Please cite this paper as: Ping Wang, Zijian Zhang, Ding Wang.Revisiting Anonymous Two-Factor Authentication Schemes for Multi-Server Environment. Proc. of the 20th International Conference on Information and Communications Security (ICICS 2018), Springer. Accepted, to appear, 2018.

Revisiting Anonymous Two-Factor Authentication Schemes for Multi-Server Environment

Ping Wang[1,2,3,4], Zijian Zhang[1,3] and Ding Wang[2⋆]

[1] School of Electronic and Computer Engineering, Peking University Shenzhen Graduate School, Shenzhen 518055, China
[2] School of EECS, Peking University, Beijing 100871, China
[3] National Engineering Research Center for Software Engineering, Beijing, China
[4] School of Software and Microelectronics, Peking University, Beijing 100260, China
{pwang, zhangzj, wangdingg}@pku.edu.cn

Abstract. Revealing the security flaws of existing cryptographic protocols is the key to understanding how to achieve better security. At ICICS'17, Xu *et al.* proposed an efficient two-factor authentication scheme for multi-server environment to cope with the vulnerabilities in Amin *et al.*'s scheme. However, in this paper, we reveal that Xu's new scheme actually is as vulnerable as Amin *et al.*'s scheme: anyone can impersonate any legitimate user. At FC'17, Wu *et al.* also developed an improvement over Irshad *et al.*'s scheme and this improved scheme is alleged to be practical and have a number of appealing merits. Yet, Wu *et al.*'s scheme still fails to achieve truly two-factor security (which is the most important goal of a two-factor scheme), and the leakage of a session-specific parameter will lead to the leakage of the user's long-term secret key.

Besides security, efficiency is another great concern. Recently, Leu-Hsieh showed that Lee *et al.*'s two-factor scheme fails to achieve truly two-factor security, and further suggested an enhanced anonymous scheme which is claimed to be robust against various attacks, while only using lightweight symmetric-key techniques. In this work, we show that Leu-Hsieh's enhanced scheme still fails to achieve truly two-factor security once again. Moreover, it cannot preserve user privacy. Our results invalidate any use of these three schemes for practical applications without further improvement, and underscore some new challenges (e.g., attacks arising from the leakage of session-specific parameters and from malicious insiders) in designing practical password authentication schemes.

Keywords: Password authentication; User anonymity; Smart card loss attack; Truly two-factor security.

1 Introduction

User authentication plays a crucial part in ensuring that resources and services at the remote server can only be accessed by legitimate parties. In 1991, Chang *et al.* [5] suggested the first two-factor authentication scheme based on passwords and smart cards, and this influential study has given rise to a series of enhanced

⋆ Corresponding author.

Please cite this paper as: Ping Wang, Zijian Zhang, Ding Wang.Revisiting Anonymous Two-Factor Authentication Schemes for Multi-Server Environment. Proc. of the 20th International Conference on Information and Communications Security (ICICS 2018), Springer. Accepted, to appear, 2018.

proposals with each diversified in aspects of usability [25], security [16] efficiency [10] and anonymity [22].

However, most of these schemes are designed for the single-server architecture, which means that the user needs to memorize n pairs of identity and password to login n different service servers. As the number of services increases rapidly, e.g., a very recent survey [14] finds that common users generally have 25∼67 such pairs. This is a great burden for use to maintain (memorize) such an amount of password pairs. Accordingly, a number of two-factor authentication protocols for multi-server architecture has been developed [15, 21, 24].

In a two-factor scheme[1] for multi-server architecture, there are three participants (i.e. a set of users, a control server CS and a set of service servers) involved. User U can login any service server under the same control server by using the same (identity, password)-pair. User U holds a memorable password and a smart card stored with some initial security parameters; The servers (including CS and service server S) only need to keep some secret key material of the system (but not the user). Since there is no need to keep a table with password-related verification information on the server side, the server is free from the threat of password dataset leaks and ameliorated from the burden of maintaining a large password dataset. This feature makes this type of schemes rather desirable, considering the incessant leakages of password databases from large websites [1].

