Attacks and Improvement of "Security Enhancement for a Dynamic ID-based Remote User Authentication Scheme"

Omar Cheikrouhou[1,2], Manel Boujelben[1], Anis Koubaa[3,4], Mohamed Abid[1]

[1]CES Research Unit, National School of Engineering, Sfax, 3038, Tunisia
[2]Higher Institute of Technological Studies-Computer Science technologies dept., Sfax, Tunisia
[3]CISTER Research Unit – IPP/HURRAY, Porto, 4200-072, Portugal
[4]College of Computer Science and Information Systems,
Al-Imam Mohamed bin Saud University, 11861, Riyadh Saudi Arabia

Omar.cheikhrouhou@isetsf.rnu.tn, boujelben_manel@yahoo.fr, akoubaa@dei.isep.ipp.pt, mohamed.abid@enis.rnu.tn

Abstract

In 2004, Das et al. proposed a "Dynamic ID-based Remote User Authentication Scheme using Smart Cards". This scheme have the advantage that users can choose and change their password freely and the server does not maintain any verifier table, which avoid the risk of stolen/modifying this table. However, in 2005, Liao et al. demonstrated that Das et al.'s scheme suffers from guessing attacks, unilateral authentication and revealing of user password and propose improvements to prevent these shortcomings. However, in this paper, we demonstrate that Liao et al.'s scheme is not secure and it is vulnerable to stolen/lost smart card attack, impersonation (forgery) attack and password revealing attack. In fact, we prove that the scheme is equivalent to no password scheme. Then, we propose possible improvements to Liao et al.'s scheme. We demonstrate through comparison between the three schemes that the proposed one is more secure while maintaining the same computational overhead as Das et al.'s scheme.

1. Introduction

With the rapid growth of Internet technologies and mobile communication services, remote user authentication is being more and more critical in order to prevent access of illegal user. Because of the low computation capability of user devices, password-based user authentication schemes are the most widely used techniques for remote user authentication [1], [2].

In 2004, Das et al. [1] proposed a "Dynamic ID-based Remote User Authentication Scheme using Smart Cards" having three main advantages. First, it allows user to choose and change their password freely. Second, the server does not maintain any verifier table, which avoid the risk of stolen/modifying this verifier table. Third, it employs dynamic identity, which prevents ID-theft attack. Das et al. claim also that their scheme is secure against replay attacks, guessing attacks, forgery attacks, insider attacks, and stolen-verifier attacks.

However, in 2005, Liao et al. [4] demonstrated that Das et al.'s scheme suffers from guessing attacks, unilateral authentication and user password revealing attack and hence propose a slight modification to their scheme in order to prevent these security weaknesses. Liao et al. pretend that their scheme conserve the advantage of Das et al.'s scheme and therefore that their scheme is secure against replay attacks, guessing attacks, forgery attacks, insider attacks, and stolen-verifier attacks.

However, in this paper, we demonstrate that Liao et al.'s scheme is not secure and it is vulnerable to stolen/lost smart card attack, impersonation (forgery) attack and password revealing attack. In fact, we prove that the scheme is equivalent to no password scheme. Then, we propose a security improvement to Liao et al.'s scheme.

The rest of this paper is organised as follows. In Section 2 we give a review of Liao et al.'s scheme. Then, in Section 3 we point out security flaws of their scheme and we demonstrate how it is vulnerable to attacks. Section 4 presents our improved solution to prevent these attacks. Security analysis and efficiency analysis are presented in section 5 and section 6, respectively. Finally, we conclude and give some future works.

2. Review of Liao et al.'s scheme

Liao et al.'s scheme [4] is composed of two phases as following. Notations used across this paper are slightly different from these used in [4], in order to provide more readability, and are described in Table 1.

