Computación y Sistemas
ISSN: 1405-5546
computacion-y-sistemas@cic.ipn.mx
Instituto Politécnico Nacional
México

Martínez-Peláez, Rafael; Rico-Novella, Francisco; Velarde-Alvarado, Pablo
Security Enhancement on Li-Lee's Remote User Authentication Scheme Using Smart Card
Computación y Sistemas, vol. 18, núm. 4, 2014, pp. 709-717
Instituto Politécnico Nacional
Distrito Federal, México

Security Enhancement on Li-Lee's Remote User Authentication Scheme Using Smart Card

Rafael Martínez-Peláez[1], Francisco Rico-Novella[2], and Pablo Velarde-Alvarado[3]

[1] Institute of Informatics, University of Sierra Sur, Miahuatlán de Porfirio Díaz, Mexico

[2] Department of Telematics Engineering, Universitat Politecnica de Catalunya, Barcelona, Spain

[2] Area of Basic Sciences and Engineering, Autonomous University of Nayarit, Tepic, Mexico

rpelaez@unsis.edu.mx, f.rico@entel.upc.edu, pvelarde@uan.edu.mx

Abstract. Recently, Li and Lee proposed a new remote user authentication scheme using smart card. However, their scheme requires a verification table and the user's identity is not protected. Moreover, users cannot change their password off-line. In order to overcome the security flaws, we propose a new scheme which provides more security without affecting the merits of the original scheme.

Keywords. Cryptanalysis, mutual authentication, network security, session key, smart card.

1 Introduction

The use of new electronic services, such as e-government, requires strong security. Among the security components used to protect the access to data stored in a server, the remote user authentication process is a key element. Remote user authentication schemes are used to verify and validate the legitimacy of each user by means of the knowledge of specific security parameters.

The first remote user authentication scheme for an open network was proposed in [10]. The scheme is based on one-way hash function, such as MD5 [20] or SHA-2 [19]. However, the scheme requires that the server stores a password list making it vulnerable to threats of revealing passwords in the directory [3] or modifying the verification table [8].

In 1991, a remote user authentication scheme with smart cards and without verification table was proposed in [3]. Since 1991, several remote user authentication schemes using smart cards have been proposed [21, 22, 25, 26] to enhance security. Unfortunately, in those schemes, the user sends its identity over a common channel to the server making them susceptible to identity-theft attack [6].

Later, Das, Saxena, and Gulati proposed the first dynamic ID-based remote user authentication scheme [6]. The concept of dynamic ID prevents that an attacker can know the user's identity. Since the proposal of Das *et al*., several dynamic ID-based remote user authentication schemes [1, 4, 7, 9, 11, 14, 16, 17, 18, 23, 24, 27] have been proposed with the attempt to reduce security vulnerabilities.

In 2011, Li and Lee proposed a robust remote user authentication scheme [13] and claimed that their scheme is more secure than those in previous work. However, we demonstrate that their scheme does not achieve all the security goals [12, 15] which a strong remote user authentication scheme should provide, such as protect the identity of each user during the login phase, also, it does not maintain a verification table and password change off-line.

In this paper, we aim to modify the scheme proposed by Li and Lee and propose a new scheme. The new scheme keeps the merits of Li-Lee's scheme.

The rest of this paper is organized as follows. In Section 2, we present a brief review of Li-Lee's scheme. We show the security flaws of Li-Lee's

ISSN 1405-5546
doi: 10.13053/CyS-18-4-1398

Table 1. Notation

Notation	Meaning
U	The user
ID	The identity of U
PW	The password of U
SC	The smart card of U
S	The server
x, y	The secret key of S
h( )	One-way hash function
SK	The session key between U and S
$E_{SK}\{\ \}$	Symmetric encryption function using SK
$D_{SK}\{\ \}$	Symmetric decryption function using SK
RU	The nonce generated by U
RSC	The nonce generated by SC
RS	The nonce generated by S
N	The number of times U re-registers to S
⊕	Exclusive-OR operation
||	String concatenation operation
□	Secure channel
□	Common channel

scheme in Section 3. In Section 4, we present our scheme. The security evaluation and comparison of the proposed scheme is described in Section 5. We conclude the paper with Section 6.

2 Review of Li-Lee's Scheme

In this section, we briefly review the scheme proposed in [13]. The notation used in this paper is summarized in Table 1.

