Remote Authentication Scheme Using Smart Cards and Fingerprint Technology

Rafael Martínez-Peláez[1], Cristina Satizábal[2], Darío Barragán López[1], Edgar Aquino García[1], Oswaldo Ávila Barrón[1]

[1] Universidad de la Sierra Sur, Licenciatura en Informática, C/ Guillermo Rojas Mijangos S/N, Ciudad Universitaria, Miahuatlán de Porfirio Díaz, 70800, Oaxaca, México
{rpelaez, dbarragan, eaquino, oavila}@unsis.edu.mx
[2] Universidad de la Sierra Sur, División de Estudios de Postgrado, C/ Guillermo Rojas Mijangos S/N, Ciudad Universitaria, Miahuatlán de Porfirio Díaz, 70800, Oaxaca, México
isatizabal@unsis.edu.mx

Abstract. A remote user authentication scheme is a mechanism which identifies legal users and allows access to network services over an open network. However, several authentication schemes proposed in the literature cannot prove the user's physical participation during the login phase, making them vulnerable to different attacks. We propose a new remote user authentication scheme using nonce, smart cards and fingerprint technology for electronic activities. Our scheme provides mutual authentication and session key establishment between the user and the server. The server verifies the identity of the user by means of her fingerprint-template. In order to reduce security risks, the server does not maintain a verification table. The server computes a BioHash and stores it encrypted in user's smart card. Security analysis shows that our scheme provides strong security because the scheme resists common well-know attacks, making it suitable for practical implementation.

1 Introduction

A remote user authentication scheme allows two or more entities to establish a session key which can be used for creating a secure channel over an open network. A session key agreement protocol is used to establish the session key between two entities where each entity contributes with some information to derive that key. Moreover, a remote user authentication scheme permits to identify the legal from the illegal user.

In the literature, we can find several remote user authentication schemes [1-15]. Some of these schemes are based on smart cards [16], [17] and a few of them take advantage of biometrics [18], [19]. In this paper, we look at the remote user authentication schemes which combine smart cards and fingerprint biometric-based [19], [20].

Remote user authentication schemes based on password authentication require that a remote server maintains a verification table, making it vulnerable to steal information [4]. Also, an attacker can use social engineering attacks or brute force

© C. Delgado, C. Gutiérrez, R. Velázquez, H. Sossa (Eds.)
Advances in Computer Science and Electronic Systems
Research in Computing Science 52, 2011, pp. 107-113

Received 23/01/11
Accepted 20/02/11
Final version 07/03/11

attacks to obtain users' password. For that reasons, password authentication schemes are known as weak security mechanisms.

On the other hand, remote user authentication schemes based on public key cryptography [6], [9], [14] provide strong security in network communication, making them useful in several transactions. However, public key cryptography does not resolve the question Is really who claims to be?. Although public key cryptography offers significant security benefits, it does not resolve the question.

However, biometric technology can answer the previous question. For many years, fingerprint recognition has been used for identification and authentication [18], [19], [20]. The use of fingerprint recognition is justified by four reasons: 1) it is accepted as a valid method for personal identification; 2) the price of a fingerprint reader device is cheap; 3) the processing cost is low; and 4) it is easy to use; for those reasons, fingerprint is the most popular biometric technology around the world.

In 2002, Lee et al. [9] proposed a fingerprint-based remote user authentication scheme. However, Hsieh et al. [11] demonstrated that Lee et al.'s scheme is vulnerable to impersonate attacks.

In this paper, we take advantage of BioHash [21] to avoid storing the fingerprint-template in clear. In order to enhance the security of the proposed scheme, the BioHash is encrypted and the result is stored in user's smart card. Moreover, the scheme requires low-computational cost because user's smart card performs or-exclusive operations and one-way hash functions [22], [23] to create the session key.

The paper is organized as follows. We present the four phases of our scheme in section 2. Section 3 presents the security analysis of the proposed scheme. Finally, conclusions are given in section 4.