2.1 Registration phase

This phase is performed only once when a new user *U* wants to register to the remote system *S*. This phase is supposed to be done out-of-band and in a secure manner. As

978-1-4244-3806-8/09/$25.00 © 2009 IEEE

shown in Figure 1, in order to register, the new user U and the remote system S proceed as follows:

1) U chooses a password PW and computes $h(PW)$.
2) U submits his/her identity ID and $h(PW)$ to S through a secure channel.
3) S then computes $N = h(PW) \oplus h(x \| ID)$.
4) S stores $\{N, y, h(.)\}$, where y is a secret key of S, into a smart card and then delivers this smart card to U in a secure manner.

Table 1. Notations

U	The user
PW	The password of U
ID	User Identity
$h(\cdot)$	a one-way hash function
$\oplus$	XOR operation
$\|\|$	Concatenation
S	The remote system
x	The secret key of S
y	a S's secret number stored in each user's smart card
T	The current time-stamp

2.2 Authentication phase

This phase is done whenever a user wants to access to the remote system. The steps of this phase are shown in Figure 2 and are as follows:

1) U inserts his/her smart card into the card reader of a terminal, and keys his/her PW. Then, the smart card computes:

$CID = h(PW) \oplus h(N \oplus y \oplus T)$ as a dynamic ID,

$B = h(CID \oplus h(PW))$, and

$C = h(T \oplus N \oplus B \oplus y)$, where T is the user current time-stamp.

2) U sends $\{CID, N, C, T\}$ to S.

Upon receiving the login request at the time T^*, the remote system S:

3) Verifies if whether $(T^* - T) \le \Delta T$. If it holds, S accepts U's login request, where ΔT is the expected valid time interval.
4) Then S computes:

$HP = CID \oplus h(N \oplus y \oplus T)$,

$B^* = h(CID \oplus HP)$,

and checks if $C = h(T \oplus N \oplus B^* \oplus y)$. If it holds, S accepts U to login the system. Otherwise, rejects it.

5) Then S computes $D = h(T' \oplus N \oplus B \oplus y)$, where T' is the system current time-stamp.
6) S sends $\{D, T'\}$ to U.

Upon receiving the reply message at the time T'', U verifies if whether $(T'' - T') \le \Delta T$, where ΔT is the expected valid time interval. If it holds, U computes $h(T' \oplus N \oplus B \oplus y)$ and compares it with the received D. If it holds, U confirms that he/she communicates with a valid S.