2.1 Registration Phase

In this phase, the user and the server carry out the registration process as follows:

1. $U \rightarrow S$: $ID, h(h(PW \oplus RU_1))$
2. S: $C_1 = h(ID \,||\, x \,||\, N) \oplus h(h(PW \oplus RU_1))$
3. S: STORE ID, N, $h(h(PW \oplus RU_1))$ INTO Database
4. $S \rightarrow U$: SC containing $h(.)$, ID and C_1
5. U: STORE RU_1 INTO SC

2.2 Login Phase

In this phase, the user computes the login request message by means of the following process:

1. $U \rightarrow SC$: ID, PW, RU_2
2. SC: GENERATE RSC_1
3. SC: $C_2 = h(PW \oplus RU_1)$
4. SC: $C_3 = C_1 \oplus h(C_2)$
5. SC: $C_4 = C_3 \oplus C_2$
6. SC: $C_5 = h(h(PW \oplus RU_2))$
7. SC: $SK = h(C_2 \,||\, C_3)$
8. SC: $C_6 = E_{SK}\{\ C_5 \oplus RSC_1\ \}$
9. $U \rightarrow S$: ID, C_4, C_6

2.3 Verification Phase

In this phase, the server and the user verify the identity of each other by means of the following process:

1. S: IF $ID^* \neq ID$ THEN Abort
2. S: $C_7 = h(ID \,||\, x \,||\, N)$
3. S: $C_8 = C_4 \oplus C_7$
4. S: $C_9 = h(C_8)$
5. S: IF $C_9 \neq h(h(PW \oplus RU_1))$ THEN Abort
6. S: $SK = h(C_8 \,||\, C_7)$
7. S: $(C_5 \oplus RSC_1) = D_{SK}\{\ C_6\ \}$
8. S: GENERATE RS_1
9. S: $C_{10} = E_{SK}\{\ C_5 \,||\, RSC_1 \,||\, RS_1\ \}$
10. S: REPLACE $h(h(PW \oplus RU_1))$ by C_5 INTO Database
11. $S \rightarrow U$: C_{10}

12. *SC:* $(C_5^* \,||\, RSC_1^* \,||\, RS_1^*) = D_{SK}\{ C_{10} \}$
13. *SC:* $C_5^* \,||\, RC_1^* \,?= C_5 \,||\, RSC_1$
14. *SC:* REPLACE RU_1 by RU_2 and C_1 by $C_3 \oplus C_5$
15. $U \rightarrow S: h(RS_1)$
16. *S:* IF $h(RS_1)^* \neq h(RS_1)$ THEN Abort
17. *U:* $SK = h(RSC_1 \oplus RS_1)$
18. *S:* $SK = h(RSC_1 \oplus RS_1)$

2.4 Password Update Phase

In this phase, the user and the server perform the update password process as follows:

1. $U \rightarrow$ *SC: ID, PW,* PW_{new}, RU_3
2. $C_2 = h(PW \oplus RU_2)$
3. $C_3 = C_1 \oplus h(C_2)$
4. $C_4 = C_3 \oplus C_2$
5. $C_5 = h(h(PW_{new} \oplus RU_3))$
6. $SK = h(C_2 \,||\, C_3)$
7. $C_6 = E_{SK}\{ C_5 \oplus RSC_2 \}$
8. $U \rightarrow S$: *ID,* C_4, C_6
9. Carry out the verification phase
10. REPLACE $h(h(PW \oplus RU_1))$ by C_5 INTO Database
11. $S \rightarrow U: C_{10}$
12. *SC:* $(C_5^* \,||\, RSC_1^* \,||\, RS_1) = D_{SK}\{C_{10}\}$
13. *SC:* $C_5^* \,||\, RSC_1^* \,?= C_5 \,||\, RSC_1$
14. *SC:* REPLACE RU_1 by RU_3 and C_1 by $C_3 \oplus C_5$

3 Security Flaws of Li-Lee's Scheme

In this section, we carry out a security analysis of the scheme proposed in [13], based on the security goals described in [12, 15].

Without verification table: in this case, the scheme proposed by Li and Lee fails. The server must maintain a verification table.

Users choose password freely: in this case, the scheme proposed by Li and Lee achieves this goal. The user chooses her identity and password in the registration phase.

No password reveal: in this case, the goal is achieved. The user sends $h(h(PW \oplus RU_1))$ to the server instead of her password.

