2014

Cryptanalysis of an Improved Smartcard-based Remote Password Authentication Scheme

SK Hafizul Islam
Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333031, India, hafi786@gmail.com

G. P. Biswas
Department of Computer Science and Engineering, Indian School of Mines, Dhanbad, Jharkhand 826004, India, hafi786@gmail.com

Kim-Kwang Raymond Choo
Information Assurance Research Group, Advanced Computing Research Centre, University of South Australia, Australia, hafi786@gmail.com

Follow this and additional works at: https://digitalcommons.aaru.edu.jo/isl

Recommended Citation
Available at: https://digitalcommons.aaru.edu.jo/isl/vol3/iss1/5

This Article is brought to you for free and open access by Arab Journals Platform. It has been accepted for inclusion in Information Sciences Letters by an authorized editor. The journal is hosted on Digital Commons, an Elsevier platform. For more information, please contact rakan@aaru.edu.jo, marah@aaru.edu.jo, dr_ahmad@aaru.edu.jo.
Cryptanalysis of an Improved Smartcard-based Remote Password Authentication Scheme

SK Hafizul Islam\(^1\), G. P. Biswas\(^2\) and Kim-Kwang Raymond Choo\(^3\)

\(^1\) Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333031, India
\(^2\) Department of Computer Science and Engineering, Indian School of Mines, Dhanbad, Jharkhand 826004, India
\(^3\) Information Assurance Research Group, Advanced Computing Research Centre, University of South Australia, Australia

Abstract: In recent years, several dynamic identity-based two-factor user authentication using password and smartcard have been proposed to provide mutual authentication between the user and server over unreliable networks. However, the design of secure cryptographic schemes is still notoriously hard, and there have been several instances of detected flaws in published schemes. For example in 2010, Hao and Yu demonstrated that Wang et al.’s user authentication scheme is insecure against off-line password guessing and server masquerade attacks, and proposed an improved scheme. Subsequently in 2012, Chao pointed out that the improved scheme of Hao and Yu is, unfortunately, susceptible to off-line password guessing and server masquerade attacks, and prone to password backward security problem; and proposed an enhanced scheme. In this paper, we demonstrated that Chao’s enhanced scheme is not secure against user masquerade attack, server masquerade attack, insider attack and off-line password guessing attack in violation of its security claim as well as it fails to achieve users’ anonymity.

Keywords: Two-factor authentication, One-way hash function, Password guessing attack, Insider attack, Password, Smartcard

1 Introduction

As the Internet evolves from an academic and research network into a commercial network, more and more organizations and individuals are connecting their internal networks and computers to the Internet. Investment in network expansion by telecommunications companies will see a further expansion in capacity that will result in an increase in bandwidth availability and greater adoption of wireless and mobile technologies. As businesses continue to engage in electronic commerce, they will become increasingly globalized and interconnected. These, and other developments, create not only benefits for the community, but also risks of cybercrime [1]. Cybercriminals, for example, aim to disrupt one or more combinations of the following security notions: data confidentiality, data integrity and data availability. The ability to provide security guarantees is of paramount importance and several initiatives have been proposed to address this concern. Due to the low computation cost and portability of smartcard and easy memorization of user chosen password, two-factor smartcard authentication [2–21] using password is commonly used in Internet-based applications such as remote user/server login, online banking, Pay-TV, electronic voting, secret online order placement.

In recent years, several smartcard based password authentication schemes have been published. For example in 2002, Chien et al. [2] proposed one such scheme, but was subsequently found to be vulnerable to reflection and insider attacks [3]. To remove these drawbacks, Ku and Chen [3] designed another improved scheme, but Wang et al. [4] demonstrated that the scheme is insecure against off-line password guessing attack, forgery attack and denial of service (DoS) attack, and proposed another improved scheme. However, Chung et al. [5] revealed that Wang et al.’s scheme [2] is still susceptible to impersonation attack and off-line password guessing attack. In addition, Wang et al.’s scheme is not easily repairable and is unable to provide perfect forward secrecy of the generated session key. Other instances of vulnerabilities in published smartcard-based password authentication schemes include off-line password...
guessing attack [6–8, 22], impersonation attack [9–11], forgery attack [4, 12–14], DoS attack [4, 7, 18, 23], parallel session attack [4, 9, 10, 18], replay attack [23], stolen/lost smartcard attack [9, 22, 24], observing power consumption [25] and reverse engineering techniques [26, 27].

