Improvement of a Fingerprint-Based Remote User Authentication Scheme

Jing Xu Wen-Tao Zhu Deng-Guo Feng
State Key Laboratory of Information Security,
Graduate University of Chinese Academy of Sciences
P. O. Box 4588, Beijing 100049, P. R. China
xujing@is.iscas.ac.cn

Abstract

Password authentication has been adopted as one of the most commonly used solutions in network environments to protect resources from unauthorized access. Recently, Khan et al. proposed an efficient fingerprint-based remote user authentication scheme with smart cards [15], in which a password/verification table is not required on the remote server, and users are allowed to choose and update their passwords freely. In this paper, we show that their scheme is vulnerable to the parallel session attack. Furthermore, their scheme is susceptible to the impersonation attack provided that the information stored in the smart card is disclosed by an adversary. We also propose an improved scheme which is immune to the presented attacks.

1 Introduction

Authentication ensures that a system's resources are not obtained fraudulently by illegal users. Password based authentication is one of the most simple and convenient authentication mechanisms over insecure networks. In 1981, Lamport proposed a remote password authentication scheme [1] by employing a one-way hash chain, which Haller later used to design the famous S/KEY one-time password system [2]. However, one weakness of their scheme is that a verification table should be maintained on the remote server in order to validate the legitimacy of the requesting users; if an intruder can somehow break into the server, the contents of the verification table may be easily modified [3]. Therefore, many password authentication schemes [4–11] have recognized this problem, and solutions based on smart cards have been proposed, where a verification table is no longer required.

In a typical smart card based password authentication scheme, remote users are authenticated with their smart cards as identification tokens. The card takes as input a password from the user, creates a login message from the given password, and sends the message to a remote server, which then checks the validity of the login message before allowing access to any services or resources. This way the administrative overhead of the authentication server is reduced, and the user only needs to remember his password.

Recently, some biometrics-based remote user authentication schemes have been designed. In 2002, Lee et al. [12] proposed a fingerprint-based scheme using smart cards. It is based on ElGamal's public key cryptosystem, which also does not require password table for authentication. The scheme is novel in that biological information and two secret keys are employed to improve the security.

However, Lin et al. [13] and Ku et al. [14] pointed out in 2004 and 2005 respectively that Lee et al.'s scheme [12] cannot withstand the masquerade attack, in which an adversary can impersonate a legitimate user without knowing the password and passing the fingerprint verification. Later, in ISPEC 2006, Khan et al. [15] also showed that Lee et al.'s scheme [12] was vulnerable to the server spoofing attack. Furthermore, they proposed an improved scheme to enhance the security. Based on the one-way hash function and fingerprint verification, Khan et al.'s scheme needs only to maintain one secret key, and a password verification table is not required on the server. They claimed that their scheme achieved mutual authentication between the user and the server, and thus eliminated the drawback of Lee et al.'s scheme.

In this paper, we demonstrate that Khan et al.'s scheme [15] is still vulnerable. It is susceptible to the parallel session attack, in which an adversary without knowing a legal user's password can masquerade as the user by somehow crafting a valid login message from eavesdropped communications between the user and the server. What's more, their scheme cannot resist the impersonation attack provided that a user's smart card is stolen by the adversary and the information stored in the device is extracted, e.g., by means presented in [16,17]. Therefore, we claim that Khan et al.'s scheme [15] fails to meet the security requirement that smart card based authentication should achieve. Contributions of this paper also include a new scheme in which the security flaws are eliminated while some favorable flavors are added.

The remainder of this paper is organized as follows. In the next section, a brief review of Khan et al.'s scheme [15] is given. In Section 3 we point out the weaknesses of Khan et al.'s scheme. We then present our improved scheme and examine its security in Section 4. Finally, we conclude in Section 5.

2 Review of Khan et al.'s Scheme

In this section, we briefly review Khan et al.'s fingerprint-based remote user authentication scheme, which consists of the registration, login, authentication, and password change phases [15]. Fig.1 illustrates this smart card based password authentication scheme.