Mutual authentication: this goal is achieved because the server sends security parameters $(C_{10} \,||\, RC_1 \,||\, RS_1)$ encrypted with the session key $SK = h(C_8 \,||\, C_7)$ which can be computed only with the knowledge of X and N. On the other hand, the user needs to decrypt the message using the session key which can be computed only with the knowledge of $C_2 = h(PW \oplus RU_1)$.

Session key agreement: this goal is achieved because the server and the user compute the same session key for carrying out the mutual authentication process.

User anonymity: in this case, the scheme proposed by Li and Lee fails. The user sends her identity over a public network.

Efficiency for wrong password login: in this case, the scheme proposed by Li and Lee fails. The smart card does not verify the validity of PW before it initializes the creation of the login request message.

4 Proposed Scheme

This section describes the process for a new dynamic ID-based remote user authentication scheme. It is based on one-way hash function and symmetric cryptography. The scheme allows the user to establish a session key and get access to the server, but at the same the user does not reveal her ID.

The initial assumptions are 1) the bit length of the secret keys and nonce is 256, 2) the one-way function used is SHA-2, and 3) the one-way function is public.

4.1 Registration Phase

When the user wants to be part of the system, she chooses an ID and PW, and then hashes the ID and PW to create a message digest. Next, the user sends the message digest to the server over a secure channel. Upon receiving the message digest from the user, the server computes the

security parameters (steps 2 to 4) using exclusive-or operation, string concatenation operation and one-way hash function. Then, the server stores the security parameters into the user's smart card and delivers the smart card to the user. The process is as follows:

1. $U \rightarrow S: RU_1, h(ID \,||\, PW)$
2. $S: C_1 = h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1) \oplus h(ID \,||\, PW)$
3. $S: C_2 = h(h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1))$
4. $S: C_3 = h(h(x \oplus y) \,||\, h(x) \,||\, h(y) \,||\, RU_1)$
5. $S \rightarrow U:$ SC containing $h(.), RU_1, C_1, C_2, C_3$

4.2 Login Phase

Whenever a user wants to get access to the server, she inserts the smart card into the smart card reader and keys the correct ID and PW. Then, the smart card verifies the correctness of the ID and PW by means of steps 2, 3 and 4. If the verification is positive, the smart card computes the login request message. As a result, the user gets a unique login request message (RU_1, C_4, C_5) which does not have its ID or PW in clear text. In step 9, the smart card sends the login request message to the server over an open channel. It is very important to note that it is very hard to link the ID of the user with the login request message. The process is as follows:

1. $U \rightarrow SC: ID, PW$
2. $SC: h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1)^* = C_1 \oplus h(ID \,||\, PW)$
3. $SC: C_2^* = h(h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1)^*)$
4. $SC:$ IF $C_2^* \neq C_2$ THEN Abort
5. $SC:$ GENERATE RSC_1
6. $SC: C_4 = h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1) \oplus h(ID \,||\, PW \,||\, RSC_1)$
7. $SC: SK = h(h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1) \,||\, C_3 \,||\, h(ID \,||\, PW \,||\, RSC_1))$
8. $SC: C_5 = E_{SK}\{ C_3, RSC_1 \}$
9. $SC \rightarrow S: RU_1, C_4, C_5$

4.3 Verification Phase

Upon receiving the login request message, the server verifies the legitimacy of the user by means of steps 1 to 6. If the verification is positive, the server generates a nonce RU_2 and uses it to compute new security parameters (steps 8 to 11) for the user. Then, the server generates a nonce RS_1 and uses it to compute the secret parameter between the server and the smart card $h(RSC_1 \oplus RS_1)$. In step 15, it sends the login response message.

Upon receiving the login response message, the user's smart card decrypts the message using the session key. Then it computes and verifies the validity of the secret parameter $h(RSC_1 \oplus RS_1)$. If the verification is positive, the smart card replaces the old value of C_1, C_2, C_3, RU_1 by a new one C_{1new}, C_{2new}, C_{3new}, RU_2 and the mutual authentication is done.