In this paper, we examine the protocol of Chao [16] whose history is as follows. In 2010, Hao and Yu [17] pointed out that Wang et al.'s scheme [6] is not secure against off-line password guessing attack and server masquerade attack, and proposed an enhanced scheme. Unfortunately, Chao [16] demonstrated that Hao and Yu’s scheme [17] is still insecure against off-line password guessing attack and server masquerade attack, and prone to password backward security problem i.e., the scheme must be replaced if the scheme was attacked for one time, in violation of its security claims.

They then designed an improved ID-based scheme. The latter scheme is examined in this paper where we pointed out that this scheme is not secure from insider attack, server masquerade attack and user masquerade attack and user’s anonymity problem. Furthermore, the scheme is susceptible to off-line password guessing attacks in which an attacker exhaustively enumerates all possible passwords in an offline manner to find out the correct password on lost/stolen smartcard. Off-line password guessing attacks have been used by both criminals and law enforcement and digital forensics practitioners to enable access to password-protected data (e.g. on smart phones and portable devices based on RIM Black Berry and Apple iOS platforms).

The rest of the paper is structured as follows. Section 2 briefly describes the Chao’s smartcard-based user authentication scheme [16], and Section 3 outlines our attacks. The last section concludes the paper.

## 2 Review of Chao’s smartcard-based user authentication scheme

The Chao’s scheme consists of four phases: registration phase, login phase, verification phase and password change phase, and the notations used are listed in Table 1.

<table>
<thead>
<tr>
<th>Table 1: Notations used in Chao’s authentication scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Notations</strong></td>
</tr>
<tr>
<td>$U_i$</td>
</tr>
<tr>
<td>$ID_i$</td>
</tr>
<tr>
<td>$PW_i$</td>
</tr>
<tr>
<td>$S$</td>
</tr>
<tr>
<td>$x$</td>
</tr>
<tr>
<td>$h(·)$</td>
</tr>
<tr>
<td>$∥$</td>
</tr>
<tr>
<td>$⊕$</td>
</tr>
<tr>
<td>$T_i$</td>
</tr>
<tr>
<td>$ΔT_i$</td>
</tr>
</tbody>
</table>

This phase is executed between user $U_i$ and the remote server $S$, and consists of the following steps:

**Step 1.** $U_i$ chooses an identity-password pair $(ID_i, PW_i)$ and then sends it to $S$ through a secure channel.

**Step 2.** On receiving $(ID_i, PW_i)$, $S$ checks the identity $ID_i$ of $U_i$, selects a random number $r_i$ and computes $K_i = h(x∥r_i)⊕h(PW_i)$ and $L_i = h(ID_i∥h(x∥r_i))$.

**Step 3.** $S$ issues a smartcard and writes the parameters $(K_i, L_i, h(·))$ into it. Then $S$ sent the smartcard to $U_i$ through a secure channel.

### 2.2 Login phase

In order to login to the remote server $S$, $U_i$ inserts his smartcard into a card reader and inputs $ID_i$ and $PW_i$, then the smartcard performs the followings:

**Step 1.** The smartcard computes $h(x∥r_i) = K_i ⊕ h(PW_i)$ and $L_i = h(ID_i∥h(x∥r_i))$, and compares $L_i$ with $L_i$ and continues to the next step if they are equal, otherwise rejects the login request.

**Step 2.** The smartcard then computes $M_i = ID_i ⊕ h(x∥r_i)$ and $CID_i = h(ID_i∥T_i)$, and sends the login message $(CID_i, M_i, T_i)$ to $S$ through an open channel, where $T_i$ is the current timestamp of $U_i$.

