Computer Science and Information Technology 3(4): 117-121, 2015 http://www.hrpub.org
DOI: 10.13189/csit.2015.030404

A Novel Smart Card-based Remote User Authentication Mechanism

Deborah Uwera, Dongho Won*

Department of Computer Engineering, Sungkyunkwan University, South Korea

Abstract The past few years have seen a rapid progress of multi-user computing environments. Numerous security mechanisms have therefore been employed in a bid to ensure that sensitive information in computer systems does not get destroyed, copied or even altered by unauthorized users. Remote users attempting to login into a particular system would therefore have to authenticate themselves to the server and vice versa. This paper proposes a novel remote user authentication scheme using smart cards. Our scheme endeavors to be an efficient yet secure scheme, hence we chose to use only one-way hash functions and XOR operations, in order to avoid computationally complex operations. We also conducted a security analysis on our scheme to ensure that it is secure against possible known attacks.

Keywords Security, Authentication, Key Exchange

1. Introduction

The main reason why schemes for user authentication are necessary is because a server needs be enabled to remotely verify the legitimacy of a user trying to login, and ensure that this user is indeed genuine and trustworthy. The user on the other hand also needs to ensure that the server is truly genuine, hence they both require to authenticate each other; Mutual authentication.

In the past decade, there has been a recent influx of various remote user authentication schemes that use biometrics, passwords and smart cards. Many of these schemes however have a number of limitations that render them inadequate to be used as authentication schemes. Cryptanalysis shows us that many of them are at risk of attacks and security breaches.

Remote user authentication scheme is a very suitable authentication scheme to deal with private data that is being transmitted over insecure channels. Since Security and privacy have proven to be one of the most important factors in today's real time applications, users are therefore required to have the proper access rights in order to be able to access resources at remote system in client/server-based service architecture, which are widely used. In this type of architecture we find that a single computer can handle a huge amount of clients who are dispersed all over the world. In daily routines, there too are many real-time applications that also require user authentication such as, e-banking, e-commerce, physical access control to computer resources.

Based on various comprehensive surveys on password-based remote user authentication schemes, we see that most of the remote user authentication schemes that are password-based are impractical due to the fact that they are either very expensive in terms of computation or are susceptible to different security attacks. In [1], Das et.al proposes a dynamic ID and password-based remote user authentication scheme that uses smart cards, and incorporates the use of hash function and XOR operations. Ever since, numerous researchers have proposed improved authentication protocols. This was done in order to eliminate the weaknesses in the previous authentication protocols such as [2], [3], and [4]. These weaknesses are dealt with in the following studies; according to [5] we see a dynamic ID-based authentication scheme that has key agreement using symmetric cryptology. This scheme endeavors to deal with the security flaws and weaknesses of [2]. They incorporated a Session key in order to create a more secure channel for communication. In [6] Li et al. assert that their scheme resisted masquerading attacks and avoided the leaking of information. However, [7], pointed out that [6] was not entirely secure, since it leaked partial information about the communication party's secret parameters and any attacker would be able to access the leaked information to deduce session keys .In [8], a secure remote user authentication scheme was proposed that is also password-based was introduced. However, their scheme uses Elliptic curve cryptography and hash functions. Due to this fact, their scheme is too costly and thus not feasible.

In our paper, we propose a Novel Smart Card-Based remote user authentication scheme using XOR operations and hash functions. The rest of this paper is organized as follows. In Section 2, we propose our new and secure Smart card-based remote user authentication scheme. In Section 3, we conduct a security analysis where we perform a security analysis of our proposed scheme. In Section 4, we have the conclusion of our paper.

2. Our Proposed Scheme

In this part, we introduce our Remote User Authentication scheme that is based on Smart Cards.

Table 1. Our Scheme's Notations

Notations	Description
U_i	User
S_j	Remote Server
ID_i	User Identity
PW_i	User's Password
Xs	Remote Server's secret Key
K	User's Secret Number
T	Current Time Stamp
R	Random nonce
h(.)	One-way hash function
‖	Concatenating
⊕	XOR operation

2.2 Proposed Scheme's Phases

In this scheme, we have three phases;

i. The registration phase,
ii. The login phase,
iii. The authentication phase.

The registration phase is the phase where the user U_i first registers to the server in order to gain access to services from the remote server S_j. After the registering occurs, the server S_j then issues a smart card that contains detailed parameters stored in the smart card's memory.