1. $S: h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1)^*$
2. $S: h(h(x \oplus y) \,||\, h(x) \,||\, h(y) \,||\, RU_1)^*$
3. $S: h(ID \,||\, PW \,||\, RSC_1)^* = h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1)^* \oplus C_4$
4. $S: SK = h(h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1)^* \,||\, h(h(x \oplus y) \,||\, h(x) \,||\, h(y) \,||\, RU_1)^* \,||\, h(ID \,||\, PW \,||\, RSC_1)^*)$
5. $S: C_3, RSC_1 = D_{SK}\{ C_5 \}$
6. $S:$ IF $C_3 \neq h(h(x \oplus y) \,||\, h(x) \,||\, h(y) \,||\, RU_1)^*$ THEN Abort
7. $S:$ GENERATE RU_2
8. $S: h(h(x \,||\, y \,||\, RU_2) \,||\, h(x \oplus y) \,||\, RU_2)$
9. $S: C_{1new} = h(h(x \,||\, y \,||\, RU_2) \,||\, h(x \oplus y) \,||\, RU_2) \oplus h(ID \,||\, PW \,||\, RSC_1)$
10. $S: C_{2new} = h(h(h(x \,||\, y \,||\, RU_2) \,||\, h(x \oplus y) \,||\, RU_2))$
11. $S: C_{3new} = h(h(x \oplus y) \,||\, h(x) \,||\, h(y) \,||\, RU_2)$
12. $S:$ GENERATE RS_1
13. $S: h(RSC_1 \oplus RS_1)$

14. S: $C_6 = E_{SK}\{ C_{1new}, C_{2new}, C_{3new}, RU_2, RS_1, h(RSC_1 \oplus RS_1)\}$
15. $S \rightarrow SC$: C_6
16. SC: $C_{1new}, C_{2new}, C_{3new}, RU_2, RS_1, h(RSC_1 \oplus RS_1) = E_{SK}\{ C_6 \}$
17. SC: $h(RSC_1 \oplus RS_1)^*$
18. SC: IF $h(RSC_1 \oplus RS_1)^* \neq h(RSC_1 \oplus RS_1)$ THEN Abort
19. SC: REPLACE C_1 by C_{1new}, C_2 by C_{2new}, C_3 by C_{3new}, and RU_1 by RU_2

4.4 Password Change Phase

This phase is invoked whenever the user requires changing her PW for a new one PW_{new}. The user inserts her smart card into the smart card reader and then types her ID and PW. Then, the user's smart card computes the following operations:

1. $U \rightarrow SC$: ID, PW, PW_{new}
2. SC: $h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1)^* = C_1 \oplus h(ID \,||\, PW)$
3. SC: $C_2^* = h(h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1)^*)$
4. SC: IF $C_2^* \neq C_2$ THEN Abort
5. SC: $C_{1new} = h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1) \oplus h(ID \,||\, PW_{new})$
6. SC: REPLACE C_1 by C_{1new}

5 Security Evaluation and Comparison

In this section, we show that our proposed scheme resists very well-known attacks and achieves the security goals described in [12, 15]. Moreover, we carry out the formal verification of our protocol using the AVISPA tool to validate its security.

5.1 Security Analysis

We demonstrate that the proposed scheme is secure against very well-known attacks.

Off-line guessing attack: an adversary may attempt to extract the server secret keys (x, y) from C_1, C_2, C_3. However, this attack will fail because it is computationally infeasible to invert the one-way hash function. Moreover, if the adversary is a legal user, she can recover $h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1)$ from C_1, however, she cannot obtain x and y from $h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1)$.

Masquerade user attack: if an adversary may attempt to masquerade as a valid user, she must be able to forge a valid login request message (RU_1, C_4, C_5). However, she cannot compute a valid $C_4 = h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1) \oplus h(ID \,||\, PW \,||\, RSC_1)$ without the knowledge of ID, PW, x, and y. Moreover, the adversary should be capable to compute the session key $SK = h(h(h(x \,||\, y \,||\, RU_1) \,||\, h(x \oplus y) \,||\, RU_1) \,||\, C_3 \,||\, h(ID \,||\, PW \,||\, RSC_1))$ which at this point is very hard.

Masquerade server attack: if an adversary attempts to masquerade as a server, she must be able to forge a valid login response message $C_6 = E_{SK}\{ C_{1new}, C_{2new}, C_{3new}, RU_2, RS_1, h(RSC_1 \oplus RS_1)\}$. However, the attacker does not know the correct values of x, y, and C_3, which makes it very hard to compute the correct session key.

Stolen database attack: in this scheme, the server does not maintain a verification table which stores sensitive information related with each user.

Parallel session attack: if the adversary has captured previous communications between the victim and the server, the adversary may attempt to impersonate as a legal user. However, the value of RU_i, C_4 and C_5 are different each time because the value of RU_i is updated.