[Registration Phase]

In this phase, everyone to be registered at the server is issued a smart card. To initialize, the server selects a secure one-way hash function $h(\cdot)$ and a secret key x. Details of this phase are described in the following steps:

(1) The user freely chooses his identifier ID and password PW, and submits ID and PW to the server through a secure channel. The user also imprints his fingerprint at the sensor.

(2) Upon receiving the registration request, the server computes $A = h(ID \oplus x)$ and $V = A \oplus h(PW \oplus F)$, where F is the extracted fingerprint template of the user.

(3) The server stores $\{ID, A, V, F, h(\cdot)\}$ into a smart card and issues the device to the user.

[Login Phase]

In this phase, the user attaches his smart card to an input device, keys in his ID and PW^*, and imprints his fingerprint at the sensor. If the user passes the fingerprint verification, the smart card performs the following steps:

(1) Compute $B = V \oplus h(PW^* \oplus F)$, and checks whether B equals A stored in the device. If not, terminate the operation.

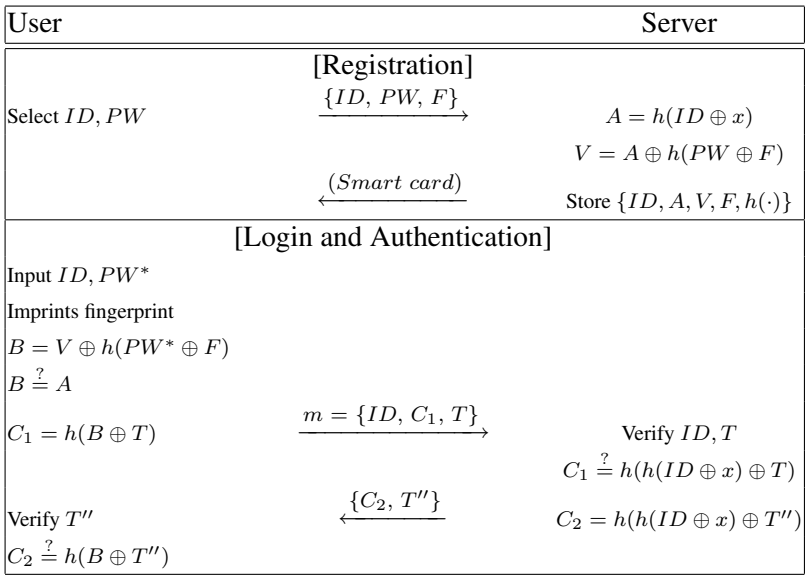

Figure 1. Khan et al.'s scheme

(2) Compute $C_1 = h(B \oplus T)$, where T is the current time of the input device.

(3) Send the login message $m = \{ID, C_1, T\}$ to the remote server (over an possibly insecure channel).

[Authentication Phase]

Upon receiving the request m, the smart card and the server perform the following steps for mutual authentication between the user and the remote system:

(1) The server verifies that ID is a registered user identifier. If not, the login request is rejected.

(2) Let T' be the time when the server receives m. The server compares T and T'. If the difference is beyond a predefined threshold, the login request is rejected.

(3) The server computes $C_1^* = h(h(ID \oplus x) \oplus T)$ and checks whether the relation $C_1 = C_1^*$ holds. If not, the request is rejected.

(4) For mutual authentication, the server computes $C_2 = h(h(ID \oplus x) \oplus T'')$ and sends the message $\{C_2, T''\}$ back to the smart card, where T'' is the current time of the server.

(5) Upon receiving the message $\{C_2, T''\}$, the device first validates T'', and then checks whether the relation $C_2 = h(B \oplus T'')$ holds. If so, the mutual authentication between the user and the remote system is completed.

[Password Change Phase]

When a user wants to update his old password PW to a new PW', he inserts his smart card into the terminal, enters his ID and PW^*, and imprints his fingerprint at the sensor. If the user passes the biometric authentication, the smart card performs the following operations without interacting with the remote server:

(1) Compute $B = V \oplus h(PW^* \oplus F)$.

(2) Check whether B equals the stored A. If not, terminate the operation.

(3) Prompt the user to input the new password PW', compute $V' = B \oplus h(PW' \oplus F)$, and then store it into the smart card to substitute V.

