Contemporary Engineering Sciences, Vol. 7, 2014, no. 26, 1467 - 1473
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2014.49118

Security Flaws of Cheng et al.'s Biometric-based Remote User Authentication Scheme Using Quadratic Residues

Eun-Jun Yoon[1]

Department of Cyber Security, Kyungil University
33 Buho-Ri, Hayang-Ub, Kyungsan-Si
Kyungsangpuk-Do 712-701, Republic of Korea

Abstract

Recently, Cheng et al. proposed a novel biometric-based remote user authentication scheme using quadratic residues. Cheng et al. claimed that their proposed scheme is secure, practical, and trustworthy remote authentication, which can be implemented on different real network environments. However, this paper points out that Cheng et al.'s scheme not only suffers from stolen smart card attack and server spoofing attack, but also does not provide forward secrecy.

Keywords: Cryptography; Biometrics authentication; Quadratic residue; Stolen smart card attack; Server spoofing attack; Forward secrecy

1 Introduction

Remote user authentication scheme using smart cards allow remote users to communicate securely over public networks simply by using easy-to-remember passwords and smart cards for the client-server architecture[1, 2, 3, 4, 5, 6, 7]. To provide strong security, the remote user authentication scheme adopts people's biometrics information (e.g. fingerprints, faces, iris scan, voice print, hand geometry, and palm-prints) for convincing users' identities[4, 5, 6, 7]. Generally, the biometric technology has three main advantages as follows[7]:

[1]Corresponding author: Eun-Jun Yoon Tel.: +82-53-600-5623; Fax: +82-53-600-5579

1. The personal biometric information is extremely hard to make duplicate or share biometrics.
2. The personal biometric information is extremely hard to forge or distribute.
3. The personal biometric information cannot lost or forgotten and cannot be guessed easily.

In 2013, Cheng et al.[7] proposed a novel biometric based remote user authentication scheme which is based on the quadratic residues and biometric verification to achieve efficient and security requirements. Through the security analysis, Cheng et al. claimed that their proposed scheme is secure, practical, and trustworthy remote authentication, which can be implemented on different real network environments. However, this paper points out that Cheng et al.'s scheme not only suffers from stolen smart card attack and server spoofing attack, but also does not provide forward secrecy.

This paper is organized as follows: Section 2 briefly reviews the Cheng et al.'s scheme. The security flaws of Cheng et al.'s scheme are shown in Section 3. Finally, conclusions are given in Section 4.

2 Review of Cheng et al.'s Scheme

This section briefly reviews Cheng et al.'s scheme[7]. The Cheng et al.'s scheme consists of three phases: registration phase, login phase, authentication phase.

2.1 Notations

We outlined some notations used in this research paper.

- U : the remote user
- R : the trusted registration center
- S : the server
- ID : the identity of remote user
- x : the secret information of the server S
- B : the biometric information of remote user
- n : the product of two large prime, p and q
- r : the random number selected by the registration center R
- t : the random number selected by the user U
- s : the random number selected by the server S

- $h(\cdot)$: the secure one-way hash function
- $\oplus$: the bitwise exclusive-or operation
- $||$: the concatenation operation

2.2 Registration phase

Figure 1 depicts the registration phase of Cheng et al.'s scheme. In this phase, the user U initially registers with the trusted registration center. The following steps are executed:

R1. In the beginning, the user U sends his/her identity ID and the related biometrics B to the registration center R over a secure channel.

R2. After receiving the message $\{ID, B\}$, the registration center R computes $f = B \oplus r$, and $A = x \oplus f \oplus ID$, where r is a random number unique to R. And then, R stores the data $\{f, A, ID, r, h(\cdot)\}$ into a smart card and issues it to U.

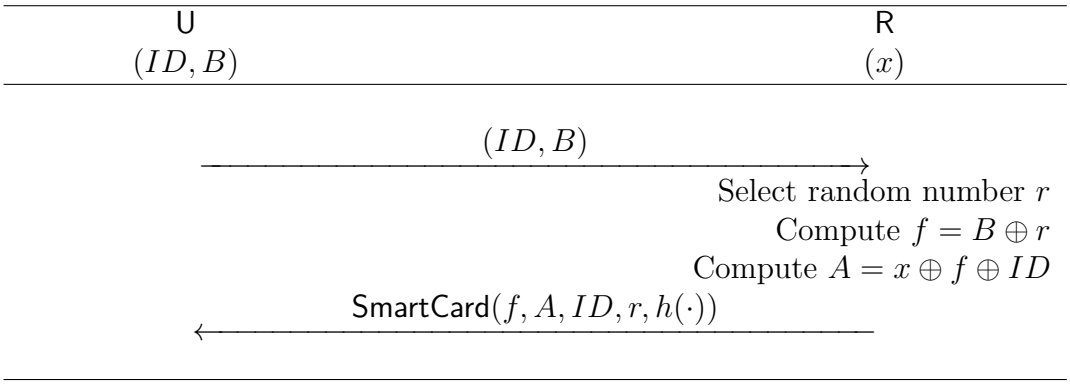

Figure 1: Registration phase of Cheng et al.'s scheme

2.3 Login phase

Figure 2 depicts the login and authentication phases of Cheng et al.'s scheme. The login phase is invoked whenever the user U asks the services from the server S.