Leak of password attack: if the adversary obtains the victim's smart card, she cannot recover ID or PW from C_1, C_2 or C_3 or any combination of them.

5.2 Security Goals

We demonstrate that the proposed scheme achieves the security goals described in [12, 15].

Early detection of incorrect password: in this scheme, if an adversary obtains the victim's smart card and she tries to initialize the login phase, she will fail because she must be authenticated by the smart card before she initializes the login phase. In this case, the adversary needs to know the correct ID and PW.

Without verification table: in this scheme, the server does not maintain a verification table or database.

Users choose password freely: in this scheme, each user chooses her password freely without the participation of the server.

No password reveal: this security goal is achieved; the user shares $h(ID \| PW)$ with the server instead of her password in clear.

User anonymity: this security goal is achieved; the user does not send her ID in clear to the server over an open channel.

Mutual authentication: this goal is achieved because the smart card and the server verify the identity of each other.

Session key agreement: this goal is achieved because the smart card and the server compute the same session key to encrypt and decrypt sensitive information.

5.3 Formal Verification

We model our protocol using AVISPA (Automated Validation of Internet Security Protocols and Applications) [2] tool. The specifications of the protocol are in HLPSL (High-Level Protocol Specification Language) [5]. An HLPSL is divided into roles played by any entity in the protocol, as well as the session and environment roles. Moreover, it is necessary to define the security goals that have to be done by the protocol.

In the validation process, we considered the smart card and server roles played by SC and S, respectively. The role *smart card* appears in Figure 1.

The role *environment* is shown in Figure 2. This role is used to find vulnerabilities in the protocol that an intruder (i) can use to break the security. In this case, the intruder is the network and it knows all the messages sent by role *smart card* and role *server*.

```
role smartcard (    SC, S : agent,
                    K : symmetric_key,
                    X, Y : text,
                    H : function,
                    Snd, Rcv: channel(dy))
played_by SC def=
local
State : nat,
Ru, Rsc, Rs : text,
Id, Pw : text,
C3, C4, K1 : message
init
State := 0
transition
1. State = 0 /\ Rcv(start) =|>
  State' := 2 /\ Ru' := new()
      /\ Rsc' := new()
      /\ Id' := new()
      /\ Pw' := new()
      /\ C3' := H(H(xor(X, Y)).H(X).H(Y).Ru')
      /\ C4' := xor(H(H(X.Y.Ru').H(xor(X, Y)).Ru'), H(Id'.Pw'.Rsc'))
      /\ Snd(Ru'.C4'.{C3'.Rsc'}_K)
2. State = 2 /\ Rcv({Rs'.H(Rsc.Rs')}_K) =|>
  State' := 4 /\ K1' := H(H(X.Y.Ru).H(xor(X, Y)).Ru).C3.H(Id.Pw.Rsc)
     /\ Snd({Rsc.H(Rsc.Rs)}_K1')
     /\ request(SC, S, smartcard_server_rsc, Rsc')
     /\ witness(SC, S, server_smartcard_rs, Rs')
end role
```

Fig. 1. Role *smart card* in HLPSL

```
role environment()
def=
const
      server_smartcard_rs,
      smartcard_server_rsc,
      sc, s : agent,
      x, y : text,
      h : function,
      kscs, ksci, ksi : symmetric_key,
      rsc, rs, k1 : protocol_id
intruder_knowledge = {sc, s, ksci, ksi, x, y, h}
composition
      session(sc,s,kscs,x,y,h)
      /\ session(sc,i,ksci,x,y,h)
      /\ session(s,i,ksi,x,y,h)
end role
```

Fig. 2. Role *environment* in HLPSL

```
goal
      secrecy_of k1, rs, rsc
      authentication_on server_smartcard_rs
      authentication_on smartcard_server_rsc
end goal
```

Fig. 3. Security goals

We verify the following security goals: (1) confidentiality of the nonce generated by the smart card and server, and the session key; and