The login phase, is the phase where we see that whenever the user U_i needs to gain access to the services from the server S_j, the user U_i is required to input his/her identity and password in order to login to the server, while also using the smart card issued to them by the registration server.

The authentication phase is the phase where mutual authentication occurs between the server and the user; the server S_j authenticates the user U_i and the user U_i also authenticates the server S_j. After mutual authentication between U_i and S_j, both U_i and S_j establish a secret session key shared between them so that they communicate securely using that established key in future.

2.2.1 Registration Phase.

These are the steps found in this phase.

Step 1. First, the user U_i selects his/her own secret identity ID_i and then chooses a strong password PW_i

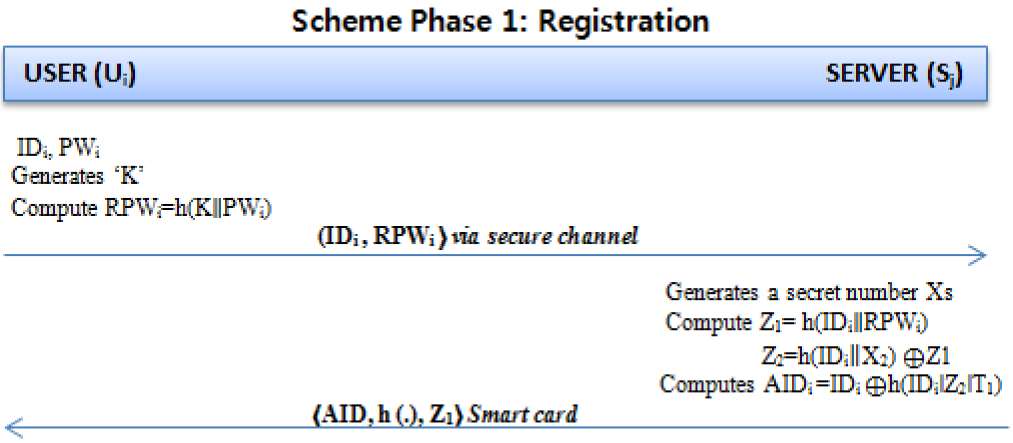
Step 2. U_i then generates a secret number 'K' randomly, and makes sure to keep it secret to everyone else except from U_i themselves.

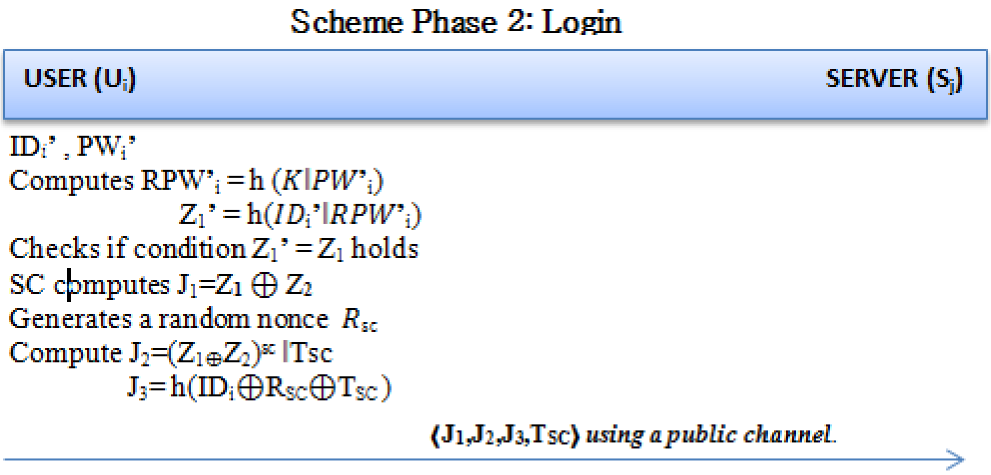
Step 3. The user U_i then uses the secret number generated 'K' in order to mask the password using, PW_i as RPW_i= h(K ‖ PW_i) .And stores 'K' in the memory of the smart card and then proceeds to send the registration request message ⟨ID_i,RPW_i⟩ to the registration remote server S_j via a secure channel.

Step 4. After the server S_j receives the registration request message from the user U_i, the server S_j then generates a secret number X_s randomly, which is kept secret to S_j only.

Step 5. S_j then computes Z_1= h(ID_i ‖ RPW_i) and Z_2= h(ID_i ‖ X_s) ⊕ Z_1. Furthermore, S_j computes AID_i= ID_i⊕h(ID_i ‖ Z_2 ‖ T_s). Here the AID is incorporated in order to achieve user anonymity, and it is a temporary identity for the user U_i, which is used rather than the permanent identity ID_i

Step 6. In the Final step, S_j issues the smart card SC which contains the information ⟨AID, h (.), Z_1⟩ and sends it to the user U_i via a secure channel.