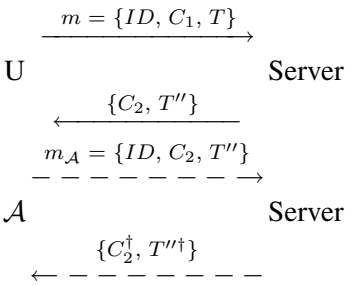

Figure 2. Parallel session attack

3 Cryptanalysis of Khan et al.'s Scheme

In this section, we show that Khan et al.'s scheme [15] is vulnerable to the following parallel session attack and the impersonation attack.

3.1 Parallel Session Attack

We demonstrate the parallel session attack by considering an adversary $\mathcal{A}$, who neither knows the intended user U's password nor holds the smart card of U (hence a successful attack under these two assumptions/limitations should be considered as a strong one). Although it is clearly impossible for $\mathcal{A}$ to have the same fingerprint with U, we suppose $\mathcal{A}$ has the ability to eavesdrop on the communication channel between U and the authentication server. In the following scenario, $\mathcal{A}$ attempts to masquerade as U by means of crafting a valid login message.

Assume that in the login phase a message $m = \{ID, C_1, T\}$ is sent by U as the request, which is followed by a server response $\{C_2, T''\}$ in the (mutual) authentication phase. The parallel session attack can be plotted if $\mathcal{A}$ observes and makes use of the above information. To do so, $\mathcal{A}$ simply sends a message $m_{\mathcal{A}} = \{ID, C_2, T''\}$ to the server, where the time T'' is still "fresh" to the server and trickily, $C_2 = h(h(ID \oplus x) \oplus T'')$ is computed by the server itself (instead of $\mathcal{A}$). It is easy to see that $\mathcal{A}$ can then pass the verification (in parallel with U) and thus login the server successfully.

Fig. 2 depicts the messages transmitted in the parallel session attack. We note that such an attack is made possible due to the *symmetric* nature of the information exchanged between the user and the remote server in the login and authentication phases (i.e., the values C_1 and C_2 in Fig. 1).

3.2 Impersonation Attack

We now show that Khan et al.'s scheme [15] is vulnerable to the impersonation attack provided that the adversary has stolen a user U's smart card. We note that as observed by Kocher et al. [16] and Messerges et al. [17], all existent smart cards are vulnerable in that the confidential information stored in the device could be extracted by physically monitoring its power consumption; once a card is lost, all secrets in it may be revealed. In the following scenario, we assume the adversary $\mathcal{A}$ has acquired U's smart card, but he does not known the owner password.

Suppose $\mathcal{A}$ has extracted the stored value $A\,(= h(ID \oplus x))$ from the stolen device. Then $\mathcal{A}$ constructs a message $m_{\mathcal{A}} = \{ID, C_1', T\}$, where $C_1' = h(A \oplus T)$. Since $C_1' = h(h(ID \oplus x) \oplus T)$, the server will accept the login request $m_{\mathcal{A}}$. Note that not only the password PW is blind to $\mathcal{A}$, but it is also infeasible (and unnecessary) for $\mathcal{A}$ to pass the fingerprint verification.