The most important security goal of a two-factor authentication scheme is the so-called "two-factor security" [16]. This security concept essentially means that only the user that has the smart card as well as knows the correct password can be verified by the server. Nevertheless, past research [6, 18, 19, 22] have, again and again, proved that designing a two-factor authentication scheme with "two-factor security" for single-server architecture is a hard task, and the design of a truly two-factor scheme for multi-server architecture can only be harder.

In 2017, Amin *et al.* [4] developed an anonymous two-factor authentication scheme relying on the intractability of large integer factoring problem (i.e., RSA), and stated that their scheme is able to support "two-factor security" under the hypothesis that smart cards can be tampered. Later on, Xu *et al.* [24] found that Amin *et al.*'s scheme cannot resist against user impersonation attack if the parameters kept in the smart cards can be extracted, invalidating Amin *et al.*'s claim of ensuring "two-factor security". Accordingly, Xu *et al.* [24] further proposed a new scheme based on the same cryptographic primitive (i.e., RSA) at ICICS'17. In addition, their scheme was "proved secure" in the random oracle model. Surprisingly, we find that Xu *et al.*'s scheme [24] is subject to a damaging security hole: anyone can impersonate any legitimate user.

At FC'17, Wu *et al.* [21] demonstrated that various security drawbacks existed in both Irshad et al.'s [7] and Zhu's [26] schemes. More specifically, Irshad *et al.*'s scheme is vulnerable to stolen-verifier attack and insider attack, and provides no user anonymity; Zhu's scheme suffers from insider attack, provides no user

[1] As with [19, 25], in this work we mainly consider the most typical kind of two-factor schemes that are composed of password and smart card.

Please cite this paper as: Ping Wang, Zijian Zhang, Ding Wang.Revisiting Anonymous Two-Factor Authentication Schemes for Multi-Server Environment. Proc. of the 20th International Conference on Information and Communications Security (ICICS 2018), Springer. Accepted, to appear, 2018.

anonymity, and has the de-synchronization problem in case the attacker simply modify the third message flow. Wu *et al.* [21] also put forward an improved scheme and argued that their scheme is robust under the condition that the sensitive data in smart card has been revealed by the attacker. It should be noted that, recent rapid developments in side-channel attacks have proved that the sensitive information stored in general commercial smart cards could be extracted by power analysis [13] or reverse engineering [3]. Based on a weak yet realistic assumption, Wu *et al.*'s scheme [21] appears very practical.

However, as we will show, this scheme is prone to a much more serious problem (i.e., no truly two-factor security) than the original schemes (i.e., Irshad et al.'s [7] and Zhu's [26] schemes). Besides, Wu *et al.*'s scheme will leak the user's long-term secret key once a session-specific parameter is leaked. This is rather undesirable, because session-specific data is often less well protected than long-term keys, and the leakage of the former should not affect the latter. Our attack highlight the challenges arising from the leakage of session-specific data.

Besides robust security guarantees, protocol efficiency is an important concern due to the fact that users' devices are generally of resource-constrained nature. In 2011, Lee et al. [9] presented an anonymous two-factor authentication scheme. It is claimed to ensure user privacy and robust security while only requiring a few lightweight hash operations. In 2014, Leu-Hsieh [10] showed that an attacker can figure out the user's password once she has extracted data in a legal user's smart card. Thus, Lee et al.'s scheme fails to reach the goal of truly two-factor security. What's worse, even a legitimate yet curious user can impersonate other users by only obtaining sensitive information from her own smart card and intercepting some communication messages.

Leu-Hsieh [10] further suggested an improved scheme which is purported to mitigate the described attacks. Unlike their claims, we will show that Leu-Hsieh's enhanced scheme still cannot provide the essential goals of truly two-factor security and user anonymity. In addition, the important property of forward secrecy cannot be attained. We note that Maitra *et al.* [12] have also analyzed Leu-Hsieh's scheme and presented some attacks, but their attacks are different from ours. Besides, Maitra *et al.* [12] further gave an improved scheme, which suffers some critical issues as pointed out in [15].

