Cryptanalysis of Biometric-based Multi-server Authentication Scheme Using Smart Card

Jongho Mun, Jiye Kim, Donghoon Lee and Dongho Won*
College of Information and Communication Engineering
Sungkyunkwan University
2066 Seobu-ro, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Korea
{jhmoon, jykim, dhlee, dhwon}@security.re.kr

***Abstract*—Remote user authentication scheme is one of the most convenient authentication schemes to deal with secret data via insecure communication channel. During the last couple of decades, many researchers have proposed a remote user authentication schemes which are ID-based, password-based, and smart card-based. Above all, smart card-based remote user authentication schemes for multi-server environment are a widely used and researched method. One of the benefits of smart card-based authentication scheme is that a server does not have to keep a verifier table. Furthermore, remote user authentication scheme for multi-server environment has resolved the problem of users to manage the different identities and passwords. In 2015, Baruah et al. improved Mishra et al.'s scheme, and claimed that their scheme is more secure and practical remote user authentication scheme. However, we find that Baruah et al.'s scheme is still insecure. In this paper, we demonstrate that their scheme is vulnerable to outsider attack, smart card stolen attack, user impersonation attack and replay attack.**

Keywords*—*Remote User Authentication, Biometric, Smart card, Network Security

I. INTRODUCTION

Since Lamport [1] proposed the first password-based authentication scheme via insecure communication in 1981, password-based authentication schemes [2]-[8] have been extensively investigated. However, a problem of password-based authentication scheme is that a server must maintain a password table for verifying the legitimacy of a remote user. Therefore, the server requires additional memory space for storing the password table for verifying user identity. Furthermore, password is generally simple and can be easily broken or forgotten. For this reason, many researchers has proposed a new remote user authentication scheme by using biological characteristics of persons such as fingerprint, iris and so on. The main property of using biometric is its uniqueness. In the view of the fact that many remote user authentication schemes using biological characteristics [9]-[12] have been proposed. In 2010, Li and Hwang [13] proposed a remote user authentication scheme which was based on biometric verification, smart card, one-way hash function and nonce for authentication. However, in 2011, Li et al. [14] found that Li and Hwang's scheme does not provide proper authentication and cannot resist man-in-the-middle attack. After that, Chuang and Chen [15] proposed an anonymous multi-server authentication scheme based on trust computing. However, Mishra et al. [16] demonstrated that the authentication scheme of Chuang and Chen cannot resist stolen smart card attack and impersonation attack and then proposed an improved multi-server based authentication scheme using smart cards for security enhancement. In 2015, Baruah et al. [17] showed that the authentication scheme of Mishra et al. cannot withstand stolen smart card attack and impersonation attacks as well and proposed biometric-based remote user authentication scheme in multi-server environment. However, Baruah et al.'s authentication scheme is still insecure. We find that their scheme cannot withstand outsider attack, smart card stolen attack, impersonation attack and replay attack as well. The remainder of the paper is organized as follows. We begin by reviewing Baruah et al.'s remote user authentication scheme in Section 2. In Section 3, we describe security weaknesses of Baruah et al.'s scheme. Finally, we conclude this paper in Section 4.

II. REVIEW IN BARUAH ET AL.'S SCHEME

This section reviews the biometric-based multi-server authentication scheme proposed by Baruah et al. in 2015. As previous researches, Baruah et al.'s scheme consists of four phases: registration, login, authentication and password change phases which as follows. The notations used in this paper are summarized as Table 1.

TABLE I. NOTATIONS USED IN BARUAH ET AL.'S SCHEME

Notations	Description
ID_i	Identity of the i^{th} user
SID_j	Identity of the j^{th} server
PW_i	Password of the i^{th} user
BIO_i	Biometric of the i^{th} user
PSK	Pre-shared key of the servers
x	Master secret maintained by the registration center
T_r	Time of registration of the user
$h(\cdot)$	A collision resistant one-way hash function
N_i, n_1	Random nonce of the i^{th} user
N_j, n_2	Random nonce of the j^{th} server
$\oplus$	The bitwise XOR operation
$\|\|$	Message concatenation operation

A. Registration phase

The registration phase is the initial phase of the scheme. In this phase, the registration center provides the secrets to the user as well as the server. It consists of the server registration phase and the user registration phase.