L1. The user U inserts his/her smart card into the card reader, and inputs his/her identity ID and the personal biometrics B.

L2. The smart card checks $f \oplus r \stackrel{?}{=} B$ to verify the user U's biometrics on the specific device. If it holds, U passes the biometrics verification; otherwise, the scheme is aborted.

L3. The user U randomly selects a number t to compute $D = h(A \oplus f \oplus ID \oplus t)$, $T = t^2 \bmod n$, and $M = h(t)$.

L4. The user U forwards the message $\{D, T, M\}$ to the server S.

2.4 Authentication phase

After receiving the login message from the user U, both the server S and the user U perform the following steps to achieve mutual authentication.

A1. The server S utilizes the Chinese Remainder Theorem[7] to solve $T = t^2 \bmod n$, since S can derive four roots (t_1, t_2, t_3, t_4) with two large primes p and q.

A2. The server S compares $h(t_i)$ with the received M, for $i = 1$ to 4, so that it can obtain the correct value of t.

A3. The server S checks $h(x \oplus t) \stackrel{?}{=} D$. If it holds, S believes the validity of U; otherwise, S rejects the user's login request.

A4. The server S computes $E = h(x \oplus t) \oplus s$ and $N = h(h(x \oplus t)||s)$, where s is a random number selected by the server S, and S forwards the message $\{E, N\}$ to U.

A5. After receiving the message, the user U computes $s' = D \oplus E$.

A6. The user U checks $N \stackrel{?}{=} h(D||s') = h(h(x \oplus t)||s')$ by using the derived s'. If it holds, the user believes the trustworthy of S.

After finishing the mutual authentication, both the user and the server compute the common session key $sk = h(D||s'||r) = h(h(x \oplus t)||s||r)$ for their subsequent communication.

3 Cryptanalysis of Cheng et al.'s Scheme

This section demonstrates that Cheng et al.'s scheme not only suffers from stolen smart card attack and server spoofing attack, but also does not provide forward secrecy.