2 Adversary models

Since a series of influential work [19, 23, 25], generally three assumptions are made about the attacker's capabilities against two-factor authentication.

Assumption 1. The malicious attacker $\mathcal{M}$ completely manipulates the public channel (e.g., eavesdrop, delete, insert, modify or block any transcripts).

Assumption 2. $\mathcal{M}$ can somehow obtain the victim's smart card and exploit side-channel attacks [3, 13] to extract sensitive data from the card memory.

Assumption 3. Users' passwords are selected from a very constrained space and the attacker $\mathcal{M}$ can brutal force it. To increase usability, most schemes (e.g., the ones in [16, 22, 25]) allow the users to choose passwords at their discretion during registration phase or password change phase. Generally, human beings are

Please cite this paper as: Ping Wang, Zijian Zhang, Ding Wang.Revisiting Anonymous Two-Factor Authentication Schemes for Multi-Server Environment. Proc. of the 20th International Conference on Information and Communications Security (ICICS 2018), Springer. Accepted, to appear, 2018.

only capable of memorizing 5∼7 different passwords, and tend to select popular passwords, use personal info to build passwords and reuse passwords. Therefore, user-chosen passwords follow the Zipf's law [17] and come from a small space.

Note that, if all *Assumptions* 2 and 3 hold at the same time, then the attacker (with no need of other abilities) is able to impersonate any victim user and can trivially breach any scheme. Thus, it is common practice to do *not* assume that the attacker acquires a victim user's both (all) authentication factors when analyzing security. [6, 11, 19, 22].

Also note that, an attacker might be an insider of the system, in this case it is practical for her to obtain both her own card and password. As shown in Section 5.2.3 of [18], such an attacker is really powerful and poses great threat to the security of the system. Overlooking the threats from this kind of attacker is likely to open large security loopholes. One can see that many previous password authentication schemes employing smart cards (e.g., [8, 20, 23]) fail to achieve "two-factor security" or user un-traceability when confronted with such a malicious insider. In this work, special attention are devoted to this kind of attacker and we show its perniciousness.

According to the abilities that are exploited by an attacker to launch a attack, four types of attackers can be further classified as follows:

(I) **Basic attacker**. This attacker is only based on Assumption 1.
(II) **Attacker with the target user's smart card**. This attacker rest on the Assumption 1 and 2.
(III) **Attacker with the target user's password**. This attacker rests on the Assumption 1 and 3.
(IV) **Attacker with her own smart card and password**. This attacker is based on the Assumption 1, 2 and 3, and she is a malicious insider.

It is evident that among the above four kinds of attackers, the *basic attacker* is with the least capabilities, and the three remaining attackers are all realistic according to the aforementioned discussions. Consequently, any scheme aiming for practical use shall be able to withstand these four attackers. All the three schemes examined in this work are claimed to be secure under the above three assumptions. Actually, as we will show, this is not the case.

3 Cryptanalysis of Xu et al.'s scheme

We first review Xu et al.'s scheme [24] proposed at ICICS'17, and then show that it is subject to a damaging security flaw: anyone can impersonate any legitimate user without guessing the victim's password or obtaining the victim's device.

3.1 A brief review of Xu et al.'s scheme

To be self-contained, here we sketch the two-factor authentication scheme put forward by Xu et al. [24] in 2017. Their scheme is composed of four phases (i.e., initialization, registration, login and authentication) and two activities (i.e., password change and revocation of lost smart card). For simplicity, the notations

Please cite this paper as: Ping Wang, Zijian Zhang, Ding Wang.Revisiting Anonymous Two-Factor Authentication Schemes for Multi-Server Environment. Proc. of the 20th International Conference on Information and Communications Security (ICICS 2018), Springer. Accepted, to appear, 2018.