Scheme Phase 1: Registration
USER (U_i)
SERVER (S_j)
ID_i, PW_i
Generates 'K'
Compute RPW_i=h(K‖PW_i)
(ID_i , RPW_i) via secure channel
Generates a secret number Xs
Compute Z_1= h(ID_i‖RPW_i)
Z_2=h(ID_i‖X_2) ⊕Z1
Computes AID_i =ID_i ⊕h(ID_i|Z_2|T_1)
(AID, h (.), Z_1) Smart card



Scheme Phase 2: Login

ID_i' , PW_i'

Computes $RPW'_i = h\ (K|PW'_i)$

$Z_1' = h(ID_i'|RPW'_i)$

Checks if condition $Z_1' = Z_1$ holds

SC computes $J_1=Z_1 \oplus Z_2$

Generates a random nonce R_{sc}

Compute $J_2=(Z_1 \oplus Z_2)^{sc}\ |Tsc$

$J_3=h(ID_i \oplus R_{SC} \oplus T_{SC})$

(J_1,J_2,J_3,T_{SC}) *using a public channel.*

2.2.2. Login Phase

The following steps are executed in this phase.

Step 1. The user U_i first inserts his/her smart card SC into a card reader then. U_i inputs his/her identity ID_i' and password PW_i'.

Step 2. Then Smart Card SC computes the masked password RPW'_i as $RPW'_i = h\ (K \parallel PW'_i)$ using the secret number 'K' stored in the memory of the smart card. memory. SC then computes $Z_1' = h(ID_i' \parallel RPW'_i)$ and checks if the condition $Z_1' = Z_1$ holds. If this condition holds, then U_i is able to pass the password verification step and the next step is executed. Otherwise, this phase has to be terminated immediately.

Step 3. The smart card SC computes $J_1 = Z_1 \oplus Z_2$ where these parameters are embedded within the smart card. And then the Smart Card generates a random nonce R_{sc} and proceeds to compute $J_2= (Z_1 \oplus Z_2)^{Rsc}\ \parallel Tsc$ and $J_3= h(ID_i \oplus R_{SC} \oplus T_{SC}$ where T_{SC} is the current system timestamp. Finally, SC sends the login request message $\langle J_1,J_3,T_{SC}\rangle$ to the server S_j using a public channel.

2.2.3. Authentication Phase

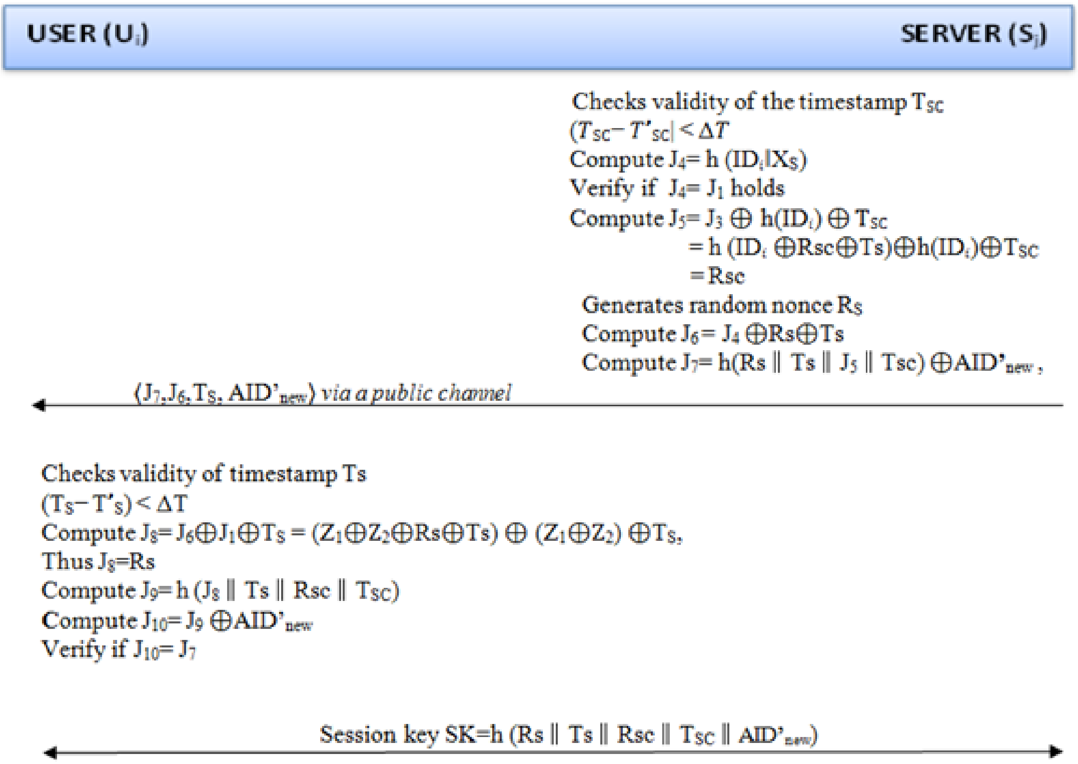
These are the steps found in this phase.