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\SPAN\testsuite\results\RMP.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 3.81s
  visitedNodes: 2636 nodes
  depth: 8 plies
```

Fig. 4. Results from back-end OFMC

(2) authentication of the smart card and server. The security goals are shown in Figure 3.

The verification was done using the back-end OFMC because it can be used to verify protocols which compute operations with or-exclusive. Moreover, the back-end OFMC can detect the following attacks: replay and parallel session. The total number of nodes that have been tested was 2,636 in 3.81 seconds. Figure 4 shows the results of the simulation.

From the result, we can conclude that the proposed protocol is secure under the test of AVISPA and it achieves the security goals.

5.4 Comparison

We compare our proposal with Li-Lee's scheme in terms of security goals. Table 2 summarizes the security comparison.

The proposed scheme does not need a verification table. As it is explained in [3] and [8], an attacker or intruder can modify or extract sensitive information from the database. For that reasons, Chan and Wu proposed a remote password authentication without verification table.

The proposed scheme keeps the user anonymity during the registration phase and login phase. As it is explained in [6], an attacker or intruder can get access to the network in order to obtain the user's identity. By means of this action, the attacker or intruder can trace the user's activity and can make identity theft attack. For that reasons, Das, Saxena and Gulati introduced the concept of dynamic identity.

Table 2. Security comparison between our scheme and Li-Lee's scheme

Security goals	Li-Lee's scheme	Our scheme
Without verification table	No	Yes
Users choose password freely	Yes	Yes
No password reveal	Yes	Yes
Mutual authentication	Yes	Yes
Session key agreement	Yes	Yes
User anonymity	No	Yes
Efficiency for wrong password login	No	Yes

6 Conclusions

In this paper, we proposed a new remote user authentication scheme which removes all the security flaws found in Li-Lee's scheme described in Section 3. The proposed scheme can resist very well-known attacks and achieves all the security goals that a secure remote user authentication scheme should have. We evaluated the security of our proposal using HLPSL, AVISPA tool, and back-end OFMC. After the simulation, the result was safe.

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions. This research was supported by the Mexican Teacher Improvement Program (PROMEP), under the project number PROMEP/103.5/12/4525.

References

1 **Ahmed, M.A., Lakshmi, D.R., & Sattar, S.A. (2009).** Cryptanalysis of a more efficient and secure dynamic ID-based remote user authentication scheme. *International Journal of Network Security & Its Applications*, Vol. 1, No. 3, pp. 32–37.

2 **Armando, A., Basin, D., Boichut, Y., Chevalier, Y., Compagna, L., Cuellar, J., & Hankes Drielsma, P. (2005).** The AVISPA Tool for the automated validation of internet security protocols and applications. *Proc. of 17th International Conference on Computer Aided Verfication*, pp. 281–285.

3 **Chang, C.C. & Wu, T.C. (1991).** Remote password authentication with smart cards. *IEE Proceedings-E*, Vol. 138, No. 3, pp. 165–168.

4 **Chen, T.H., Hsiang, H.C., & Shih, W.K. (2011).** Security enhancement on an improvement on two remote user authentication schemes using smart cards. *Future Generation Computer Systems*, Vol. 27, No. 4, pp. 377–380.

5 **Chevalier, Y., Compagna, L., Cuellar, J., & Hankes Drielsma, P. (2004).** A High Level Protocol Specifiction Language for Industrial Security-Sensitive Protocols. *Workshop on Specification and Automated Processing of Security Requirements*, pp. 193–205.

6 **Das, M.L., Saxena, 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.

7 **Hu, L.I., Niu, X.X., & Yang, Y.X. (2007).** Weaknesses and improvements of a remote user authentication scheme using smart cards. *The Journal of China Universities of Posts and Telecommunications*, Vol. 14, No. 3, pp. 91–94.

8 **Hwang, M.S. & Li, L.H. (2000).** A new remote user authentication scheme using smart card. *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, pp. 28–30.

9 **Kim, S.K. & Chung, M.G. (2009).** More secure remote user authentication scheme. *Computer Communications*, Vol. 32, No. 66, pp. 1018–1021.

10 **Lamport, L. (1981).** Password authentication with insecure communication. *Communications of the ACM*, Vol. 24, No. 11, pp. 770–772.

