Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Technology 3 (2012) 351 – 353

Procedia Technology

The 2012 Iberoamerican Conference on Electronics Engineering and Computer Science

Weaknesses of an efficient and secure dynamic ID-based remote user authentication scheme

Rafael Martínez-Peláez[a,*], Francisco Rico-Novella[b]

[a]*Universidad de la Sierra Sur, Calle Guillermo Rojas Mijangos S/N, Esq. Av. Universidad Col. Ciudad Universitaria, Miahuatlán de Porfirio Díaz, México*
[b]*Technical University of Catalonia, Department of Telematics Engineering, Jordi Girona 1-3 C3, 08034 Barcelona, Spain*

Abstract

Recently, Wang, Liu, Xiao and Dan proposed an efficient and secure dynamic ID-based remote user authentication scheme and claimed that their scheme provides strong security. We demonstrate that Wang et al.'s scheme is vulnerable to insider, masquerade and server spoofing attacks.

Keywords: authentication; low-cost cryptography; secure communication; smart cards

1. Introduction

In 1991, Chang and Wu [1] proposed a remote user authentication scheme using smart cards. Since 1991 several remote user authentication schemes using smart cards have been proposed [2-8] to enhance the security and reduce the computational cost, and provide services to electronic activities.

In 2002, Chien et al. proposed a remote user authentication scheme [2]. The merits of Chien et al.'s scheme are: the scheme requires low-computational and low-communication cost, and provide mutual authentication. Although, the scheme does not maintain a verification table, the server must maintain a table to store the users' *ID* to check its validity. However, Hsu demonstrated that Chien et al.'s scheme is vulnerable to parallel session attack [9]. Das et al. proposed a dynamic ID-based remote user authentication scheme using smart cards [5]. They introduced the concept of dynamic ID-based which prevents that an attacker can know the user's *ID*. However, the scheme is susceptible to insider, masquerade, and server spoofing attacks [7].

In 2009, Wang et al. [7] presented an authentication scheme to provide mutual authentication between a user and a remote server, and resolves the security flaws of Das et al. scheme.

In this paper, we demonstrate that Wang et al.'s scheme is vulnerable to insider, masquerade, and server spoofing attacks.

The rest of this paper is organized as follows. In Section 2, we give a brief review on Wang et al.'s scheme. We demonstrate the vulnerabilities of Wang et al.'s scheme, in Section 3. Finally, we conclude this paper in Section 4.

2. Wang et al.'s scheme

Wang et al. [7] proposed a dynamic ID-based remote user authentication scheme in which the remote server does not maintain a verification table and chooses the user's password. Moreover, the scheme establishes a mutual authentication. The scheme consists of four phases – registration, login, verification, and password change. We explain the registration, login, and verification phases, because we will use it to carry out the security analysis. Table 1 describes the notations used in this paper.

* Corresponding author. Tel.: +01-951-57-2-41-00 (ext. 205); fax: +01-951-57-2-41-00.
E-mail address: rpelaez@unsis.edu.mx.

2212-0173
doi:10.1016/j.protcy.2012.03.038

Table 1. Notations

Notation	Meaning
U	The user
S	The server
ID	Unique identity of U
PW	Unique password of U
$h(\cdot)$	A one-way hash function
$SK(\cdot)$	A symmetric encryption function
x, y	Secret keys of S
$\oplus$	Exclusive-or operation
$\|\|$	String concatenation operation

2.1. Registration phase

When U wants to access the resources of S, she submits her ID to S, through a secure channel. Then, S performs the following operations:

1. Chooses PW.
2. Computes $A = h(PW) \oplus h(x) \oplus ID$, where PW is chosen by S.
3. Sends $(PW, A, y, h(\cdot))$ to U, through a secure channel.

Note that U's smart card contains A, y, and $h(\cdot)$.

2.2. Login phase

The user U keys her ID and PW. Then, the smart card performs the following operations:

1. Computes CID = h(PW) ⊕ h(A ⊕ y ⊕ T) ⊕ ID, where T is the current date and time of Ui's device.
2. Sends the login request message (ID, CID, A, T) to S.

2.3. Verification phase

Upon receiving the login request message, S verifies the time interval between T and T^*, where T^* is the arrival time of the message. If the time interval is correct, S performs the following operations:

1. Computes $h(PW)^* = CID \oplus h(A \oplus y \oplus T) \oplus ID$ and $ID^* = h(PW)^* \oplus h(x) \oplus A$.

Then, S checks whether or not ID^* is equal to ID. If the verification fails, S rejects the request; otherwise, S confirms the identity of U and performs the following operations:

2. Computes $B = h(h(PW)^* \oplus y \oplus T_2)$.
3. Sends (B, T_2) to U.

Upon receiving the acknowledgement message (B, T_2), U checks the validity of the timestamp T_2 and performs the following operation:

4. Computes $B^* = h(h(PW_i) \oplus y \oplus T_2)$.

Then, U checks whether or not B^* is equal to B. If it holds, U confirms the identity of S.