Step 1. The server S_j checks the validity of the timestamp T_{SC} in the received message by the condition $(T_{SC} - T'_{SC}| < \Delta T$, where T'_{SC} is the current system timestamp of S_j. If this condition is satisfied, S_j computes $J_4= h\ (ID_i \parallel X_S)$, where Xs is the secret number of the server. S_j then verifies if $J_4= J_1$ If it does not hold, Server S_j rejects the login request message and this phase terminates immediately. After that S_j computes $J_5= J_3 \oplus h(ID_i) \oplus T_{SC} = h(ID_i \oplus Rsc \oplus Ts) \oplus h(ID_i) \oplus T_{SC} = Rsc$

Step 2. Then the server S_j generates a random nonce R_S and then computes $J_6 = J_4 \oplus Rs \oplus Ts$ where Ts is the current system time stamp of the server S_j, $J_7=h(Rs \parallel Ts \parallel J_5 \parallel Tsc) \oplus AID'_{new}$, where AID'_{new} is a random and temporary identity generated by the server S_j, The server S_j then sends the authentication request message$\langle J_7,J_6,T_S, AID_{new}\rangle$ to the user U_i via a public channel.

Step 3. After receiving the authentication request message, Smart Card SC checks the validity of the timestamp Ts in the received message with the condition $(T_S - T'_S) < \Delta T$, where T'_S is the current system timestamp of SC. If this condition does not hold, the phase terminates immediately. Otherwise, SC computes $J_8= J_6 \oplus J_1 \oplus T_S = (Z_1 \oplus Z_2 \oplus Rs \oplus Ts) \oplus (Z_1 \oplus Z_2) \oplus T_S$, thus $J_8=Rs$, Then the Smart card SC further computes $J_9= h(J_8 \parallel Ts \parallel Rsc \parallel T_{SC})$

Step 4. SC then computes $J_{10}= J_9 \oplus AID'$, $J_{10}= J_7$, Smart Card SC verifies that this holds, if not, the procedures are terminated. Otherwise the Smart card computes a secret session key shared between U_i and S_j; $SK=h\ (Rs \parallel Ts \parallel R_{sc} \parallel T_{SC} \parallel AID'_{new})$. Thus, after successful authentication, both U_i and S_j can communicate securely using the established secret session key.



USER (U_i) SERVER (S_j)

Checks validity of the timestamp T_{SC}

$(T_{SC} - T'_{SC}| < \Delta T$

Compute $J_4 = h\ (ID_i \| X_S)$

Verify if $J_4 = J_1$ holds

Compute $J_5 = J_3 \oplus h(ID_i) \oplus T_{SC}$

$= h\ (ID_i \oplus Rsc \oplus Ts) \oplus h(ID_i) \oplus T_{SC}$

$= Rsc$

Generates random nonce R_S

Compute $J_6 = J_4 \oplus Rs \oplus Ts$

Compute $J_7 = h(Rs \parallel Ts \parallel J_5 \parallel Tsc) \oplus AID'_{new}$,

$\langle J_7, J_6, T_S, AID'_{new} \rangle$ *via a public channel*

Checks validity of timestamp Ts

$(T_S - T'_S) < \Delta T$

Compute $J_8 = J_6 \oplus J_1 \oplus T_S = (Z_1 \oplus Z_2 \oplus Rs \oplus Ts) \oplus (Z_1 \oplus Z_2) \oplus T_S,$

Thus $J_8 = Rs$

Compute $J_9 = h\ (J_8 \parallel Ts \parallel Rsc \parallel T_{SC})$

Compute $J_{10} = J_9 \oplus AID'_{new}$

Verify if $J_{10} = J_7$

Session key $SK = h\ (Rs \parallel Ts \parallel Rsc \parallel T_{SC} \parallel AID'_{new})$

Scheme Phase 3: Authentication

3. Security Analysis of the Proposed Scheme

In this section, we first show that our scheme is secure against various known attacks.

