International Journal of Security and Its Applications
Vol. 10, No. 2 (2016), pp.163-170
http://dx.doi.org/10.14257/ijsia.2016.10.2.15

Cryptanalysis of a Biometric-based Multi-Server Authentication Scheme

Tao Wan[1, *], Nan Jiang[2], Jianfeng Ma[1], Lin Yang[3]

[1]School of Computer Science and technology, Xidian University, Xi'an 710071, China
[2]School of Information Engineer, East China Jiaotong University, Nanchang 330013, China
[3]The Research Institute, China Electronic Equipment and Systems Engineering Corporation, Beijing 100039, China
[1]wantao217@163.com, [2]jiangnan1018@gmail.com

Abstract

Authentication and key agreement protocol becomes an important security issue for multi-server architecture. Combining biometrics with password enhances the level of security. Recently, Baruah et al. analyzed that Mishra et al.'s protocol has several drawbacks and proposed an improved biometric based multi-server authentication scheme. They claimed that their scheme satisfies all the required security attributes for a secure authentication. In this paper, we indicate that their scheme is not secure against key reveal attack, replay attack, and smart card forgery attack. Any registered user can retrieve the session key or launch the replay attack by eavesdropping on the communication channel. In addition, registered user can forge smart card when colluding with registered server.

***Keywords**: Authentication, Multi-server, Biometric, Smart card*

1. Introduction

With the rapid development of Internet service, remote user authentication scheme becomes an important issue for practical applications. More and more network architectures are used in multi-server environments. However, it is extremely hard for a user to remember these numerous different identities and passwords when he/she uses the single-server authentication protocol to login and access different remote service providing servers. In order to resolve this problem, many multi-server authentication and key agreement schemes have been proposed.

In 2001, Li *et al*. [1] first proposed the concept of multi-server authentication protocol. But their scheme need large memory and high computational cost. In 2004, Tsaur *et al*. [2] designed a multi-server authentication scheme based on the RSA cryptosystem and Lagrange interpolating polynomial. But their scheme is subject to high communication and computation costs. In 2008, Tsai [3] proposed a multi-server authentication scheme based on the nonce and one-way hash function. [1] However, his scheme was found susceptible to the server spoofing and the impersonation attacks [4]. In 2008, Lee *et al*. [5] proposed an efficient remote authenticated key agreement scheme for multi-server by adopting hash function and exclusive-OR. Nevertheless, Chang *et al*. [6] indicated that their scheme is vulnerable to the forgery attack. In 2009, Liao and Wang [7] designed a dynamic identity based remote user authentication protocol for multi-server environment to achieve user's anonymity. However, this scheme was found to be vulnerable to insider attack, masquerade attack, server spoofing attack, and registration center spoofing attack

Tao Wan is the corresponding author.

ISSN: 1738-9976 IJSIA

by Hsiang and Shih [8]. Wan *et al*. [9] analyzed that two dynamic ID based remote user authentication schemes for multi-server environment proposed by Lee *et al*. [10] and Li *et al*. [11] were susceptible to stolen smart card attack, leak-of-verifier attack and so on.

More recently, many researches have combined user's biometrics (e.g., fingerprints, irises, and hand geometry) with password and smart card to design remote user authentication scheme to enhance the level of security. The main feature of using biometric is its uniqueness. Yang *et al*. [12] and Yoon *et al*. [13] proposed biometric based multi-server authentication schemes, but they did not consider the user anonymity. Moreover, Yang *et al*.'s scheme need high computational cost, and Yoon *et al*.'s scheme was found by He [14] to be vulnerable to insider attack, masquerade attack, and stolen smart card attack.

Recently, Chuang *et al.* [15] introduced an anonymous biometric based multi-server authentication scheme. But Mishra *et al.* [16] demonstrated their scheme was vulnerable to stolen smart card attack, impersonation attack and server spoofing attack, and proposed an improved multi-server authentication scheme. However, Baruah *et al.* [17] found that their scheme still cannot withstand stolen smart card attack and impersonation attack, and then proposed an enhanced authentication scheme. They declaimed their scheme satisfies all the required security attributes. Unfortunately, we identify that Baruah *et al.*'s scheme is susceptible to key reveal attack, replay attack and smart card forgery attack.

