP_j and choose a trial identity id_i', a trial password pw_i' and a random nonce N_U'. Then the adversary computes $TID_i'=T_i \| id_i'$, $\alpha_1'=\sigma_i \oplus h(id_i' \| pw_i' \| r) \oplus N_U'$ and $\alpha_2' = h((TID_i' \| SID_j) \oplus N_U')$ and sends $\{TID_i, \alpha_1', \alpha_2'\}$ to SP_j. However, the adversary needs to get real identity id_i and password pw_i correctly at the same time. Therefore, the adversary's login messages cannot pass the verification process of RC due to $TID_i' \neq TID_i$ and $h((TID_i' \| SID_j) \oplus \alpha_1' \oplus H(TID_i \| k)) \neq \alpha_2'$. Finally, the adversary cannot launch forgery or impersonation attacks in the proposed mechanism.

Provide mutual authentication: Our proposed mechanism provides the mutual authentication to keep faith between the login user, the service provider and the registration center. First, in Step 1 and 2 of the authentication and session key agreement phase, the registration center authenticates the login user and the service provider by checking $H(TID_i \| k)$ and $H(SID_j \| k)$. Moreover, in Step 4 and 5 of the authentication and session key agreement phase, the service provider and the login user authenticate the registration center by checking γ_S and γ_U, respectively. As a result, the mutual authentication is done safely to the proposed mechanism.

Provide session key agreement: In the proposed mechanism, a session key $SK = h(N_U \oplus N_S \oplus N_R)$ is shared between U_i, SP_j and RC. Three nonces (N_U, N_S and N_R) are generated by U_i, SP_j and RC, respectively. The session key SK will be different for each login session and cannot be reused after the expiration of login session due to the freshness of N_U and N_S will be checked by RC. Therefore, U_i, SP_j and RC can use SK to securely perform encryption and decryption of subsequence communications.

4. Performance Analysis

In this section, we compare the computational primitives involved in registration, login, authentication and session key agreement phases of our proposed mechanism with some related multi-server authentication protocols [2, 3, 17] and tabulate the results in Table 2. To evaluate the performance, we define the notation *Hash* as the time complexity for one-way hashing function. In general, it is usually negligible considering the computation cost of exclusive-OR operation because it requires very few computations. From the result of Table 2 shows, the total computations of our proposed mechanism is lower than most of authentication protocols [3, 17]. On the other hand, Chang-Cheng's protocol [2] adopts only 19 computations of one-way hash function to construct a multi-server authentication protocol. However, in [12], Li, et al., found that Chang-Cheng's authentication protocol is not secure against many types of attacks such as smart card lost problems, leak-of-verifier attack, session key disclosure attack and insider attack etc. It is clear that the overhead of few additional hash function computations is negligible, especial in view of the level of security the proposed mechanism offers.

Table 2. Performance Comparisons between our Proposed Mechanism and Other Related Protocols

Protocols/Phases	Registration	Login	Authentication	Total computations
Hsiang et al.'s protocol (2009) [3]	6 *Hash*	7 *Hash*	17 *Hash*	30 *Hash*
Chang-Cheng's protocol (2011) [2]	2 *Hash*	3 *Hash*	14 *Hash*	19 *Hash*
Li et al.'s protocol (2012) [17]	6 *Hash*	7 *Hash*	21 *Hash*	34 *Hash*
The proposed mechanism	3 *Hash*	4 *Hash*	15 *Hash*	32 *Hash*

5. Conclusions

Single registration and user authentication are important issues for multi-server environments. Two-factor (passwords and smart cards) verification is one of the mechanisms that were widely adopted to verify the authenticity of a remote login user. Recently, Chang and Cheng proposed a secure and lightweight user authentication mechanism for multi-server architecture. For enhancing the security of multi-server networks, Chang-Cheng's authentication mechanism lets each service providing server share different secret keys with registration center. However, we found that Chang-Cheng's authentication mechanism is still vulnerable to smart card lost attack, leak-of-verifier attack, session key disclosure attack and insider attack, and is not easily reparable. To solve security problems of Chang-Cheng's authentication mechanism, in this paper, we proposed an improvement on Chang-Cheng's login mechanism and security analysis showed that the proposed mechanism not only resists various attacks but also achieves mutual authentication and session key agreement between the login user, the service provider and the registration center. Performance analysis shows that our proposed mechanism has much better performance when compared to other related protocols so as to be practically applicable.