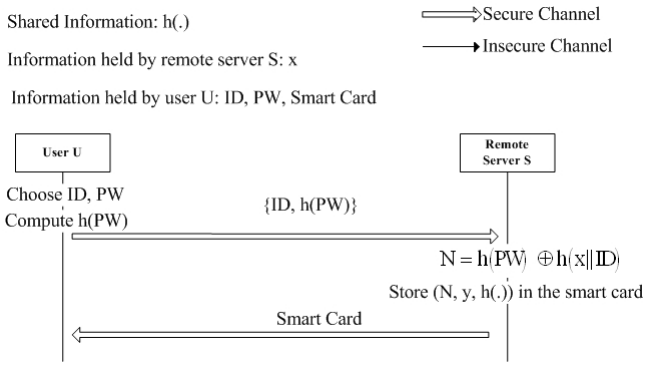

Figure 1. Registration phase

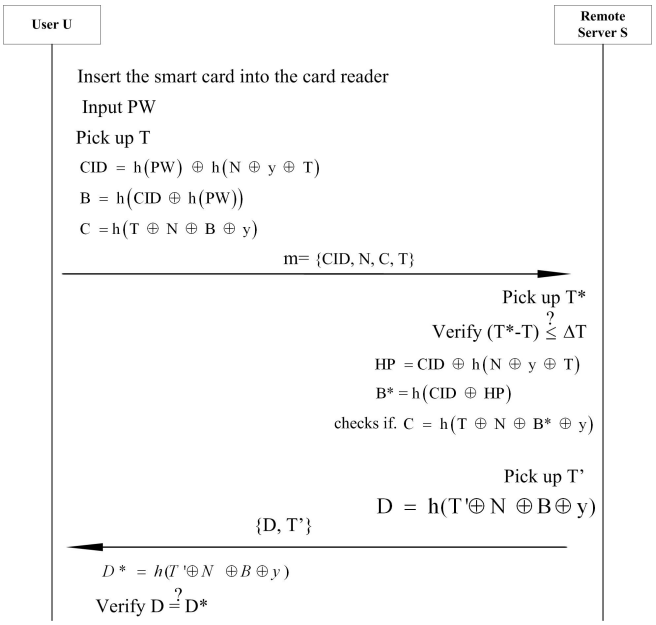

Figure 2. Authentication phase

3. Attacks on Liao et al.'s scheme

In this section we pick out attacks found in Liao et al.'s scheme and we demonstrate that the scheme is vulnerable to

stolen/lost smart card attack, impersonation (forgery) attack and password revealing attack.

3.1 Stolen/Lost Smart card attack

When an attacker gains access to a legal user's smart card. He proceeds as follows:

1) Attacker inserts the stolen/lost smart card into the card reader of a terminal, and keys a random password P. Then, the smart card computes:

$CID = h(P) \oplus h(N \oplus y \oplus T)$,

$B = h(CID \oplus h(P))$, and

$C = h(T \oplus N \oplus B \oplus y)$, where T is the current time-stamp.

*2) Attacker sends {*CID, N, C, T*} to* S.

Upon receiving the login request at the time T^*, the remote system *S*:

3) Verifies if whether $(T^* - T) \leq \Delta T$, which will holds as attacker uses a fresh time-stamp.
4) Then *S* computes:

$HP = CID \oplus h(N \oplus y \oplus T)$, which is equal to $h(P)$ and, $B^* = h(CID \oplus HP)$, which is equal to $B = h(CID \oplus h(P))$,

It can be noted that the B* calculated at the server is equal to B sent by user and this is true whatever the value of the used password. Thus, this scheme is equivalent to no password scheme i.e. it is a password independent scheme.

As a consequence of the above, $C = h(T \oplus N \oplus B^* \oplus y)$ will holds whatever the value of the used password and thus, *S* accepts attacker to login the system.

Note that the message sent by server to the attacker in order to be authenticated can be ignored by this latter.

3.2 Forgery attack

Forgery attack, known also as impersonation attack, consists in sending a forged message by an attacker to the server in order to be authenticated.

This attack is launched as follows:

1) Attacker intercepts an authorized user's login message {*CID*, *N*, *C*, *T*}

In order to be authenticated, attacker must provide CIDa, Na, Ca, Ta which verify that: $Ca = h(Ta \oplus Na \oplus B^* \oplus y)$ (1), where $B^* = h(CID \oplus HP)$ (2). However, attacker can not compute Ca as he doesn't know the secret value y. Thus attacker will use the value of the intercepted C as Ca. As a consequence, CIDa, Na, and Ta must verifies $C = h(Ta \oplus Na \oplus B^* \oplus y)$ i.e. $h(T \oplus N \oplus B \oplus y) = h(Ta \oplus Na \oplus B^* \oplus y)$ (3). In addition, putting $HP = CID \oplus h(Na \oplus y \oplus Ta)$ in (2) gives $B^* = h(CIDa \oplus CIDa \oplus h(Na \oplus Ta \oplus y))$

Using the following mathematic property, $a \oplus a = 0$ and $a \oplus 0 = a$ we obtain:

$B^* = h(h(Na \oplus Ta \oplus y))$. Thus, (3) holds if $Na \oplus Ta = N \oplus T$ and $B^* = B$ i.e. $h(h(Na \oplus Ta \oplus y)) = h(h(N \oplus T \oplus y))$ which is also true when $Na \oplus Ta = N \oplus T$. In conclusion, the authentication equation is true for all Ta and Na that verifies $Na = N \oplus T \oplus Ta$. Thus

2) Attacker send a new forged message ma={CID, Na, *C*, Ta}where:

Ta is the attacker current time-stamp and, $Na = N \oplus T \oplus Ta$

Upon receiving the login request at the time T^*, the remote system *S*:

3) Verifies if whether $(T^* - T) \leq \Delta T$, which will holds as attacker uses a fresh time-stamp.
4) Then *S* computes:

$HP = CID \oplus h(Na \oplus y \oplus Ta)$,

$B^* = h(CID \oplus HP)$, which is equal to

$= h(h(Na \oplus Ta \oplus y)) = h(h(N \oplus T \oplus y))$

$= B$

Then *S* checks if $C = h(Ta \oplus Na \oplus B^* \oplus y)$. Indeed this equation will holds as

$h(Ta \oplus Na \oplus B^* \oplus y) = h(T \oplus N \oplus B \oplus y)$ as $B^* = B$ and $Na \oplus Ta = N \oplus T$

The above demonstrations show that the attacker will succeeds in impersonating the server by using a forged message.

3.3 Password revealing attack

We define insider attacker by attacker, who is in the same time a user of the system. Thus this attacker has a valid smart card and as a consequence he can have a copy of the value of the server's secret y. (for more information about how we can extract information from smart card the interested reader can refer to [5] and [6]).

By intercepting a user login message {*CID*, *N*, *C*, *T*}, insider attacker can reveal user password by computing $h(PW) = CID \oplus h(N \oplus y \oplus T)$ as *CID*, *N*, *T* are intercepted from the insecure network and y is copied from its smart card.

4. Improvement of Liao et al.'s scheme

This section presents our proposed improvement. In our improved solution we conserve the registration phase as it is and we make the necessary change in the authentication phase in order to prevent attacks mentioned above.

The major problem of Liao et al.'s Scheme is that it is password independent and this characteristic result from the manner of using this secret information. In fact, the server extracts the password from the same parameter where user puts his password (the parameter is *CID*).

To resolve this problem we suggest that the server extract password from another parameter, example from *N* as follows: $h(PW) = N \oplus h(x \parallel ID)$. However, the identity of user (ID) is not sent and we wish to guarantee user anonymity. In order to resolve this problem we sent ID encapsulated in *CID*. Thus, we change *CID* as follows: $CID = ID \oplus h(N \oplus y \oplus T)$. By this manner we conserve anonymity of user and the principles of dynamic identity proposed in Das et al.'s scheme. The resulting authentication phase from this improvement is described in Figure 3 and has the following steps:

1) *U* inserts his/her smart card to the card reader of a terminal, and keys his/her *PW*. Then, the smart card computes:

$CID = ID \oplus h(N \oplus y \oplus T)$ as a dynamic ID,

$B = h(CID \oplus h(PW))$, and

$C = h(T \oplus N \oplus B \oplus y)$, where *T* is a time-stamp.

2) *U* sends {*CID*, *N*, *C*, *T*} to *S*.

Upon receiving the login request at the time T^*, the remote system *S*:

3) Verifies if whether $(T^* - T) \leq \Delta T$. If it holds, *S* accepts *U* the login request, where ΔT is an expected valid time interval.
4) Then *S* computes:

$ID^* = CID \oplus h(N \oplus y \oplus T)$,

$HP = N \oplus h(x \parallel ID)$

$B^* = h(CID \oplus HP)$,

and checks if $C = h(T \oplus N \oplus B^* \oplus y)$. If it holds, *S* accepts *U* to login the system. Otherwise, rejects it.

Then the scheme proceeds as in step 5 of Liao et al.'s one to authenticate the server.