2 Proposed Scheme

Our scheme is based on low-computational cryptography which does not require high computational power but provides strong security. The notations used in this paper are described in Table 1.

Table 1. Notations

U	User
S	Server
T	Fingerprint-Template of *U*
ID	Identity of *U*
PW	Password of *U*
K_{pri}/K_{pub}	Private/public key of *U* or *S*
SK	Session key between *U* and *S*
Z	Secret key of *S*
Y	Secret value of *S*
$E_K(.)$	Encryption function using *K*
$D_K(E_K(.))$	Decryption function using *K*
H(.)	One-way hash function
||	Concatenate operator
$\oplus$	OR-exclusive operation

The proposed scheme contains four phases:

1. Registration phase, in where *U* will obtain the security parameters to be a legal member.
2. Login phase, in where *U* will be identified by her smart card and initialize the authentication process.
3. Mutual authentication and session key establishment phase, in where *S* will verify the identity of *U* and share common information to create *SK*.
4. Password change phase, in where *U* will have the possibility to change her *PW* without contact *S*.

2.1 Registration Phase

In this phase, *U* is registered by *S*. The process is as follows:

U shares her *ID* with *S* and imprints her fingerprint biometric impression at the sensor to obtain her template *T* which is extracted by the method described in [24]. Then, *S* performs the following operations:

```
Chooses randomly a PW
Computes $A = H(H(ID || PW) || Y)$
Computes $B = H(T)$
Computes $C = F(B, Z)$
Computes $G = E_{Kpub}(C)$
Computes $I = H(PW) \oplus A \oplus H(ID)$
Computes $J = H (A || H(ID || PW))$
```

S stores (*G*, *I*, *J*) in *U*'s smart card. Then, *S* delivers *U*'s smart card and *PW*, through a secure channel.

2.2 Login Phase

In this phase, *U* is identified by her smart card. *U* keys her *ID* and *PW*. Then, *U* carries out the following steps:

```
Computes $A' = H(PW) \oplus I \oplus H(ID)$
Computes $J' = H(A' || H(ID || PW))$
Verifies $J' ?= J$
Generates randomly N
Computes $L = A \oplus N$
Computes $M = H(H(ID || PW) || N)$
```

U sends (L, M, $H(ID \| PW)$) to *S*.

2.3 Mutual Authentication and Session Key Establishment Phase

In this phase, *S* verifies the identity of *U*. Moreover, *U* and *S* establish $SK_{U\text{-}S}$. The process is as follows:

```
Computes A′ = H(H(ID || PW) || Y)
Computes N′ = A′ $\oplus$ L
Computes M′ = H(H(ID || PW) || N)
Verifies M′ ?= M
```

If *M'* and *M* does not hold, *S* rejects it. Otherwise, *S* performs the following operations:

```
Computes $N_2$
Computes P = H(A || N)
Computes Q = P $\oplus$ $N_2$
Computes SK = H($N_2$ || N || A)
Computes R = $E_{SK}$(N+1, Request_hash_value_T)
```

S sends (*Q*, *R*) to *U*.

Upon receiving *Q* and *R*, *U* performs the following operations:

```
Computes P′ = H(A || N)
Computes $N_2$′ = P $\oplus$ Q
Computes SK = H($N_2$′ || N || A)
Computes N+1′
Computes $D_{SK}$($E_{SK}$(R)) = N+1, Request_hash_value_T
Verifies N+1′ ?= N+1
```

If *N+1'* and *N+1* does not hold, *U* rejects it. Otherwise, *U* imprints her fingerprint-biometric impression at the sensor and performs the following operations:

```
Computes H(T)
Computes V = $E_{SK}$(H(T), G)
```

U sends (*V*) to *S*.

Upon receiving *V*, *S* performs the following operations:

```
Computes $D_{SK}$($E_{SK}$(V))= H(T), G
Computes $D_{Kpriv}$($E_{Kpub}$(G)) = C
Computes C′ = F(H(T), Z)
Verifies C′ ?= C
```

If *C'* and *C* are equal, the identity of *U* is assured. Otherwise, *S* rejects *U*'s request.