Acknowledgements

Authors would like to thank the publishing editors of International Journal of Security and Its Applications and the reviewers of our previous conference paper published in ISA 2012 for their valuable comments and suggestions. Moreover, this work was partially supported by the National Science Council of the Taiwan under grants NSC 101-2221-E-165-002 and NSC 101-2221-E-030-018.

References

[1] C. C. Chang and J. S. Lee, "An efficient and secure multi-server password authentication scheme using smart cards", Proceedings of the Third International Conference on Cyberwords, **(2004)**, pp. 417-422.
[2] C. C. Chang and T. F. Cheng, "A robust and efficient smart card based remote login mechanism for multi-server architecture", International Journal of Innovative Computing, Information and Control, vol. 7, **(2011)**, pp. 4589-4602.
[3] H. C. Hsiang and W. K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment", Computer Standards and Interfaces, vol. 31, **(2009)**, pp. 1118-1123.
[4] W. Juang, "Efficient multi-server password authenticated key agreement using smart cards", IEEE Transactions on Consumer Electronics, vol. 50, **(2004)**, pp. 251-255.
[5] J. T. Kohl, B. C. Neuman and T. Ts'o, "The evolution of the Kerberos authentication system", Distributed Open System, IEEE CS Press, **(1994)**, pp. 78-94.
[6] C. C. Lee, T. H. Lin and R. X. Chang, "A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards", Expert Systems with Applications, vol. 38, **(2011)**, pp. 13863-13870.
[7] C. C. Lee, C. T. Li and R. X. Chang, "A simple and efficient authentication scheme for mobile satellite communication systems", International Journal of Satellite Communications and Networking, vol. 30, **(2012)**, pp. 29-38.
[8] C. C. Lee, Y. M. Lai and C. T. Li, "An improved secure dynamic ID based remote user authentication scheme for multi-server environment", International Journal of Security and Its Applications, vol. 6 **(2012)**, pp. 203-209.
[9] 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, **(2001)**, pp. 1498-1504.
[10] C. T. Li and M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks", Information Sciences, vol. 181, **(2011)**, pp. 5333-5347.
[11] 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, **(2011)**, pp. 4821-4831.
[12] C. T. Li, C. Y. Weng and C. I. Fan, "Two-factor user authentication in multi-server networks", International Journal of Security and Its Applications, vol. 6, **(2012)**, pp. 261-267.
[13] C. T. Li, "A more secure and efficient authentication scheme with roaming service and user anonymity for mobile communications", Information Technology and Control, vol. 41, **(2012)**, pp. 69-76.
[14] 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, **(2012)**, pp. 35-44.
[15] C. T. Li, C. C. Yang and M. S. Hwang, "A secure routing protocol with node selfishness resistance in MANETs", International Journal of Mobile Communications, vol. 10, **(2012)**, pp. 103-118.
[16] C. T. Li, C. C. Lee and C. W. Lee, "An improved two-factor user authentication protocol for wireless sensor networks using elliptic curve cryptography", Sensor Letters, **(2012)**, article in press.
[17] X. Li, Y. Xiong, J. Ma and W. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards", Journal of Network and Computer Applications, vol. 35, **(2012)**, pp. 763-769.
[18] C. T. Li, C. C. Lee, C. Y. Weng and C. I. Fan, "An extended multi-server-based user authentication and key agreement scheme with user anonymity", KSII Transactions on Internet and Information Systems, **(2012)**, article in press.
[19] C. T. Li, "A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card", IET Information Security, **(2012)**, article in press.
[20] C. T. Li, C. C. Lee, C. Y. Weng and C. I. Fan, "A RFID-based macro-payment scheme with security and authentication for retailing services", ICIC Express Letters, **(2012)**, article in press.
[21] Y. P. Liao and S. S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment", Computer Standards and Interfaces, vol. 31, **(2009)**, pp. 24-29.
[22] S. K. Sood, "An improved and secure smart card based dynamic identity authentication protocol", International Journal of Network Security, vol. 14, **(2012)**, pp. 39-46.
[23] J. L. Tsai, "Efficient multi-server authentication scheme based on one-way hash function without verification table", Computers and Security, vol. 27, **(2008)**, pp. 115-121.
[24] W. J. Tsaur, C. C. Wu and W. B. Lee, "A smart card-based remote scheme for password authentication in multi-server Internet Services", Computer Standards and Interfaces, vol. 27, **(2004)**, pp. 39-51.
[25] F. Zhu, M. W. Matka and L. M. Ni, "Private entity authentication for pervasive computing environments", International Journal of Network Security, vol. 14, **(2012)**, pp. 86-100.