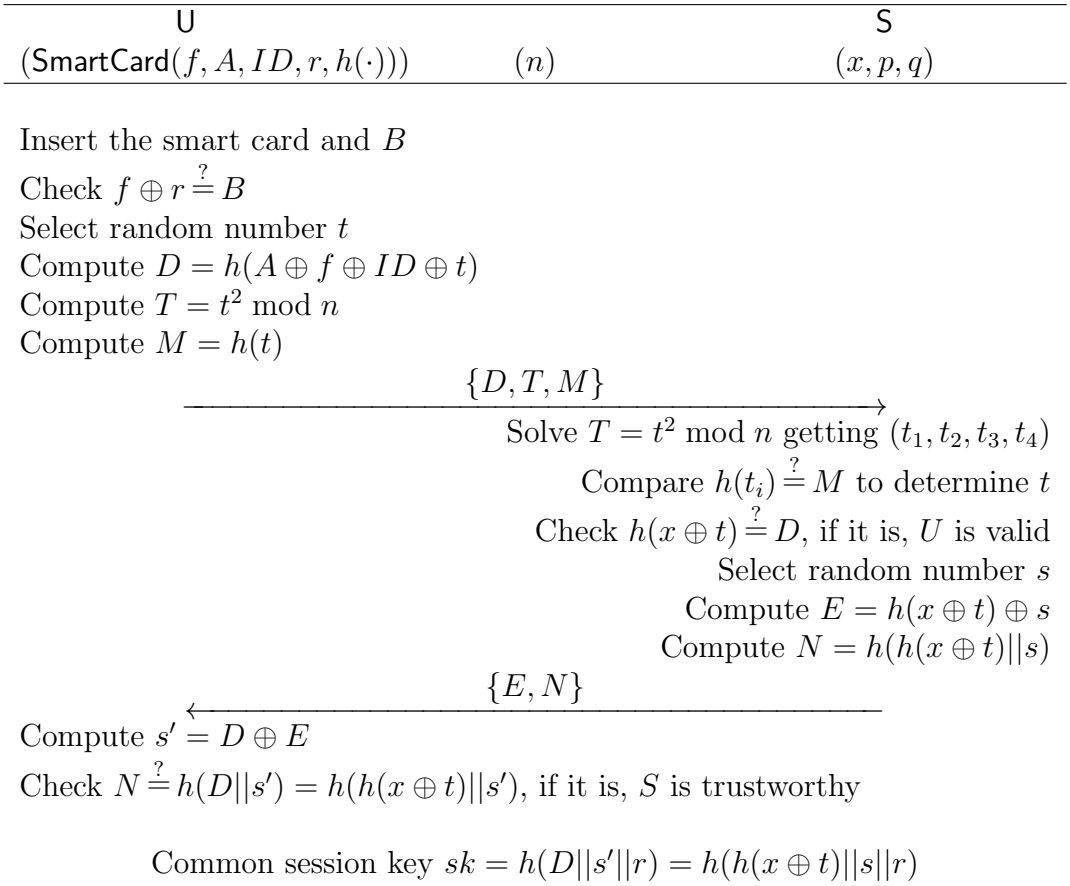

Figure 2: Login and authentication phases of Cheng et al.'s scheme

3.1 Stolen smart card attack

Suppose that an attacker *Eve* obtained a legal user's smart card. We know that the smart card has the data $\{f, A, ID, r, h(\cdot)\}$ for the user U. Then, the attacker *Eve* can perform the following stolen smart card attack.

1. Extract the biometrics B by computing $f \oplus r$. Because $f \oplus r = B \oplus r \oplus r = B$, *Eve* can easily obtain B.

2. Extract the secret key x of the server S by computing $f \oplus A \oplus ID$. Because $f \oplus A \oplus ID = f \oplus x \oplus f \oplus ID \oplus ID = x$, *Eve* can easily obtain the secret key x.

By using B and x, the attacker *Eve* can freely perform the user impersonation attack or the server impersonation attack. Therefore, Cheng et al.'s scheme is vulnerable to the above stolen smart card attack.

3.2 Server spoofing attack

An attacker *Eve* can perform the following server spoofing attack.

1. *Eve* intercepts $\{D, T, M\}$.
2. *Eve* selects a random number s.
3. *Eve* computes $E' = D \oplus s$.
4. *Eve* computes $N' = h(D||s)$.
5. *Eve* finally sends $\{E', N'\}$ to the user U.

After receiving $\{E', N'\}$, the user U will perform the following steps.

1. Compute $s' = D \oplus E'$. Here, we can see that $D \oplus E' = D \oplus D \oplus s = s'$.
2. Check $N' \stackrel{?}{=} h(D||s')$ by using the derived s'.

Because N' always equals $h(D||s')$, the user U will believe the trustworthy of the attacker *Eve*. Therefore, Cheng et al.'s scheme is vulnerable to the above server spoofing attack.

3.3 Forward secrecy problem

Forward secrecy is one of the security notions addressing the session key exposure issues[7]. Without knowing the master key x, an attacker *Eve* can easily compute the previous session keys $sk = h(D||s'||r) = h(h(x \oplus t)||s||r)$ by using the compromised long-term random number r which generated by the registration center R. We assume that *Eve* gets the long-term random number r in Cheng et al.'s scheme, and he/she wants to compromise the previously generated session keys sk. *Eve* can simply compute any past versions of session keys by computing $sk = h(D||s||r)$ because D is public value and s can be obtained by computing $D \oplus E$. Therefore, Cheng et al.'s scheme cannot provide the forward secrecy.

4 Conclusions

This paper pointed out that recently proposed Cheng et al.'s biometric-based remote user authentication scheme using quadratic residues not only suffers from stolen smart card attack and impersonation attacks, but also does not provide forward secrecy. Further works will be focused on improving the Cheng et al.'s scheme which can be able to provide strong security.

Acknowledgements

This work was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(No. 2010-0010106).

References

[1] L. Lamport, Password authentication with insecure communication, *Communications of the ACM*, **24(11)** (1993), 770-772.

[2] J. Jan and Y. Chen, Paramita wisdom password authentication scheme without verification tables, *The Journal of Systems and Software*, **42(1)** (1998), 45-57.

[3] M. Hwang and L. Li, A new remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electronics*, **46(1)** (2000), 28-30.

[4] M. Khan, J. Zhang, and X. Wang, Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices, *Chaos, Solitons and Fractals*, **35(3)** (2008), 519-524.

[5] C. Li and M. Hwang, An efficient biometric-based remote user authentication scheme using smart cards, *Journal of Network and Computer Applications*, **33(1)** (2010), 1-5.

[6] 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, *Journal of Network and Computer Applications*, **34(1)** (2011), 73-79.

[7] Z. Cheng, Y. Liu, C. Chang, and C. Liu, A novel biometric-based remote user authentication scheme using quadratic residues, *International Journal of Information and Electronics Engineering*, **3(4)** (2013), 419-422.

Received: September 4, 2014; Published: October 28, 2014