### 2.3 Verification phase

Assume that $S$ received the message $(CID_i, M_i, T_i)$ at time $T_i$ and then $S$ does the followings:

**Step 1.** $S$ checks whether $T_i′ − T_i ≤ ΔT_i$ holds, if not, $S$ rejects $U_i$’s login request. Otherwise, $S$ proceeds to the next step.

**Step 2.** $S$ computes $N_i = h(x∥r_i)$, $ID_i′ = M_i ⊕ N_i ⊕ T_i$ and $CID_i′ = h(ID_i∥T_i)$. $S$ checks whether $CID_i′ = CID_i$ holds and terminates the login request if they are not equal. Otherwise, $S$ computes $a = h(T_S∥ID_i∥N_i)$ and sends the message $(a, T_i)$ to $U_i$, where $T_S$ is the current timestamp of $S$.

**Step 3.** Suppose that $U_i$ receives $(a, T_i)$ at time $T_i$. Now $U_i$ computes $a′ = h(T_S∥ID_i∥h(x∥r_i))$ and authenticates $S$ if both of the conditions $T_S − T_i ≤ ΔT_S$ and $a′ = a$ hold. $U_i$ terminates the login request if either of the above fails.

### 2.4 Password change phase

This phase allows $U_i$ to change his old password $PW_i$ to a new password $PW_i′$ with the following operations:
This section demonstrated that Chao’s authentication scheme [16] is vulnerable to insider attack, user masquerade attack, server masquerade attack and off-line password guessing attack, as well as it fails to achieve users’ anonymity. Before introducing the proposed attacks, we describe the following widely used assumptions about the power of an adversary $\mathcal{A}$ [10, 11, 15, 18, 22, 28, 29].

(A1) $\mathcal{A}$ can sniff the communication media through which $U_i$ and $S$ communicate with each other i.e., $\mathcal{A}$ can intercept, block, inject, remove, or modify, any messages transmitted in the media.

(A2) $\mathcal{A}$ may either (a) steal user’s smartcard and extract the stored secrets by monitoring the timing information, power consumption and reverse engineering techniques as mentioned in [25–27] and guess the user’s password in off-line manner using the secrets extracted from the smartcard; or (b) obtain a user’s password directly by some means. However, the adversary is not allowed to do both (a) and (b) as having the smartcard and knowing the password would be trivial to impersonate the legitimate user.

3.1 Users’ anonymity problem

In recent years, many dynamic identity-based remote login schemes [6, 16–21] have been proposed to provide mutual authentication between the user and the remote server. In any dynamic identity-based remote login scheme, users’ anonymity [6, 7, 22] is an important security requirement. Now, we show that Chao’s scheme [16] fails to achieve the same as follows:

(a) $\mathcal{A}$ intercepts a login message $(CID_i, M_i, T_i)$ of $U_i$ of a previous session, where $M_i = ID_i \oplus h(x || r_i) \oplus T_i$, $CID_i = h(ID_i || T_i)$ and $T_i$ is the current timestamp.

(b) $\mathcal{A}$ guesses an identity $ID_i^*$ and computes $CID_i^* = h(ID_i^* || T_i)$.

(c) $\mathcal{A}$ verifies the correctness of $ID_i^*$ by checking whether the computed $CID_i^*$ and the intercepted $CID_i$ are equal.

(d) $\mathcal{A}$ repeats the steps (b) and (c) until it finds the exact identity $ID_i$ of $U_i$.

The adversary $\mathcal{A}$ can easily guess the identity $ID_i$ of $U_i$ by checking all possible identities from the search space $\mathcal{D}_{ID}$, where $|\cdot|$ indicates the cardinality of $\mathcal{D}_{ID}$. The running time of the aforementioned procedure is $O(|\mathcal{D}_{ID}|) \times (T_c + T_b)$, where $T_c$ and $T_b$ represents the execution time of concatenation and hash operations, respectively. It can be noted that for easy memorization, user generally chooses his identity with low intensity value from the set $\mathcal{D}_{ID}$ having small number of elements. Since $\mathcal{D}_{ID}$ is not large enough in practice, for example, $|\mathcal{D}_{ID}| \leq 10^{-6}$ [30–33] and the time complexities $T_c$ and $T_b$ are also negligible, thus $\mathcal{A}$ can complete the above procedure in polynomial time.