11 **Lee, Y.C., Chang, G.K., Kuo, W.C., & Chu, J.L. (2008).** Improvement on the dynamic ID-based remote user authentication scheme. *Proc. of 7th International Conference on Machine Learning and Cybernetics*, pp. 3283–3287.

12 **Li, C.T. (2011).** Secure smart card based password authentication scheme with user anonymity. *Information Technology and Control*, Vol. 40, No. 2, pp. 157–162.

13 **Li, C.T. & Lee, C.C. (2011).** A Robust remote user authentication scheme using smart card. *Information Technology and Control*, Vol. 40, No. 3, pp. 236–244.

14 **Liou, Y.P., Lin, J., & Wang, S.S. (2006).** A New Dynamic ID-Based Remote User Authentication Scheme using Smart Cards. *Proc. of 16th Information Security Conference*, pp. 198–205.

15 **Madhusudhan, R. & Mittal, R.C. (2012).** Dynamic ID-based remote user password authentication schemes using smart cards: A review. *Journal of Network and Computer Applications*, Vol. 35, No. 4, pp. 1235–1248.

16 **Martinez-Peláez, R., Rico-Novella, F., & Velarde-Alvarado, P. (2013).** Cryptanalysis and improvement of Chen-Hsiang-Shih's remote user authentication scheme using smart cards. *Revista Facultad de Ingeniería Universidad de Antioquia*, Vol. 68, pp. 27–35.

17 **Martínez-Peláez, R., Rico-Novella, F.J., Forné, J., & Velarde-Alvarado, P. (2013).** Security Improvement of Two Dynamic ID-based Authentication Schemes by Sood-Sarje-Singh. *Journal of Applied Research and Technology*, Vol. 11, No. 5, pp. 755–763.

18 **Misbahuddin, M. & Bindu, C.S. (2008).** Cryptanalysis of Liao-Lee-Hwang's dynamic ID scheme. *International Journal of Network Security*, Vol. 6, No. 2, pp. 211–213.

19 **NIST (1995).** Secure Hash Standard (SHA), FIPS PUB 180-1, National Institute of Standards and Technology, http://www.itl.nist.gov/fipspubs/fip180-1.htm.

20 **Rivest, R. (1992).** RFC 1321 - the MD5 message-disgest algorithm, IETF Working Group, http://www.ietf.org/rfc/rfc1321.txt.

21 **Sandirigama, M., Shimizu, A., & Noda, M.T. (2000).** Simple and secure pass-word authentication protocol (SAS). *IEICE Transactions on Communications*, E83-B(6), pp.1363–1365.

22 **Sun, H.M. (2000).** An efficient remote user authentication scheme using smart cards. *IEEE Transactions on Computers*, Vol. 46, No. 4, pp. 958–961.

23 **Wang, X.M., Zhang, W.F., Zhang, J. S., & Khan, M.K. (2007).** Cryptanalysis and improvement on

two efficient remote user authentication scheme using smart cards. *Computer Standards & Interfaces*, Vol. 29, No. 5, pp. 507–512.

24 **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. 2, pp. 583–585.

25 **Wu, T. & Sung, H. (1996).** Authenticating passwords over an insecure channel. *Computer & Security*, Vol.15, No. 5, pp. 431–439.

26 **Yang, W.H. & Shieh, S.P. (1999).** Password Authentication Schemes with Smart Cards. *Computers & Security*, Vol.18, No. 8, pp. 727–733.

27 **Yoon, E.J. & Yoo, K.Y. (2006).** Improving the dynamic ID-based remote mutual authentication scheme. in *On the Move to Meaningful Internet Systems*, Vol. LNCS 4277, pp. 499–507.

Rafael Martínez Peláez received his Ph.D. from the Technical University of Catalonia (Spain) in 2010. He is a researcher-professor with the Institute of Informatics, University of Sierra Sur, Miahuatlan de Porfirio Diaz, Mexico. He is a member of the National Network on Information and Communication Technologies supported by CONACYT. His research interests include authentication technologies, smart cards, and security issues on electronic services.

Francisco Rico Novella received his degree in Telecommunication Engineering and his Ph.D. from the Technical University of Catalonia (Spain) in 1989 and 1995, respectively. Presently, he works at the Department of Telematic Engineering with the Telematics Service Group. His current research interests include network security and electronic commerce.

Pablo Velarde Alvarado is a researcher and full-time professor at the Area of Basic Sciences and Engineering of the Universidad Autónoma de Nayarit. He received his B.Tech. degree in Electronics Engineering from the Universidad Autónoma de Guadalajara (UAG), in 1993, and his M.Sc. and Ph.D. degrees in Electrical Engineering from the Centro de Investigación y de Estudios Avanzados del IPN (CINVESTAV-IPN) in Guadalajara City, in 2001 and 2009, respectively. He has been a member of SNI (National System of Researchers, Mexico) at the candidate level since 2011. His current research interests include intrusion detection systems and network traffic modeling.

Article received on 19/09/2012, accepted on 07/08/2013.