The remainder of this manuscript is organized as follows. We review the biometric based multi-server authentication protocol proposed by Baruah *et al.* in Section 2. We analyze the security flaws of Baruah *et al.*'s protocol in Section 3. We conclude this paper in Section 4.

2. Review of Baruah *et al.*'s Scheme

Here we will review Baruah *et al.*'s biometric based multi-server authentication scheme. The notations used throughout this paper are summarized in Table 1.

Table 1. Notations used in the paper

Symbols	Their meaning
RC	the registration center
U_i	the i_{th} user
ID_i	the identity of U_i
PW_i	the password of U_i
BIO_i	the biometric of U_i
PSK	Pre-shared key
S_j	the j_{th} server
SID_j	the identity of S_j
x	the master secret key of RC
$h(\cdot)$	a secure one way hash function
$\oplus$	Exclusive-OR operation
$\|$	string concatenation operation

Their scheme involves three participants, the user U_i, the server S_j and the registration center RC. Their scheme can be divided into five phases: server registration phase, user registration phase, login phase, authentication phase and password change phase. We show the login and authentication phases in Figure 1. More details are provided in the following.

2.1. Server Registration Phase

An application server S_j sends a registration request along with its identity SID_j to the registration center RC, if he wishes to become a registered server. Then the registration center RC chooses the master key x and the pre-shared key PSK to compute

$h(SID_j||h(PSK))$ and $h(PSK||x)$, then sends them to the application server S_j using the Internet Key Exchange Protocol (IKEv2) [18].

2.2. User Registration Phase

When a new user U_i wishes to access any services provided by the registered servers, he must first register himself. This registration phase consists of the following steps:

*Step R*1: The user U_i freely chooses his identity ID_i, password PW_i and personal biometric BIO_i, and computes $R_i = h(PW_i||BIO_i)$. Then U_i sends ID_i and R_i to RC over a secure channel.

*Step R*2: RC computes $A_i = h(ID_i||x)$, $B_i = h(PSK||x)\oplus A_i$, $C_i = h(R_i||ID_i)\oplus h(A_i)$, $D_i = h(PSK)\oplus h(ID_i)$, $E_i = R_i\oplus ID_i$, and securely issues the smart card containing $\{B_i, C_i, D_i, E_i, h(\cdot)\}$ to the user U_i.

2.3. Login Phase

*Step L*1: U_i inserts his smart card and inputs his identity ID_i, password PW_i and personal biometric BIO_i. The smart card computes $R_i = h(PW_i||BIO_i)$, and checks whether the entered identity ID_i is equal to $E_i\oplus R_i$. If it holds, the legitimacy of U_i can be assured.

*Step L*2: The smart card computes $h(PSK) = h(ID_i)\oplus D_i$ and $h(A_i) = C_i\oplus h(R_i||ID_i)$, then generates a nonce N_i, and computes $M_1 = h(SID_j||h(PSK))\oplus h(ID_i||N_i)$, $M_2 = N_i\oplus h(A_i)$, $V_1 = h(N_i\oplus B_i)$.

Afterwards, the smart card sends the login request massage $\{B_i, M_1, M_2, V_1\}$ to the server S_j via a public channel.