* Corresponding Author: Dongho Won

QSHINE 2015, August 19-20, Taipei, Taiwan
Copyright © 2015 ICST
DOI 10.4108/eai.19-8-2015.2260660

Server Registration phase
When a server wants to provide some service to the public, then it has to first register itself to the registration center. The server sends a join request along with its identity (say, SID_j) to the registration center. In return, the registration center replies with $h(SID_j||h(PSK))$ and $h(PSK||x)$ through the Internet Key Exchange Protocol version 2 (IKEv2) [18]. The server uses these secret to authenticate any registered user.

User Registration phase
The users must first register themselves if they want to access any services provided by the set of registered servers. Therefore, the user submits his/her identity ID_i and $R_1 = h(PW_i||BIO_i)$ via a secure channel. Then, the registration center performs the following.

1) The registration center computes,

   $A_i = h(ID_i||x),$
   $B_i = h(PSK||x) \oplus A_i,$
   $C_i = h(R_1||ID_i) \oplus h(A_i),$
   $D_i = h(PSK) \oplus h(ID_i),$
   $E_i = R_1 \oplus ID_i.$

2) Then, the registration center creates a smart card SC_i with the following information $\{B_i, C_i, D_i, E_i, h(\cdot)\}$ and sends the smart card to user over a secure channel.

B. Login phase

To start any conversation, the user must first login to a specific terminal using smart card. The user inserts his/her the smart card into card-reader and inputs his/her identity ID_i, password PW_i and biometric information BIO_i. Then, the smart card executes the following sequence of operations.

1) The smart card before sending any information to the server first checks whether the user is authorized to gain access or not. Therefore, it computes $R_1 = h(PW_i||BIO_i)$ and then verifies whether the entered identity ID_i is equal to stored identity $ID_i = R_1 \oplus E_i$ or not. If failure occurs, the login phase is immediately aborted. Otherwise, proceeds for the succeeding steps.
2) After checking the identity of user, the smart card extracts $h(PSK) = h(ID_i) \oplus D_i$ and $h(A_i) = C_i \oplus h(R_1||ID_i)$ from the stored data.
3) Then, the smart card randomly generates a nonce N_i and computes the messages.

   $M_1 = h(SID_j||h(PSK)) \oplus h(ID_i||N_i)$
   $M_2 = N_i \oplus h(A_i)$
   $V_1 = h(N_i \oplus B_i)$

4) The smart card transmits the login request message $\{B_i, M_1, M_2, V_1\}$ to the server SID_j over a public channel for authentication.

C. Authentication phase

After receiving the login request messages, the server SID_j performs the following set of operations to agree on the same session key.

1) The server uses its secrets, obtained during registration, to compute $A_i = B_i \oplus h(PSK||x)$ and $h(ID_i||N_i) = M_1 \oplus h(SID_j||h(PSK))$. Using $h(A_i)$, it gets N_i from $M_2 : N_i = M_2 \oplus h(A_i)$.
2) Before generating any messages, the server must verify the user's authenticity. So, it uses the above derived information and verifies whether V_1 is equal to the computed value $h(N_i \oplus B_i)$ or not. If this holds, then the server generates a random nonce N_j. On failure, the phase is simply exited.
3) The server uses the user's information and its nonce N_j and identity SID_j to generate the session key as $SK_{ji} = h(h(ID_i||N_i)||SID_j||B_i||N_j)$.
4) Now, the server sends its randomly selected nonce to the user as $M_3 = N_j \oplus h(ID_i||N_i)$ and also $V_2 = N_i \oplus h(SK_{ji}||N_j)$ over a public channel.
5) Once the message is received, the user computes N_j from M_3. It then uses the information to compute the session key as $SK_{ij} = h(h(ID_i||N_i)||SID_j||B_i||N_j)$. It is to be noted that both session keys are the same.
6) Now, the user verifies whether the server is the actual one or not with whom he/she wants to communicate with. It is done by checking N_i with the computed value $V_2 \oplus h(SK_{ij}||N_j)$.

D. Password change phase

The mechanism is simple enough that if the user wants to change his/her password, it can be done without informing the registration center.

1) The user U_i inserts his/her smart card into card-reader and enters his/her identity ID_i, password PW_i and biometric BIO_i.
2) Smart card checks the entered information. If the user is the authentic one, then the smart card prompts the user for new password PW_i^* and computes,

   $R_1^* = h(PW_i^*||BIO_i)$
   $E_i^* = E_i \oplus R_1 \oplus R_1^*$
   $C_i^* = h(R_1^*||ID_i) \oplus h(R_1||ID_i) \oplus C_i$

3) Lastly, the smart card updates E_i^* and C_i^* in the place of E_i and C_i. Now, the updated smart card has $SC_i = \{B_i, C_i^*, D_i, E_i^*, h(\cdot)\}$.