2.4 Password Change Phase

Whenever *U* wants to change or update her *PW* for another one new, she must perform the following operations:

```
Computes $A' = H(PW) \oplus I \oplus H(ID)$
Computes $J' = H(A' || H(ID || PW))$
Verifies $J'$ ?= $J$
Request new password = $PW_{new}$
Computes $I_{new} = H(PW_{new}) \oplus A \oplus H(ID)$
Computes $J_{new} = H(A || H(ID || PW_{new}))$
```

Finally, the smart card stores I_{new} and J_{new} replacing the old *I* and *J*. Now, the new password is successfully updated.

3 Security Analysis

In this section, we prove that our proposed scheme is secure.

Lemma 1: The proposed scheme authenticates the source of the message.

Proof: In fact, $SK = H(N_2 \| N \| A)$ is known only by *U* and *S*. *S* is the unique entity who can compute $H(H(ID \| PW) \| Y)$ and *U* can recover *A* from *I* because she knows the correct *ID* and *PW*. Hence, *U* is sure that she and *S* share a session key *SK*. Even though an attacker can capture message *V*, she cannot recover $H(T)$ and *G* without know the correct key *SK*. Moreover, if an attacker can capture message *L*, she cannot recover *A* from *L* without know *N* and she cannot extract *N* without know *A*. In addition, if the attacker intercepts *M*, she cannot extract $H(ID \| PW)$ and *N* from *M* because is computationally infeasible invert a one-way hash function.

Lemma 2: The proposed scheme can resist impersonate attack.

Proof: Suppose that an attacker wants to impersonate *U*. Assuming that the attacker obtains *U*'s smart card and extracts *G*, *I* and *J* by means of [25], she cannot recover *A*, *PW* and *ID* using any type of combination of *G*, *I* and *J*.

Lemma 3: The proposed scheme can resist server spoofing attack.

Proof: If an attacker has the possibility to intercept messages *L*, *M* and $H(ID \| PW)$, she cannot compute *A* without know *Y*, she cannot extract *N* without have *A*, she cannot compute *P* without know *A* and *N*, and she cannot compute $SK = H(N_2 \| N \| A)$, giving as a result that she cannot compute a valid messages *Q* and *R*.

Lemma 4: The proposed scheme can resist user spoofing attack.

Proof: If an attacker has the possibility to intercept messages *Q* and *R*, she cannot compute *P* without know *A* and *N*, she cannot recover N_2 from *Q* without have *P* and she cannot computes *SK* for decrypting *R*.

Lemma 5: The proposed scheme protects *U*'s template.

Proof: In this scheme, *S* computes a one-way hash function over *U*'s template creating a BioHash. Moreover, *S* encrypts the BioHash using its public key K_{pub}.

Furthermore, S stores U's BioHash encrypted in U's smart card without store any type of information in a private/public database. If an attacker obtains $G = E_{Kpub}(H(T))$, she cannot recover $H(T)$ without know K_{priv}.

Lemma 6: The proposed scheme withstands leak of password attack.

Proof: In an attacker obtains U's smart card, she cannot recover U's *ID*, *PW* and T by using G, I and J or by any type of combination among them.

4 Conclusions

We have proposed a remote user authentication scheme, based on nonce, smart-cards and fingerprint technology, which does not require a verification table. The scheme is based on two key concepts: 1) ID-based, which is used to create the session key between the user and the server; and 2) fingerprint verification, which is used to verify the identity of the user. Thus, the scheme requires the three authentication categories – something she knows, something she has and something she is –, it can resist well-known attacks. Security analysis demonstrated that the proposed scheme is secure against impersonate, server spoofing, user spoofing, and leak of password attacks. Moreover, the scheme protects the user's template creating a BioHash. The scheme can be used in a system which requires high security, such as e-banking.