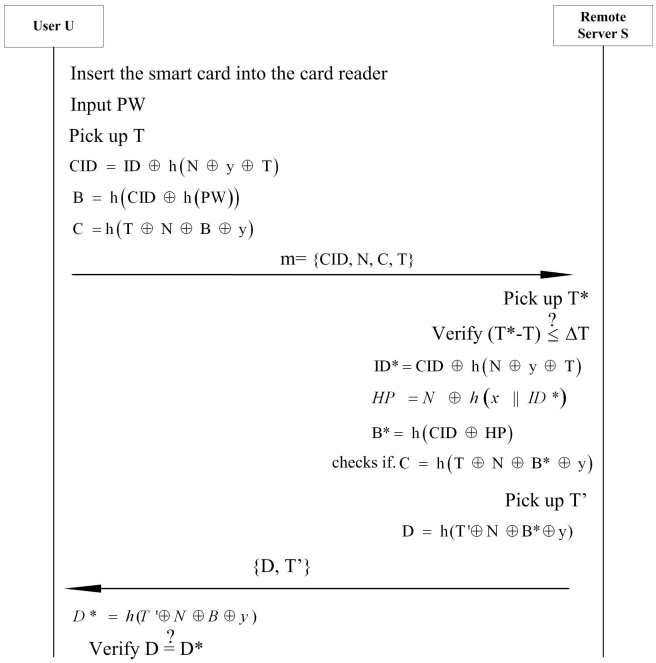

Figure 3. Our improved user authentication scheme

5. Security analysis

With this light modification, Liao et al.'s scheme becomes password and identity dependant and it is secure against:

- Stolen/lost smart card attack:

If an attacker gains access to a stolen/lost smart card, he can not be authenticated as he must prove the knowledge of the corresponded *PW* and ID.

Suppose an attacker gains access to a smart card which he knows the corresponding identity. The attacker will proceed as follows:

1) Enter a random password Pa
2) Then, the smart card computes:

$CID = ID \oplus h(N \oplus y \oplus T)$,

$Ba = h(CID \oplus h(Pa))$, and

$Ca = h(Ta \oplus N \oplus Ba \oplus y)$, where Ta is the current time-stamp at the attacker device.

3) Attacker sends {*CID*, *N*, Ca, Ta} to *S*.

Upon receiving the login request at the time T^*, the remote system *S*:

4) Verifies if whether $(T^* - Ta) \leq \Delta T$. We suppose it holds, so *S* will accept attacker's login request.
5) Then *S* computes:

$ID^* = CID \oplus h(N \oplus y \oplus Ta)$,

$HP = N \oplus h(x \parallel ID^*)$, which is, in principle, different from h(Pa), where Pa is the random password chosen by attacker.

$B^* = h(CID \oplus HP)$, which is different from Ba calculated by attacker as $HP <> h$(Pa) and thus the verification of $Ca = ? h(Ta \oplus N \oplus B^* \oplus y)$ will not hold, and therefore S will reject U to login the system.

- Forgery attack:

Suppose an attacker intercepts a login message m={CID, N, C, T} of an authorized user. Then he will try to forge it in order to gain access. The first thing to do is to change the value of time-stamp in order to be in expected interval ΔT. Thus attacker will change T by Ta where Ta is the current time-stamp. In order to conserve the same identity at the server side attacker must change N by Na as follows: $Na = N \oplus T \oplus Ta$. Identity will match at the server side however the password will not as server will compute $Na \oplus h(x \parallel ID) \neq [h(PW) = N \oplus h(x \parallel ID)]$ and as a consequence Ba ≠ B and $[C = h(T \oplus N \oplus B \oplus y)] \neq [h(Ta \oplus Na \oplus Ba \oplus y) = h(T \oplus N \oplus Ba \oplus y)]$. The attacker's login request will be rejected.

- Password Revealing Attack:

The password revealing attack mentioned in section 3.3 is no longer possible as the value $h(PW)$ is no longer used in the computing of parameters transmitted in the login message. The only thing that the insider attacker can reveal is the identity of user and we showed above that with this information attacker can not succeed in authentication phase.

The following table summarizes the security analysis comparison between Liao al.'s scheme and our improved scheme.