U_i		S_j
Input ID_i, PW_i, BIO_i		
$R_i = h(PW_i \| BIO_i)$		
Check $ID_i ?= E_i \oplus R_i$		
$h(PSK) = D_i \oplus h(ID_i)$		
$h(A_i) = C_i \oplus h(R_i \| ID_i)$		
Gen N_i		
$M_1 = h(SID_j \| h(PSK)) \oplus h(ID_i \| N_i)$		
$M_2 = N_i \oplus h(A_i)$		
$V_1 = h(N_i \oplus B_i)$	$\{B_i, M_1, M_2, V_1\}$ →	$A_i = B_i \oplus h(PSK \| x)$
		$h(ID_i \| N_i) = M_1 \oplus h(SID_j \| h(PSK))$
		$N_i = M_2 \oplus h(A_i)$
		Check $V_1 ?= h(N_i \oplus B_i)$
		Gen N_j
		$SK_{ij} = h(h(ID_i \| N_i) \| SID_j \| B_i \| N_j)$
		$M_3 = N_j \oplus h(ID_i \| N_i)$
	← $\{M_3, V_2\}$	$V_2 = N_i \oplus h(SK_{ij} \| N_j)$
$N_j = M_3 \oplus h(ID_i \| N_i)$		
Check $N_i ?= V_2 \oplus h(SK_{ij} \| N_j)$		
$SK_{ij} = h(h(ID_i \| N_i) \| SID_j \| B_i \| N_j)$		

Figure 1. Login and Authentication Phase of Baruah *et al*.'s Scheme

2.4. Authentication Phase

*Step V*1: Once S_j receives the login request massage $\{B_i, M_1, M_2, V_1\}$, S_j computes $A_i = B_i\oplus h(PSK||x)$, $h(ID_i||N_i) = M_1\oplus h(SID_j||h(PSK))$, $N_i = M_2\oplus h(A_i)$.

*Step V*2: S_j computes $h(N_i \oplus B_i)$ and checks it with V_1. If they are equivalent, S_j accepts the login request. Then S_j generates a nonce N_j to compute $SK_{ij} = h(h(ID_i||N_i)||SID_j||B_i||N_j)$, $M_3 = N_j \oplus h(ID_i||N_i)$, $V_2 = N_i \oplus h(SK_{ji}||N_j)$. Finally, S_j sends the message $\{M_3, V_2\}$ to U_i.

*Step V*3: Upon receiving the message $\{M_3, V_2\}$, U_i computes $N_j = M_3 \oplus h(ID_i||N_i)$, $SK_{ij} = h(h(ID_i||N_i)||SID_j||B_i||N_j)$, and compares N_i with $V_2 \oplus h(SK_{ji}||N_j)$. If they are equivalent, U_i authenticates S_j.

After the mutual authentication, U_i and S_j can use the current session key $SK_{ij} = h(h(ID_i||N_i)||SID_j||B_i||N_j)$ for securing communication.

2.5. Password Change Phase

This phase is invoked whenever U_i wants to change his password PW_i to a new password PW_i^*.

*Step P*1: U_i inserts his smart card and inputs his identity ID_i, password PW_i and personal biometric BIO_i.

*Step P*2: The smart card computes $R_i = h(PW_i||BIO_i)$, and checks whether the entered identity ID_i is equal to $E_i \oplus R_i$. If it holds, U_i chooses a new password PW_i^* to compute $R_i^* = h(PW_i^*||BIO_i)$, $C_i^* = h(R_i^*||ID_i) \oplus h(R_i||ID_i) \oplus C_i$, and $E_i^* = E_i \oplus R_i \oplus R_i^*$.

*Step P*3: The smart card stores C_i^*, E_i^* to replace C_i, E_i respectively.

3. Security Analysis of Baruah *et al.*'s scheme

In Baruah *et al*.'s scheme, every servers has different secret information $h(SID_j || PSK)$, so their scheme can successful thwart server masquerading attack. Unfortunately, we find that their scheme still has many vulnerabilities. Any registered but malicious user can not only derive the session key between any user and server by eavesdropping their communication information in public channel, but also masquerade as the user to log into the server. In addition, when a registered but malicious user colludes with a server, they can successful log into any server by forging smart card.

3.1. Key Reveal Attack

From the login phase of Baruah *et al*.'s scheme, we find that each registered user knows $h(PSK)$. If a legal but malicious user U_z can eavesdrop the valid login request message $\{B_i, M_1, M_2, V_1\}$ of U_i and the authentication message $\{M_3, V_2\}$ of S_j on the public channel, he can compute $h(ID_i \,||\, N_i) = M_1 \oplus h(SID_j \,||\, h(PSK))$, $N_j = M_3 \oplus h(ID_i \,||\, N_i)$, and $SK_{ij} = h(h(ID_i \,||\, N_i) \,||\, SID_j \,||\, B_i \,||\, N_j)$. Then U_z easily derive the current session key SK_{ij} shared between U_i and S_j. After that, the attacker U_z can decrypt all encrypted information between U_i and S_j.