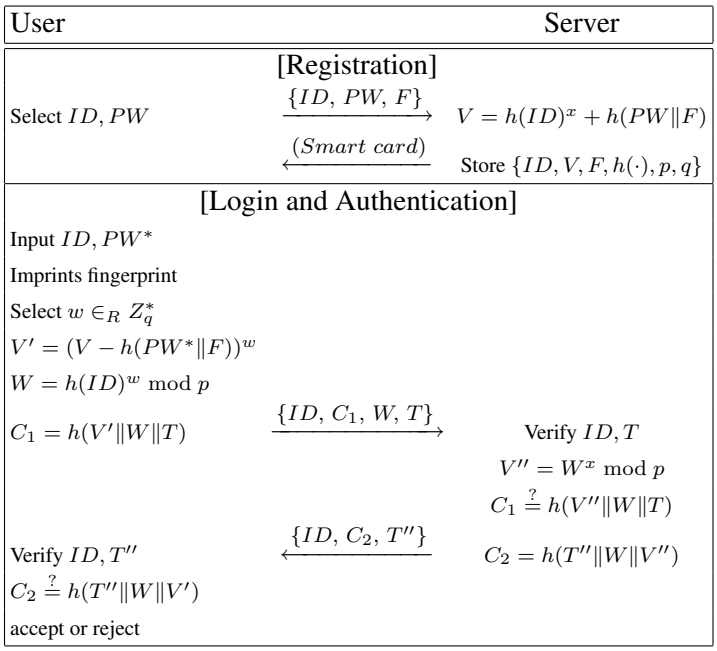

Figure 3. Improved scheme

4 Improved Scheme

To counter the afore-discussed attacks, we now propose an improved smart card based authentication scheme, which also consists of the registration, login, authentication, and password change phases. The scheme is illustrated in Fig. 3, which is then followed by a security evaluation.

[Registration Phase]

To initialize, the server selects large prime numbers p and q satisfying $p = 2q + 1$. The server also choose its secret key x and an appropriate one-way hash function $h(\cdot) : \{0,1\}^* \rightarrow Z_p^*$. Then the protocol proceeds in the following steps:

(1) The user submits his identifier ID and password PW to the server through a secure channel. The user also imprints his fingerprint at the sensor.

(2) Upon receiving the registration request and the extracted fingerprint template F, the server computes $V = h(ID)^x + h(PW\|F) \bmod p$.

(3) The server stores $\{ID, V, F, h(\cdot), p, q\}$ into a smart card and issues the device to the user.

[Login Phase]

The user attaches his smart card to a device reader, inputs his ID and PW^*, and imprints his fingerprint at the sensor. If the user passes the fingerprint verification, the smart card performs the following steps:

(1) Choose $w \in_R Z_q^*$, and compute $V' = (V - h(PW^*\|F))^w \bmod p$, $W = h(ID)^w \bmod p$, and $C_1 = h(V'\|W\|T)$, where T is the current time of the input device.

(2) Send the login message $\{ID, C_1, W, T\}$ to the remote server (over an possibly insecure channel).

[Authentication Phase]

In this phase, the server and the smart card performs the following steps for mutual authentication. Moreover, a session key K is agreed by the two parties.

(1) The server checks that ID is valid. If not, the login request is rejected.

(2) The server checks that the difference between T and T' is within a predefined threshold, where T' is the time when receiving the login request.

(3) The server computes $V'' = W^x \bmod p$ and compares C_1 with $h(V''\|W\|T)$. If they are not equal, the login request is rejected.

(4) The server computes $C_2 = h(T''\|W\|V'')$, and sends the message $\{ID, C_2, T''\}$ to the device, where T'' is the current time stamp of the server.

(5) Upon receiving the message, the smart card validates ID and T'', and then compares C_2 with $h(T''\|W\|V')$. If they are equal, the server is authenticated.

[Password Change Phase]

When a user wants to update his old password PW to a new PW', he inserts his smart card into the terminal, enters his ID and PW, and imprints his fingerprint at the sensor. If the user passes the biometric authentication, the smart card confirms the validity of PW (by interacting with the authentication server). Then the smart card prompts the user to input the new password PW', and replaces $V(= h(ID)^x + h(PW\|F) \bmod p)$ stored in the smart card with a new value $V + h(PW'\|F) - h(PW\|F) \bmod p$.

[Security Evaluation]

We now evaluate the security of our improved scheme. Similar to the discussion in Section 3.2, we consider an adversary $\mathcal{A}$ who has partial control over the communication channel, and may have stolen a smart card from a legitimate user but does not know the owner password.

(1) We claim that the proposed scheme is immune to the parallel session attack. This is due to the asymmetric structure of the two values C_1 and C_2 in the mutual authentication, where $C_1 = h(V'\|W\|T)$ and $C_2 = h(T''\|W\|V'')$.