Table 1. Notations and abbreviations

Symbol	Description	Symbol	Description
U_i	i^{th} user	S_j	j^{th} server
RC	the register center	S_x	the foreign server
S_y	the home server	k_{xy}	secret key shared by S_x and S_y
k_y	the secret key of S_y	$\mathcal{M}$	the malicious adversary
x/d	the secret key of RC	e	the public key of RC
ID_i	identity of U_i	PW_i	password of U_i
$\Rightarrow$	a secure channel	$\oplus$	bitwise XOR operation
$\rightarrow$	a common channel	$h(\cdot)$	one-way hash function

employed throughout this paper are listed in Table 1; For convince, we will comply with the abbreviations in Xu et al.'s scheme closely.

Server Registration Phase. This phase proceeds as follows:

Step 1. $S_j \Rightarrow RC$: $\{e_j, n_j, SID_j\}$. S_j computes $n_j = p_j \times q_j$, $\phi(n_j) = (p_j - 1)(q_j - 1)$ where both p and q are large prime numbers, then chooses a public key $e_j (1 < e_j < \phi(n_j))$ where $\gcd(\phi(n_j), e_j) = 1$, and computes $d_j \equiv e_j^{-1} \bmod \phi(n_j)$ as its private key.

Step 2. $RC \Rightarrow S_j$: $\{Cer_j\}$. RC computes selects $Cer_j = h(e_j \parallel SID_j \parallel n_j)^d$.

User Registration Phase. This phase proceeds as follows:

Step 1. $U_i \Rightarrow RC$: $\{ID_i\}$.

Step 2. $RC \Rightarrow S_j$: $\{d_i\}$. RC computes $d_i = h(ID_i)^d \bmod n_j$.

Login and authentication phase. This phase proceeds as follows:

Step 1. $U_i \rightarrow S_j$: a random number T_i.

Step 2. $S_j \rightarrow U_i$: $\{e_j, n_j, Cer_j, A_j\}$ where $A_j = h(T_i)^{d_j}$.

Step 3. $U_i \rightarrow S_j$: $\{PID_i, R_i, S_i, x\}$. If $Cer_j^e \bmod n_j$ equals $h(SID_j \parallel e_j \parallel n_j)$ and $A_j^{e_j}$ equals $h(T_i)$, U_i computes $PID_i = (ID_i \oplus a_i \parallel a_i)^{e_j} \bmod n_j$, $R_i = h(PID_i)^r \bmod n_j$, $x = h(m, R_i)$ and $Si = d_i^{r-x}$ where a_i, r, m are three random numbers.

Step 4. S_j computes $S_i^{e_j} = h(ID_i)^{r-x}$, $PID_i^{d_j} \bmod n_j = ID_i \oplus a_i \parallel a_i$, $ID_i' = ID_i \oplus a_i \parallel a_i$. If $S_i^{e_j} h(ID_i')^x$ equals Ri, then S_j authenticates U_i.

3.2 Flaws in Xu et al.'s scheme

We now reveal that Xu et al.'s scheme [24] is prone to user impersonation attack and has poor repairability, which makes this scheme unpractical for real use.

User impersonation attack. Xu et al. claimed that their "proposed scheme can provide proper mutual authentication", but we show this is not the case. The following procedure describes how anyone can impersonate any legitimate user without guessing password or accessing the victim's device:

Step 1. $\mathcal{M}$ chooses a random number $T_i \in_R (1, n_j]$;

Step 2. $\mathcal{M}$ receives $\{e_j, n_j, Cer_j, A_j\}$ that comes from the service server S_j;

Step 3. $\mathcal{M}$ chooses a random number $X \in_R (1, n_j]$;

Please cite this paper as: Ping Wang, Zijian Zhang, Ding Wang.Revisiting Anonymous Two-Factor Authentication Schemes for Multi-Server Environment. Proc. of the 20th International Conference on Information and Communications Security (ICICS 2018), Springer. Accepted, to appear, 2018.