3.2 User masquerade attack

We now demonstrate that Chao’s scheme [16] is not secure against user masquerade attack.

(a) $\mathcal{A}$ monitors the communication channel and intercepts a login message $(CID_i, M_i, T_i)$ in a session.

(b) $\mathcal{A}$ finds the exact identity $ID_i$ of $U_i$ by executing steps discussed in section 3.1.

(c) $\mathcal{A}$ selects a valid timestamp $T_i^*$ (> $T_i$), computes $M_i^* = M_i \oplus T_i \oplus T_i^*$, $ID_i = h(ID_i || T_i^*)$ and then sends the forged message $(CID_i^*, M_i^*, T_i^*)$ to $S$ for login operation.

(d) On receiving $(CID_i^*, M_i^*, T_i^*)$, $S$ will confirm that the timestamp validity condition $T_i^* - T_i^* \leq \Delta T_i^*$ is correct, and computes $N_i^* = h(x || r_i)$, $ID_i = M_i^* \oplus N_i \oplus T_i^*$, $CID_i^* = h(ID_i || T_i^*)$ after confirming that $CID_i^* = CID_i$. With these successful verifications, $S$ accepts the forged login request and allows $\mathcal{A}$ to login to $S$. Thus, $\mathcal{A}$ impersonates the valid user $U_i$.

3.3 Server masquerade attack

This section demonstrated that Chao’s user scheme [16] is vulnerable to server masquerade attack.

(a) $\mathcal{A}$ intercepts $U_i$’s login message $(CID_i, M_i, T_i)$ of previous session.

(b) $\mathcal{A}$ finds the exact identity $ID_i$ of $U_i$ by executing steps discussed in section 3.1.

(c) $\mathcal{A}$ computes $h(x || r_i) = M_i \oplus ID_i \oplus T_i$, selects a timestamp $T_i^*$ (> $T_i$), computes a fabricated message $(a^*, T_i^*)$ and sends it to $U_i$, where $a^* = h(T_i^* || ID_i || h(x || r_i))$.

(d) Upon receiving the message $(a^*, T_i^*)$, $U_i$ found that both the conditions $T_i^* - T_i^* \leq \Delta T_i^*$ and $a^* = a^*$ are satisfied, where $a^* = h(T_i^* || ID_i || h(x || r_i))$ is computed by $U_i$. Therefore, $\mathcal{A}$ get able to trick the legitimate user $U_i$ to believe that $\mathcal{A}$ is legal server $S$ not an adversary.
3.4 Off-line password guessing attack

Assume that if the smartcard of $U_i$ is lost/stolen and it is in the physical possession of $\mathcal{A}$, who then extracts the original contents $(K_i, L_i, h(\cdot))$ by monitoring their timing information [25], power consumption and reverse engineering techniques [26, 27], where $K_i = h(x \parallel r_i) \oplus h(PW_i)$ and $L_i = h(ID_i \parallel h(x \parallel r_i))$. Also we suppose that $\mathcal{A}$ monitors the communication channel and recovers $U_i$’s valid login message $(CID_i, M_i, T_i)$ of a session, where $M_i = ID_i \oplus h(x \parallel r_i) \oplus T_i$, $CID_i = h(ID_i \parallel T_i)$ and $T_i$ is the timestamp. In order to launch an off-line password guessing attack on the stolen smartcard, $\mathcal{A}$ executes the following operations:

(a) $\mathcal{A}$ finds the exact identity $ID_i$ of $U_i$ and $h(x \parallel r_i)$ from the intercepted message $(CID_i, M_i, T_i)$ by executing the steps discussed in section 3.3.