3.2. Replay Attack

From the above analysis, we know that any legal user U_z can retrieve $h(ID_i \,||\, N_i)$ by eavesdropping the login request message $\{B_i, M_1, M_2, V_1\}$ of U_i. Then U_z can also replay the message $\{B_i, M_1, M_2, V_1\}$ to S_j. This verification holds, since the messages has not been modified. Then S_j selects a nonce N_j', generates the session key as $SK_{ij}' = h(h(ID_i \,||\, N_i) \,||\, SID_j \,||\, B_i \,||\, N_j')$, and computes the authentication messages $M_3' = N_j' \oplus h(ID_i \,||\, N_i)$, $V_2' = N_i \oplus h(SK_{ij}' \,||\, N_j')$. Using the received authentication message $\{M_3', V_2'\}$, U_z can compute $N_j' = M_3' \oplus h(ID_i \,||\, N_i)$ and $SK_{ij}' = h(h(ID_i \,||\, N_i) \,||\, SID_j \,||\, B_i \,||\, N_j')$.

At last, the legal but malicious user U_z successful masquerade as U_i to log into the server S_j.

3.3. Smart card Forgery Attack

As shown in Baruah *et al.*'s scheme, any registered server has the same

U_z		S_j
Forge ID_A, PW_A, BIO_A, x'		
$R_A = h(PW_A \| BIO_A)$		
$A_A = h(ID_A \| x')$		
$B_A = h(PSK \| x) \oplus A_A$		
$C_A = h(R_A \| ID_A) \oplus h(A_A)$		
$D_A = h(PSK) \oplus h(ID_A)$		
$E_A = R_A \oplus ID_A$		
The smart card containing $\{B_A, C_A, D_A, E_A, h(\cdot)\}$		
Input ID_A, PW_A, BIO_A		
Check $ID_A ?= E_A \oplus R_A$		
$h(PSK) = D_A \oplus h(ID_A)$		
$h(A_A) = C_A \oplus h(R_A \| ID_A)$		
Gen N_A		
$M_1' = h(SID_j \| h(PSK)) \oplus h(ID_A \| N_A)$		
$M_2' = N_A \oplus h(A_A)$		
$V_1' = h(N_A \oplus B_A)$	$\{B_A, M_1', M_2', V_1'\}$ $\longrightarrow$	$A_A = B_A \oplus h(PSK \| x)$
		$h(ID_A \| N_A) = M_1' \oplus h(SID_j \| h(PSK))$
		$N_A = M_2' \oplus h(A_A)$
		Check $V_1' ?= h(N_A \oplus B_A)$
		Gen N_j'
		$SK_{Aj} = h(h(ID_A \| N_A) \| SID_j \| B_A \| N_j')$
		$M_3' = N_j' \oplus h(ID_A \| N_A)$
$N_j' = M_3' \oplus h(ID_A \| N_A)$	$\longleftarrow$ $\{M_3', V_2'\}$	$V_2' = N_A \oplus h(SK_{Aj} \| N_j')$
Check $N_A ?= V_2' \oplus h(SK_{Aj} \| N_j')$		
$SK_{Aj} = h(h(ID_A \| N_A) \| SID_j \| B_A \| N_j')$		

Figure 2. Smart Card Forgery Attack on Baruah *et al.*'s Scheme

Information $h(PSK \| x)$ and any registered user can derive the information $h(PSK)$. Under the condition that the registered but malicious user U_z colludes with the registered but malicious S_k, they can forge a smart card to log in to any registered server (e.g., S_j) without knowing the personal biometric as show in Figure 2. The procedure is as follow:

- forge a new identity ID_A, password PW_A and personal biometric BIO_A, and forge a master key x'.
- compute $R_A = h(PW_A \| BIO_A)$, $A_A = h(ID_A \| x')$, $B_A = h(PSK \| x) \oplus A_A$, $C_A = h(R_A \| ID_A) \oplus h(A_A)$, $D_A = h(PSK) \oplus h(ID_A)$, $E_A = R_A \oplus ID_A$, then the forged smart card containing $\{B_A, C_A, D_A, E_A, h(\cdot)\}$.
- insert the forged smart card and input identity ID_A, password PW_A and personal biometric BIO_A. Obviously the legitimacy of user can be assured.
- the forged smart card computes $h(PSK) = h(ID_A) \oplus D_A$ and $h(A_A) = C_A \oplus h(R_A \| ID_A)$, then generates a nonce N_A, and computes $M_1' = h(SID_j \| h(PSK)) \oplus h(ID_A \| N_A)$, M_2'

$= N_A \oplus h(A_A)$, $V_1' = h(N_A \oplus B_A)$. Then, the forged smart card sends the login request massage $\{B_A, M_1', M_2', V_1'\}$ to the server S_j via a public channel.

Upon receiving the message $\{B_A, M_1', M_2', V_1'\}$, S_j computes $A_A = h(PSK \| x) \oplus B_A$, $h(ID_A \| N_A) = M_1' \oplus h(SID_j \| h(PSK))$, $N_A = M_2' \oplus h(A_A)$, and compares $h(N_A \oplus B_A)$ with V_1'. Because they are equivalent, S_j will accept the login request.

Then S_j generates a nonce N_j' to compute $SK_{Aj} = h(h(ID_A \| N_A) \| SID_j \| B_A \| N_j')$, $M_3' = N_j' \oplus h(ID_A \| N_A)$, $V_2' = N_A \oplus h(SK_{Aj} \| N_j')$. Finally, S_j sends the message $\{M_3', V_2'\}$ to U_z.

When receiving the message $\{M_3', V_2'\}$, U_z computes $N_j' = M_3' \oplus h(ID_A \| N_A)$, $SK_{Aj} = h(h(ID_A \| N_A) \| SID_j \| B_A \| N_j')$, and compares N_A with $V_2' \oplus h(SK_{Aj} \| N_j')$.

At last, the attacker U_z logs in to the server S_j using the forged smart card. Therefore, Baruah *et al.*'s scheme cannot withstand smart card forgery attack.

4. Conclusions

Secure communication without repeating registration and biometrics based authentication are two important issues over multi-server environments. In this paper, we analyzed Baruah *et al.*'s biometric-based multi-server authentication scheme. Our analysis reveals its inherent security vulnerabilities, *i.e.*, key reveal attack, replay attack and smart card forgery attack. In the future, we plan to propose an improved version of their scheme and these security weaknesses should be considered for multi-server networks.

Acknowledgments

The author would like to thank Prof. Jianfeng Ma and the anonymous referees for their constructive comments. This research was supported by the Key Program of NSFC-Guangdong Union Foundation under Grant No.U1135002.

References

[1] L.H. Li, I.C. Lin, M.S. Hwang, “A remote password authentication scheme for multi-server architecture using neural networks”, Neural Networks, IEEE Transactions on, vol. 12, no. 6, **(2001)**, pp. 1498-1504.

[2] W.J. Tsaur, C.C. Wu, W.B. Lee, “A smart card-based remote scheme for password authentication in multi-server Internet services”, Computer Standard & Interfaces, vol. 27, no. 1, **(2004)**, pp. 39-51.

[3] J.L. Tsai, “Efficient multi-server authentication scheme based on one-way hash function without verification table”, Computers & Security, vol. 27, no. 3, **(2008)**, pp. 115-121.

[4] R.C. Wang, W.S. Juang, C.L. Lei, “User authentication scheme with privacy-preservation for multi-server environment”, Communications Letters, IEEE, vol. 13, no. 2, **(2009)**, pp. 157-159.

[5] J.H. Lee, D.H. Lee, “Efficient and secure remote authenticated key agreement scheme for multi-server using mobile equipment”, Consumer Electronics, 2008. ICCE 2008. Digest of Technical Papers. International Conference on. IEEE, **(2008)** January 1-2.