Step 4. $\mathcal{M}$ sets $S_i = X$, $R_i = X^{e_j} h(ID_i)^X$;
Step 5. $\mathcal{M} \rightarrow S_j$: $\{PID_i, R_i, S_i, x = X\}$, where PID_i is intercepted from the open channel;

Note that the above attack will succeed, because $\{PID_i, R_i, S_i, x = X\}$ will be accepted by the the service server S_j. More specifically, according to attack Step 4, we have $S_i^{e_j} h(ID_i)^x = X^{e_j} h(ID_i)^X$, which equals R_i and passes Step 4 of login phase. This demonstrates that even a Type-I attacker (see Sec. 2) can completely break the scheme.

Poor repairability. In Xu *et al.*'s scheme, there should be times that a user suspects (or realizes) that her smart card might be power analysed and the secret $d_i = h(ID_i)^d \bmod n$ has been leaked. However, even if U_i has detected this abnormality and changes her password to a new one, no means can be employed to deter $\mathcal{M}$ from using the master secret d_i to login the server S_j. In other words, U_i cannot be easily repaired [19]. More detailedly, since $d_i = h(ID_i)^d \bmod n$ is uniquely defined by U_i's identity ID_i and RC's long-term private key d, RC is unable to update d_i for U_i unless either ID_i or d is updated. Nevertheless, because d is usually utilized for all legitimate users of the entire system rather than only one user U_i, it would be irrational and inefficient to change d to restore the security of a single user, i.e. U_i. Furthermore, since ID_i is typically bound with U_i in many application systems, it is also unreasonable to change ID_i to address the problem. In summary, the repairability of Xu *et al.*'s scheme constitutes a realistic issue.

4 Cryptanalysis of Wu *et al.*'s scheme

Here we first review Wu *et al.*'s scheme [21]. This scheme is an improvement over existing schemes aims to attain user anonymity lacked in [7,26]. Wu *et al.*'s scheme can preserve user anonymity, however, we observe that it still remains feasible for an attacker to break the critical goal of "truly two-factor security". In addition, the scheme cannot provide sound repairability.

4.1 A brief review of Wu *et al.*'s scheme

Wu *et al.*'s scheme [21] is composed of four phases: initialization, registration, login and authentication, and one activity: password change. The notations and initial system parameters employed in Wu *et al.*'s scheme are same as employed in the scheme of Xu et al. (see Table 1).

Initialization phase. Let $k_{xy} (1 \leq x, y \leq n, x \neq y)$ be the common secret key of each pair of servers (S_x, S_y) $(x \neq y)$, and s be their common parameter, k_y be the secret key of S_y.

User Registration. This phase proceeds as follows:

Step 1. $U_i \Rightarrow S_y$: $\{ID_i, HPW_i\}$, where $HPW_i = h(PW_i \parallel b_i)$.
Step 2. $S_y \Rightarrow U_i$: $\{PID_i, B_1, B_2, s, h(\cdot)\}$. S_y selects PID_i, then computes: $B_{01} = h(PID_i \parallel k_y \parallel ID_{S_y})$, $B_1 = B_0 \oplus HPW_i$, $B_{02} = h(ID_i \parallel k_y \parallel ID_{S_y})$ and $B_2 = B_{02} \oplus h(ID_i \parallel HPW_i)$, and stores ID_i.

Please cite this paper as: Ping Wang, Zijian Zhang, Ding Wang.Revisiting Anonymous Two-Factor Authentication Schemes for Multi-Server Environment. Proc. of the 20th International Conference on Information and Communications Security (ICICS 2018), Springer. Accepted, to appear, 2018.

Step 3. U_i inputs $(PID_i, B_1, B_2, B_3, s, h(\cdot))$ into mobile device, where $B_3 = b_i \oplus h(ID_i \parallel PW_i)$.