III. SECURITY ANALYSIS OF BARUAH ET AL.'S SCHEME

In this section, we demonstrate the vulnerability of Baruah et al.'s scheme in various communication scenarios. The following assumptions are made during the analysis and design of the scheme.

1) An adversary can be either a user or a server. A registered user as well as a registered server can act as an adversary.
2) An adversary can eavesdrop every communication in public channels. He/she can capture any message exchanged between user and server.

3) An adversary has the ability to alter, delete or reroute the captured message.
4) Information can be extracted from the smart card by examining the power consumption of the card.

A. *Outsider Attack*

Any adversary U_a who is the legal user and owns a smart card can obtain information $\{B_a, C_a, D_a, E_a, h(\cdot)\}$ and then he/she can compute $h(PSK) = D_a \oplus h(ID_a)$. Thus, an adversary U_a can get $h(PSK)$ which same for each legal user and is the hash value of pre-shared key of the servers.

B. *Smart Card Stolen & Off-line Identity Guessing Attack*

Smart card stolen attack means an adversary who possessed with smart card performs any operation which the smart card and obtains any information. If an outsider adversary U_a steals the smart card of legitimate user U_i and obtains parameters $\{B_i, C_i, D_i, E_i, h(\cdot)\}$, then he/she can easily compute out the hash value of the identity of the user U_i by computing $D_i \oplus h(PSK)$. Now, an adversary U_a performs an off-line identity guessing to get the current identity of the user U_i.

1) The adversary calculates $h(ID_i) = D_i \oplus h(PSK)$.
2) Then, the adversary selects a random identity ID_i^*, calculates $h(ID_i^*)$ and compares it with $h(ID_i)$. If the result is equal to $h(ID_i)$, the adversary infers that ID_i^* is user U_i's identity. Otherwise the adversary selects another identity nominee and performs the same processes, until he locates the valid identity.
3) After computing the identity of user U_i, an adversary can compute $R_1 = E_i \oplus ID_i$ and $h(A_i) = C_i \oplus h(R_1||ID_i)$.

C. *User Impersonation Attack*

An outsider and smart card stolen adversary U_a can get the value $h(PSK)$ from his own card which is same for each user and the values ID_i, $h(A_i)$ from legitimate user U_i's smart card. Then, he/she can easily impersonate as user U_i to login and access the remote server because he can compute $\{B_i, M_1, M_2, V_1\}$.

1) The adversary randomly generates a nonce N_i.
2) Then, the adversary calculates,

$$M_1 = h(SID_j||h(PSK)) \oplus h(ID_i||N_i)$$
$$M_2 = N_i \oplus h(A_i)$$
$$V_1 = h(N_i \oplus B_i)$$

3) After computing parameters, an adversary transmits the login request message $\{B_i, M_1, M_2, V_1\}$ to the server SID_j over a public channel for authentication.

D. *Replay Attack*

An outsider adversary U_a eavesdrop a communication between a user and the server and then may try to use these messages for opening a communication to a server in future. An adversary U_a may eavesdrop a communication and store the login messages, $\{M_1, M_2, V_1, B_i\}$, for performing replay attack in future where $M_1 = h(SID_j||h(PSK)) \oplus h(ID_i||N_i)$, $M_2 = N_i \oplus h(A_i)$, $V_1 = h(N_i \oplus B_i)$ and $B_i = h(PSK||x) \oplus A_i$. He/She can compute $h(ID_i||N_i) = M_1 \oplus h(SID_j||h(PSK))$. After computing $h(ID_i||N_i)$, the adversary transmits these stored messages, $\{M_1, M_2, V_1, B_i\}$, to a registered server SID_j. The server SID_j, upon receiving the messages retrieves $A_i = h(PSK||x) \oplus B_i$, $h(ID_i||N_i) = h(SID_j||h(PSK)) \oplus M_1$, $N_i = M_2 \oplus h(A_i)$ and also verifies these using V_1. This verification holds, since the messages has not been modified by the adversary. Upon verification, the server SID_j selects a random nonce N_j^* and generates the session key as $SK_{ji}^* = h(h(ID_i||N_i)||SID_j||B_i||N_j^*)$. It then uses this session key for computing the reply messages $M_3^* = N_j^* \oplus h(ID_i||N_i)$ and also $V_2^* = N_1 \oplus h(SK_{ji}^*||N_j^*)$, and transmits to the adversary. Then, the adversary easily can compute $N_j^* = M_3^* \oplus h(ID_i||N_i)$ and $SK_{ij} = h(h(ID_i||N_i)||SID_j||B_i||N_j^*)$, because he/she knows $h(ID_i||N_i)$.