(2) For the attacker $\mathcal{A}$ who does not know the user password PW to construct a valid login message, even if he has extracted the necessary information from the stolen smart card, the knowledge of $V' = h(ID)^{x \cdot w} \bmod p$ is essential to compute the value C_1. Hence to impersonate a legal user, $\mathcal{A}$ needs to know $h(ID)^x$. The computational values transmitted online are $C_1 = h(h(ID)^{x \cdot w} \bmod p \parallel h(ID)^w \bmod p \parallel T)$, $W = h(ID)^w \bmod p$, and $C_2 = h(T'' \parallel h(ID)^w \bmod p \parallel h(ID)^{x \cdot w} \bmod p)$. It is impossible for $\mathcal{A}$ to learn x or $h(ID)^x$ from those data, provided that the one-way function $h(\cdot)$ is secure and the discrete logarithm problem (DLP) is intractable. Therefore, $\mathcal{A}$ cannot impersonate a legal user.

(3) In our scheme, an attacker $\mathcal{A}$ is infeasible to impersonate the server to cheat the requesting user. In fact, if $\mathcal{A}$ wants to masquerade as the server, he needs to send a message $\{ID, C_2, T''\}$ to respond to the user login request, where $C_2 = h(T'' \parallel h(ID)^w \bmod p \parallel h(ID)^{x \cdot w} \bmod p)$. Clearly, without knowing x it is impossible for $\mathcal{A}$ to do so. Therefore, our scheme achieves mutual authentication.

(4) Our scheme is immune to the so called off-line password guessing attack even if the smart card is stolen. In such an attack, the adversary strategically selects a candidate string S from a reasonable set $\mathbb{S}$ (which corresponds to a "password dictionary"), computes a value

$\mathcal{V}(S)$ based on various information including the candidate password S, and compares $\mathcal{V}(S)$ with a certain "reference value" $\mathcal{V}(PW)$ derived from the real password PW. For example, $\mathcal{V}(PW)$ is typically obtained either from a stolen smart card or via sniffing on the network data link. Such a selection-computation-comparison process is repeated *off-line* until a collision $\mathcal{V}(S) = \mathcal{V}(PW)$ is found, thus yielding the real password $S = PW$. However, we claim that it is infeasible for an adversary to launch such a guessing attack in the improved scheme:

- $\mathcal{A}$ may utilize the revealed F from the stolen smart card, and may try to determine the correctness of a candidate password S by computing $\mathcal{V}(S) = h(ID)^x + h(S\|F) \bmod p$ and then comparing it with $\mathcal{V}(PW) = V$, which can also be extracted from the stolen device. However, this approach is impractical since $\mathcal{A}$ does not know $h(ID)^x$.
- Then $\mathcal{A}$ may turn to C_1 and C_2 and have one of them play the role of $\mathcal{V}(PW)$. Note that these "referential" $C_1(PW)$ and $C_2(PW)$ can both be easily obtained by means of eavesdropping. For example, a "computational" C_1 with respect to a candidate string S can be viewed as $C_1(S) = h((V - h(S\|F))^w \bmod p \parallel W \parallel T)$. However, even if the values like $V, F, h(\cdot), p, g$ are revealed from the stolen smart card, without knowing w (hidden in $W = h(ID)^w \bmod p$) it is impossible for $\mathcal{A}$ to compute $C_1(S)$ (so as to compare it with $C_1(PW)$ for the collision attack).

(5) Our scheme does not involve a verification table on the server side and thus is not affected by the stolen-verifier and modification attacks [3]. Moreover, if $h(\cdot)$ is published in advance, and in the registration phase we have the user submit $h(PW)$ instead of PW, we can even blind the server to the user password for even higher security.

5 Conclusion

In this paper, we presented a security analysis of Khan et al.'s password authentication scheme based on the smart card [15]. Our results showed that their scheme is vulnerable to the parallel session attack. Furthermore, their scheme cannot resist the impersonation attack provided that the information stored in the smart card is disclosed by an adversary. We then proposed an improved scheme to counter various known attacks.

Acknowledgements

This work is supported by the National Basic Research Program of China 973 Program under Grant No. 2007CB311202, the National Natural Science Foundation of China under Grant No. 60503046, 60673083, and the National Key Technology R&D Program of China under Grant No. 2006BAH02A02. The authors would like to thank the anonymous referees for their helpful comments.

References

[1] L. Lamport, Password authentication with insecure communication, Communications of the ACM, 24(11), 1981, pp. 770–772.