Table 2. Resistance to attack comparison

Attack / scheme	Our improved scheme	Liao al.'s scheme
Smart card lost attack	Robust	Vulnerable
Forgery attack	Robust	Vulnerable
Password revealing attack	Robust	Vulnerable

6. Efficiency analysis

We show in this section a comparison between Das et al.'s scheme [1], Liao et al.'s scheme [4] and our improved solution. This comparison is based on the number of operation that requires each scheme. The comparative results are shown in Table 3, where T_H represents the execution time of the one-way hash function h(.) and T_{XOR} the execution time of the exclusive-or operation $\oplus$.

Our improved scheme requires the same number of operation in the registration phase as Liao et al.'s and $(8 \text{ x } T_H + 15 \text{ x } T_{XOR})$ operations in the authentication phase, which is less compared to Liao et al.'s scheme.

Table 3. Comparison of computational cost

Phase	Das et al.'s scheme	Liao et al.'s scheme	Our improved scheme
Registration	$2T_H + T_{XOR}$	$2T_H + T_{XOR}$	$2T_H + T_{XOR}$
Authentication	$7T_H + 14T_{XOR}$	$9T_H + 20T_{XOR}$	$8T_H + 15T_{XOR}$
Total Cost	$9T_H + 15T_{XOR}$	$11T_H + 21T_{XOR}$	$10T_H + 16T_{XOR}$

In conclusion, our complete scheme is more efficient than Liao et al.'s one as it requires less hash function and XOR computation.

- Possible Efficiency improvement:

In our improved scheme we can eliminate some calculation without weaken its security. In fact, in the authentication phase computing C as a function of B is equivalent of computing C as a function of $h(PW)$. Thus step 1 in authentication phase can be replaced by $C = h(T \oplus N \oplus h(PW) \oplus y)$.

7. Conclusion

Remote user authentication is a critical security service, which allows remote system to verify the validity of the user before allowing him the requested services.

In this paper, we cryptanalysed a previously published remote user authentication scheme and we have shown that Liao *et al.*'s scheme is vulnerable to stolen/lost smart card attack, impersonation (forgery) attack and password revealing attack and we have proposed a security improvement to their scheme. The efficiency comparison of our scheme with other one shows that our scheme is more efficient and requires a lower computation cost.

Thanks to this characteristics our scheme have more chance to be implemented in the industrial community and can be used for mobile communication especially those that are resources constrained like wireless sensor networks.

Thus our future work is to give a real implementation of our proposed solution in a real platform. The platform is composed of two principals components: PDA (Personnal Digital Assistant) equipped with smart card, which will play the role of the client and sensor node CC2430 [7], which will play the role of the remote authentication system.

8. Acknowledgement

We would like to thank member of computer science department of ISET Sfax and Wireless Sensor Network team of CES Laboratory (ENIS Sfax) for their support and help in doing this work.

9. References

[1] C.S Tsai, C.C Lee, and M.S Hwang, “Password Authentication Schemes: Current Status and Key issues”, International Journal of Network security, Vol.3 No.2, 2006, pp.101-115.

[2] I.E. Liao, C.C. Lee, and M.S. Hwang, “A password authentication scheme over insecure networks”, Journal of Computer and System Sciences, 2006.

[3] M. L. Das, A. Saxena, and V. P. Gulati, “A dynamic id-based remote user authentication scheme,” IEEE Transactions on Consumer Electronics, vol. 50, no. 2, May 2004, pp. 629-631.

[4] I. E. Liao, C. C. Lee, and M. S. Hwang, “Security enhancement for a dynamic id-based remote user authentication scheme,” In Proceedings of the IEEE International Conference on Next Generation Web Services Practices (NWeSP 2005), Aug. 2005, pp. 22-26.

[5] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Proc. Advances in Cryptology (CRYPTO'99), pp.388-397, 1999.

[6] 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, 2002, pp. 541-552.

[7] CC2430: “System-on-Chip Solution for 2.4 GHz IEEE 802.15.4 / ZigBee”, Available at: http://focus.ti.com/docs/prod/folders/print/cc2430.html, viewed on 2008.