(b) $\mathcal{A}$ computes $X_i = K_i \oplus h(x \parallel r_i) = h(PW_i)$.

(c) $\mathcal{A}$ guesses a $PW_i^*$ and computes $X_i^* = h(PW_i^*)$.

(d) $\mathcal{A}$ verifies the correctness of guessed $PW_i^*$ by checking whether $X_i^*$ and $X_i$ are equal.

(e) $\mathcal{A}$ repeats the steps (c) and (d) until to have the exact password $PW_i$ of $U_i$.

The running time of the above password guessing attack is $O(|\mathcal{D}_{ID}| \times (T_e + T_h) + O(|\mathcal{D}_{PW}|) \times (T_e + T_h + T_r))$, where $T_r$ represents the execution time of bit-wise XOR operation. As discussed earlier in section 3.1, the search spaces $\mathcal{D}_{ID}$ and $\mathcal{D}_{PW}$ are unlikely to be large enough (for example, $|\mathcal{D}_{ID}| \leq 10^{-6}$ and $|\mathcal{D}_{PW}| \leq 10^{-6}$ [30–33]), and the time complexities $T_e$, $T_h$ and $T_r$ all can be executed with negligible amount of time, thus the polynomial time-bounded adversary $\mathcal{A}$ can find the exact password $PW_i$ of $U_i$ easily.

3.5 Insider attack

Studies have demonstrated that users tend to use the same password for different applications [4, 19]. If the adversary, $\mathcal{A}$, is a malicious insider of the remote server $S$ and has learned $U_i$’s password (a trivial exercise as $U_i$ sends his $(ID_i, PW_i)$ in plaintext form to $S$ during the registration phase of Chao’s scheme [16]), $\mathcal{A}$ may try to masquerade the user $U_i$ using the password $PW_i$ to access other servers.

4 Conclusion

We examined the identity-based smartcard-based remote password authentication scheme of Chao (2012), and demonstrated that the scheme is susceptible to common attacks, namely user masquerade attack, server masquerade attack, insider attack and off-line password guessing attack.

Acknowledgments

This research work is supported by the Department of Science and Technology (DST), Govt. of India under the INSPIRE fellowship Ph.D program (Grant No. IF10247) and the Department of Information Technology (DIT), Ministry of Communication and Information Technology, Govt. of India under the Information Security Education and Awareness (ISEA) program (Project No. MlIT(2)/2006-08/189/CSE). The authors would also like to express their gratitude and heartiest thanks to the Department of Computer Science and Engineering, Indian School of Mines, Dhanbad-826004, India, for providing their research support, as without such help this work could not be carried out.

References

SK Hafizul Islam completed his Ph.D in Computer Science and Engineering from Indian School of Mines, Dhanbad, India, under the prestigious INSPIRE Fellowship Ph.D Program (funded by DST, Govt. of India) and Information Security Education and Awareness (ISEA) program (funded by Department of Information Technology (DIT), Ministry of Communication and Information Technology, Govt. of India, No. MIT (2)/2006-08/189/CSE). Dr. Islam received his B.Sc (Hons.) in Mathematics and M.Sc in Applied Mathematics from Vidyasagar University, West Bengal, India in 2004 and 2006, and M.Tech from Indian School of Mines, Dhanbad in 2009, respectively. Dr. Islam is currently holding the position of Assistant Professor in the Department of Computer Science & Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333031, India. His research interest includes Cryptography, Network/Information Security and Computer Networks.

G. P. Biswas received B.Sc (Engg.) and M.Sc (Engg.) degrees in Electrical & Electronics Engineering and Computer Science & Engineering, respectively. He completed his PhD degree in Computer Science & Engineering from Indian Institute of Technology, Kharagpur, India. He is currently working as a Professor in the Department of Computer Science & Engineering, Indian school of Mines, Dhanbad, Jharkhand, India. His main research interests include Cryptography, Computer Network and Security, Cellular Automata, VLSI Design.