3. Cryptanalysis of Wang et al.'s scheme

In this section, we demonstrate that Wang et al.'s scheme is vulnerable to insider, masquerade, and server spoofing attacks.

3.1. Insider attack

We demonstrate that Wang et al.'s scheme cannot resistance the insider attack. The attacker can create a valid login request message, if she obtains A, $h(x)$, and y. The process to obtain these parameters is as follows:

If the attacker is a legal user U, she can extract $h(x)$ from A computing $h(x) = h(PW) \oplus A \oplus ID$, and she knows y.

If the attacker has intercepted a previous login request message (ID, CID, A, T), she knows ID, and A.

Then, the attacker can impersonate U as follows:

1. Chooses a random password PW_{false} and computes $h(PW_{false})$.
2. Computes $A_{false} = h(PW_{false}) \oplus h(x) \oplus ID$.
3. Computes $CID_{false} = h(PW_{false}) \oplus h(A_{false} \oplus y \oplus T_1) \oplus ID$, where T_1 is the current date and time of attacker's device
4. Sends the imitative login request message (ID, CID_{false}, A_{false}, T_1) to S.

Upon receiving the imitative login request message (ID, CID_{false}, A_{false}, T_1) and checking the validity of the time interval, S will compute $h(PW_{false})^* = CID_{false} \oplus h(A_{false} \oplus y \oplus T_1) \oplus ID$ and $ID^* = CID_{false} \oplus h(A_{false} \oplus y \oplus T_1) \oplus h(PW_{false})^*$. Then, S will check whether ID^* is equal to ID. In this case, S will accept the attacker's login request message because ID^* is equal to ID.

3.2. Masquerade attack

We demonstrate that Wang et al.'s scheme is vulnerable to masquerade attack. The attacker can masquerade as legal user U creating a valid login request message. If the attacker is a legal user U, she knows y. Then, if she has intercepted a previous U's login request message (ID, CID, A, T), she can masquerade as a legal user U as follows:

1. Computes $h(A \oplus y \oplus T)^*$.
2. Extracts $h(PW)$ from CID computing $h(PW)^* = CID \oplus h(A \oplus y \oplus T)^* \oplus ID$.
3. Computes $CID_{false} = h(PW)^* \oplus h(A \oplus y \oplus T_1)^* \oplus I_i$, where T_1 is the current date and time of attacker's device.
4. Sends the imitative login request message (ID, CID_{false}, A, T_1) to S.

Upon receiving the imitative login request message (ID, CID_{false}, A, T_1) and checking the validity of the time interval, S will compute $h(PW)^* = CID_{false} \oplus h(A \oplus y \oplus T_1) \oplus ID$ and $ID^* = CID_{false} \oplus h(A \oplus y \oplus T_1) \oplus h(PW)^*$. Then, S will check whether or not ID^* is equal to ID. In this case, S will accept the attacker's login request message because ID^* is equal to ID.

3.3. Server spoofing attack

We prove that Wang et al.'s scheme is vulnerable to server spoofing attack. In this scheme, S needs to know y and $h(x)$ for verifying the legitimacy of each user. If the attacker is a legal user U, she can impersonate as S to cheat U because she knows y and $h(x)$. After the user U receives the acknowledgement message (B_{falase}, T_2), she will compute $B^* = h(h(PW_i) \oplus y \oplus T_2)$ and checks whether or not B^* is equal to B_{false}. In this case, U will believe that the attacker is the legal S.

4. Conclusion and Future Work

Wang et al.'s scheme was proposed for resolving security issues presented in previous work. However, we have discovered some security flaws in the Wang et al.'s scheme making it vulnerable to server spoofing, masquerade, and insider attacks. Moreover, the scheme fails to establish a session key between the user and the server for posterior communication.

We are working in the design and evaluation of a new dynamic ID-based remote user authentication scheme which provides strong security.

References

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

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

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

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

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

[6] W. C. Ku and S. M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, pp. 204-207, 2004.

[7] Y. Y. Wang, J. Y. Liu, F. X. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," *Computer Communications*, vol. 32, pp. 583-585, 2009.

[8] B. Wang and Z. Q. Li, "A forward-secure user authentication scheme with smart cards," *International Journal of Network Security*, vol. 3, pp. 116-119, 2006.

[9] C. L. Hsu, "Security of two remote user authentication schemes using smart cards," *IEEE Transaction on Consumer Electronics*, vol. 49, pp. 1196-1198, 2003.

[10] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology - Crypto'99*, vol. LNCS 1666, 1999, pp. 388-397.

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