Acknowledgments

We would like to thank the reviewers for very constructive and detailed comments which contribute to improve the quality of the paper in the final version. We also would like to thank Universidad de la Sierra Sur for its support.

References

[1] Rivest R., Shamir A. and Adleman L., "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126, 1978.

[2] Shamir A., "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612-613, 1979.

[3] Lamport L., "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, pp. 770-772, 1981.

[4] Hwang T., Chen Y. and Laih C. S., "Non-interactive password authentication without password tables," presented at IEEE Region 10 Conference on Computer and Communication System, 1990.

[5] Chang C. C. and Wu T. C., "Remote password authentication with smart cards," *IEE Proceedings-E*, vol. 138, pp. 165-168, 1991.

[6] Hwang M. S. and Li L. H., "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, pp. 28-30, 2000.

[7] Chien H. Y., Jan J. K. and Tseng Y. M., "An Efficient and practical solution to remote authentication: smart card," *Computers & Security*, vol. 21, pp. 372-375, 2002.

[8] Lee C. C., Li L. H. and Hwang M. S., "A remote user authentication scheme using hash functions," *ACM SIGOPS Operating Systems Review*, vol. 36, pp. 23-29, 2002.

[9] Lee J. K., Ryu S. R. and Yoo K. Y., "Fingerprint-based remote user authentication scheme using smart cards," *IEE Electronic Letters*, vol. 38, pp. 554-555, 2002.

[10] Lin C. W., Shen J. J. and Hwang M. S., "Security enhancement for optimal strong-password authentication protocol," *Operating Systems Review*, vol. 37, pp. 12-16, 2003.

[11] Hsieh B. T., Yeh H. T., Sun H. M., and Lin C. T., "Cryptanalysis of a fingerprint-based remote user authentication scheme using smart cards," presented at IEEE 37th International Carnahan Conference on Security Technology, 2003.

[12] Carlisle A. and Lloyd S., *Understanding PKI: concepts, standards, and deployment considerations*, 2nd ed: Addison-Wesley, Cop., November, 2003.

[13] Das M. L., Saxena A. and Gulati V. P., "A Dynamic ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, pp. 629-631, 2004.

[14] Badra M. and Urien P., "Introducing smart cards to remote authenticate passwords using Public Key Encryption," presented at IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication, 2004.

[15] Martínez-Peláez R., Rico-Novella F., Satizabal C., and Pomykala J., "Strong remote user authentication scheme using smart cards," presented at Eighth International Network Conference, 2010.

[16] Vedder K. and Weikmann F., "Smart cards - requirements, properties, and applications," in *State of the Art in Applied Cryptography, Course on Computer Security and Industrial Cryptography*, vol. LNCS 1528, 1998, pp. 307-331.

[17] Trask N. T. and Meyerstein M. V., "Smart Cards in Electronic Commerce," *BT Technology Journal*, vol. 17, pp. 57-66, 1999.

[18] Pankanti S., Bolle R. M. and Jain A., "Biometrics: the future of identification," *Computer*, vol. 33, pp. 46-49, 2000.

[19] Jain A. K., Ross A. and Prabhakar S., "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, pp. 4- 20, 2004.

[20] Putte T. V. and Keuning J., "Biometrical fingerprint recognition: don't get your fingers burned," presented at IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, 2000.

[21] Jain A. K., Nandakumar K. and Nagar A., "Biometric Template Security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, pp. 1 - 20, 2008.

[22] Rivest R., "RFC 1321 - the MD5 message-disgest algorithm," IETF Working Group 1992.

[23] NIST, "Secure Hash Standard (SHA), FIPS PUB 180-1," National Institute of Standards and Technology 1995.

[24] Bae I. G. and al. e., "Online fingerprint verification system using direct minutia extraction," presented at International Conference on Computer Applications in Industry and Engineering, 2000.

[25] Messerges T. S., Dabbish E. A. and Sloan R. H., "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, pp. 541-552, 2002.