3.1. Impersonation Attack

In this kind of attack, an adversary attempts to impersonate the remote server S_j or a legal user U_i. If an attacker intercepts the login request message $\langle J_1, J_3, T_{SC} \rangle$ during the login phase and wants to start a new session, the attacker has to modify both J_1 and J_3. However, in order to change J_3 the attacker has to know both ID_i and Rsc, which are unknown to the attacker.

3.2. Stolen Smart Card Attack

In this kind of attack, we assume that the card SC_i is lost or stolen by an attacker.

The Attacker can then be able to extract all the information contained ⟨AID, h (.), Z_1, Z_2⟩ in the smart card SC_i of the user U_i with the use of power analysis attack. However, the attacker still has no way to find out the secret information Xs of the server, therefore, since $Z_2 = h\ (ID_i \parallel X_s) \oplus Z_1$and $AID_i = ID_i \oplus h(ID_i \parallel Z_2 \parallel T_s)$ this is not helpful to the attacker

3.3. Password Guessing Attack

In this attack, we consider that the smart card SC_i of a legal user U_i is lost or stolen by an attacker .All the secret information ⟨AID, h (.), Z_1, Z_2⟩ stored in the memory of the smart card SC_i is known to the attacker. Still then the attacker is not able to guess correctly the password PW_i of U_i. In addition, suppose the attacker intercepts all the transmitted messages $\langle J_1, J_3, T_{SC} \rangle$ during the login phase and $\langle J_7, J_6, T_S, AID_{new} \rangle$ during the authentication phase.

None of these messages involves the password PW_i of the user $U_{i,}$ therefore still the attacker is unable to carry out the password guessing attack

4. Conclusions

We have made an analysis of existing schemes for remote user authentication, and identified that they either have vulnerabilities to various known attacks or have a large cost for computation, this paper therefore proposes a novel password-based remote user authentication scheme using smart cards. Our scheme ensures efficiency and security, while upholding simplicity with the use of only one-way hash function and XOR operations. This enables us to avoid the usage of costly computationally complex operations. We have also conducted a security analysis on our scheme to ensure that it is secure against possible known attacks. Hence, we propose that our new scheme is both feasible and secure, making it an Ideal remote user authentication scheme.

Acknowledgements

This research was supported by the Basic Science Research Program through the National Research

Foundation of Korea (NRF) funded by the Ministry of Science, ICT, and Future Planning (2014R1A1A2002775).

REFERENCES

[1] Das, M. L.,Saxana, A., & Gulati, V. P. (2004). *A dynamic ID-based remote user authentication scheme*, IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 629-631.

[2] Wang, Y.Y., Liu J.Y., Xiao,F.X., & Dan J., (2009). *A more efficient and secure dynamic ID-based remote user authentication scheme*, Computer Communications, vol. 32, no. 4, pp. 583-585.

[3] Awasthi, A. K. (2004), *Comments on a dynamic ID-based remote user authentication scheme Transactions on Cryptology*, vol. 1, no. 2, pp. 15-16.

[4] Ku W. C., Chang, S. T. (2005), *Impersonation attacks on a dynamic ID-based remote user authentication scheme using smart cards*, IEICE Transactions, pp. 2165-2167

[5] Wen, F., & Li, X. (2012). *An improved dynamic ID based remote user authentication scheme with key agreement scheme*, Computers & Electrical Engineering, vol. 38, no. 2, pp. 381–387.

[6] Li,J. H,. & Tsaur, W. J., & & Lee. W. B., (2012). *An efficient and secure multi-server authentication scheme with key agreement*, Journal of Systems and Software, vol. 85, no.4, pp. 876-882.

[7] Kim, M., Park, N., & Won, D.(2012). *Security weakness of a dynamic ID-based user authentication scheme with key agreement*, CSA-12, LNEE, vol. 203, pp. 687–692

[8] Jiang, P., Wen, Q., Li,W., Jin Z., and Zhang, H. (2013). *An anonymous user authentication with key agreement scheme without pairings for multiserver architecture using SCPKs*. The Scientific World Journal, vol. 2013, Article ID 419592, 8 pages