[6] C.C. Chang, T.F. Cheng, “A robust and efficient smart card based remote login mechanism for multi-server architecture”, Int. J. Innov. Comput. Inf. Control, vol. 7, no. 8, **(2011)**, pp. 4589-4602.

[7] Y.P. Liao, S.S. Wang, “A secure dynamic ID based remote user authentication scheme for multi-server environment”, Computer Standards & Interfaces, vol. 31, no. 1, **(2009)**, pp. 24-29.

[8] H.C. Hsiang, W.K. Shih, “Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment”, Computer Standards & Interfaces, vol. 31, no. 6, **(2009)**, pp. 1118-1123.

[9] T. Wan, N. Jiang, J.F. Ma, “Cryptanalysis of two dynamic identity based authentication schemes for multi-server architecture”, Communications, China, vol. 11, no.11, **(2014)**, pp. 125-134.

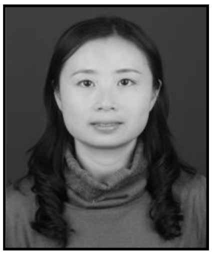
[10] C.C. Lee, T.H. Lin, R.X Chang, “A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards”, Expert Systems with Applications, vol. 38, no.11, **(2011)**, pp. 13863-13870.

[11] X. Li, J. Ma, W. Wang, Y. Xiong, J. Zhang, “A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments”, Mathematical and Computer Modelling, vol. 58, no.1, **(2013)**, pp. 85-95.

[12] D. Yang, B. Yang, “A biometric password-based multi-server authentication scheme with smart card”, Computer Design and Applications (ICCDA), 2010 International Conference on. IEEE, vol. 5, **(2010)**, pp. 554 -559.

[13] E.J. Yoon, K.Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem", The Journal of Supercomputing, vol. 63, no.1, **(2013)**, pp. 235-255.
[14] D. He, "Security flaws in a biometrics-based multi-server authentication with key agreement scheme", IACR Cryptology ePrint Archive, **(2011)**, pp. 365.
[15] M.C. Chuang, M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics", Expert Systems with Applications, vol. 41, no.4, **(2014)**, pp. 1411-1418.
[16] D. Mishra, A.K. Das, S. Mukhopadhyay, "A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards", Expert Systems with Applications, vol. 41, no.18, **(2014)**, pp. 8129-8143.
[17] K.C. Baruah, S. Banerjee, M.P. Dutta, C.T. Bhunia, "An Improved Biometric-based Multi-server Authentication Scheme Using Smart Card", International Journal of Security and Its Applications, vol. 9, no.1, **(2015)**, pp. 397-408.
[18] C. Kaufman, Internet key exchange (IKEv2) protocol, (2005)

Authors



Tao Wan, She received the B.S. degree in Mathematics from Hunan University, Changsha, China in 1997, and obtained the M.S. degree in Computer Science from Xidian University, China 2003. She is currently a Ph.D. candidate at Xidian University, Xi'an, Shaanxi, China. Her research interests include cryptography, network and information security, e-commerce security technology.

Nan Jiang, He received his Ph.D. degree in Computer Application Technology from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2008. Now he is an associate professor at East China Jiaotong University. From 2013 to 2014 he is a research scholar in Complex Networks and Security Research Lab at Virginia Tech. His research interests lie in wireless sensor networks, wireless protocol and architecture, distributed computing and complex network theory.

Jianfeng Ma, He received his M.S. and Ph.D. degrees in Computer Software and Communications Engineering from Xidian University, China in 1988 and 1995, respectively. He is an IEEE member and a senior member of CIE. Now he is a Professor and Ph.D. supervisor at Xidian University. His current research interests include distributed systems, wireless and mobile computing systems, computer networks, and information and network security.

Lin Yang, He received the B.E., M.E. and Ph.D. degrees from National University of Defense Technology of China in 1993, 1996 and 1998 respectively. He is a researcher in the Research Institute, China Electronic Equipment and Systems and doctorial supervisor of Xidian University and National University of Defense Technology. His research interests include system security and network security.