IV. Conclusion

In 2015, Baruah et al. proposed an enhanced scheme of Mishra et al.'s scheme and demonstrated it is resistance to famous attacks such as impersonation attacks, smart card stolen attacks, off-line password guessing attacks, man-in-the-middle attacks and replay attacks. However, Baruah et al.'s scheme is still insecure. We shown how their scheme can suffer from outsider attacks, smart card stolen attacks, user impersonation attacks and replay attacks. Finally, our further research direction ought to propose a secure user authentication scheme which can solve these problems.

ACKNOWLEDGEMENT

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.R0126-15-1111, The Development of Risk-based Authentication·Access Control Platform and Compliance Technique for Cloud Security)

References

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

[2] A. Conklin, G. Dietrich and D. Walz, Password-based authentication: a system perspective," in *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*, vol. 50, pp. 629-631, 2004

[3] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-Based Authenticated Key Exchange in the Three-Party Setting," in *On Public Key Cryptography-PKC 2005*, vol. 3386, pp. 65-84, 2005

[4] S. Jiang, and G. Gong, "Password based key exchange with mutual authentication," in *Selected Areas in Cryptography*, vol. 3357, pp. 267-279, 2005

[5] R. Gennaro, and Y. Lindell, "A framework for password-based authenticated key exchange," in *ACM Transactions on Information and System Security (TISSEC)*, vol. 9, pp. 181-234, 2006

[6] Y. Yang, R. Deng, and F. Bao, "A practical password-based two-server authentication and key exchange system," in *Dependable and Secure Computing, IEEE Transactions on*, vol. 3, pp. 105-114, 2006

[7] A. Groce, and J. Katz, "A new framework for efficient password-based authenticated key exchange," in *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 516-525, 2010

[8] I. Jeun, M. Kim, and D. Won, "Enhanced password-based user authentication using smart phone," in *Advances in Grid and Pervasive Computing*, vol. 7296, pp. 350-360, 2012

[9] J. Lee, S. Ryu and K. Yoo, ”Fingerprint-based remote user authentication scheme using smart cards,” in *Electronics Letters*, vol. 38, pp. 554-555, 2002

[10] C. Lin and Y. Lai, ”A flexible biometrics remote user authentication scheme,” in *Computer Standards & Interfaces*, vol. 27, pp. 19-23, 2004

[11] C. Chang and I. Lin, ”Remarks on fingerprint-based remote user authentication scheme using smart cards,” in *ACM SIGOPS Operating Systems Review*, vol. 38, pp. 91-96, 2004

[12] W. Yi, S. Kim, and D. Won, ”Smart Card Based AKE Protocol Using Biometric Information in Pervasive Computing Environments,” in *Computational Science and Its Applications-ICCSA 2009*, vol. 5593, pp. 182-190, 2009

[13] C. Li and M. Hwang, ”An efficient biometrics-based remote user authentication scheme using smart cards,” in *Journal of Network and Computer Applications*, vol. 33, pp. 1-5, 2010

[14] X. Li, J. Niu, J. Ma, W. Wang and C. Liu, ”Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards,” in *Journal of Network and Computer Applications*, vol. 34, pp. 73-79, 2011

[15] M. Chuang and M. Chen, ”An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics,” in *Experts Systems with Applications*, vol. 41, pp. 1411-1418, 2014

[16] D. Mishra, A. Das and S. Mukhopadhyay, ”A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards,” in *Expert Systems with Applications*, vol. 41, pp. 8129-8143, 2014

[17] K. Baruah, S. Banerjee, M. Dutta and C. Bhunia, ”An Improved Biometric-based Multi-server Authentication Scheme Using Smart Card,” in *International Journal of Security and Its Applications*, vol. 9, pp. 397-408, 2015

[18] C. Kaufman, Internet Key Exchange(IKEv2) protocol, 2005