Login and authentication phase. This phase proceeds as follows:

Step 1. $U_i \rightarrow S_x$: $M_1 = \{PID_i, C_1, C_2, C_3, C_5, SID_j, ID_{S_y}\}$. U_i inputs ID_i and PW_i, then the device calculates $b_i = B_3 \oplus h(ID_i \parallel PW_i)$ and $HPW_i = h(PW_i \parallel b_i)$, $C_1 = T_{r_U}(s)$, $C_2 = B_1 \oplus HPW_i \oplus N_U$, $C_3 = h(N_U) \oplus ID_i$, $C_4 = B_2 \oplus h(ID_i \parallel HPW_i)$ and $C_5 = h(C_1 \parallel N_U \parallel C_4)$, where r_U and N_U are two random nonces.

Step 2. $S_x \rightarrow S_y$: $M_2 = \{PID_i, C_1, C_2, C_3, C_5, C_6, C_7, SID_j\}$. S_x computes $C_6 = T_{r_{S_x}}(s)$ and $C_7 = h(C_6 \parallel k_{xy} \parallel SID_j)$, where r_{S_x} is a nonce.

Step 3. $S_y \rightarrow S_x$: $M_3 = \{C_8, C_9, C_{10}, C_{11}\}$. S_y computes: $N_U = C_2 \oplus h(PID_i \parallel k_y \parallel ID_{S_y})$, $ID_i = C_3 \oplus h(N_U)$, checks the validity of ID_i, then computes $B_{02} = h(ID_i \parallel k_y \parallel ID_{S_y})$. If $C_5 == h(C_1 \parallel N_U \parallel B_{02})$ and $C_7 == h(C_6 \parallel k_{xy} \parallel SID_j)$, S_y generates PID_i^{new}, computes $C8 = h(SID_j \parallel k_{xy} \parallel C_1 \parallel C_6)$, $C_9 = h(ID_i \parallel N_U \parallel PID_i) \oplus PID_i^{new}$, $B_{01}^{new} = h(PID_i^{new} \parallel k_y \parallel ID_{S_y})$, $C_{10} = B_{01}^{new} \oplus h(PID_i^{new} \parallel N_U \parallel ID_i)$ and $C_{11} = h(PID_i^{new} \parallel B_{01}^{new} \parallel N_U \parallel C_1 \parallel B_{02} \parallel C_6 \parallel SID_j \parallel ID_{S_y})$.

Step 4. $S_x \rightarrow U_i$: $M_4 = \{C_6, C_9, C_{10}, C_{11}, C_{12}\}$. If $C_8 == h(SID_j \| k_{xy} \| C_1 \| C_6)$, S_x computes $sk_{S_x} = T_{r_{S_x}}(C_1)$ and $C_{12} = h(C_1 \| C_6 \| C_9 \| C_{10} \| sk_{S_x})$.

Step 5. The mobile device computes $sk_U = T_{r_U}(C_6)$. If $C_{12} == h(C_1 \parallel C_6 \parallel C_9 \parallel C_{10} \parallel sk_U)$. U_i computes $PID_i^{new} = C_9 \oplus h(ID_i \parallel N_U \parallel PID_i)$, and $B_{01}^{new} = C_{10} \oplus h(PID_i^{new} \parallel N_U \parallel ID_i)$. If $C_{11} == h(PID_i^{new} \parallel B_{01}^{new} \parallel N_U \parallel C_1 \parallel C_4 \parallel C_6 \parallel SID_j \parallel ID_{S_y})$. U_i replaces (B_1, PID_i) with (B_1^{new}, PID_i^{new}) where $B_1^{new} = B_{01}^{new} \oplus HPW_i$.

4.2 Flaws in Wu *et al.*'s scheme

We now show the flaws of Wu *et al.*'s scheme [21]. Recall that the three assumptions listed in Sec. 2 are also explicitly made when Wu *et al.* analyzing Irshad et al.'s [7] and Zhu's [26] schemes.

Smart card loss attack. Based on Wu et al.'s own security assumptions (i.e., the three ones in Sec. 2), we now cryptanalyze the security provisions of their scheme. More specifically, in what follows we assume that $\mathcal{M}$ can extract the private data $\{B_1, B_2, B_3, h(\cdot)\}$ kept in U_i's smart card, and $\mathcal{M}$ can also eavesdrop the messages $\{PID_i, C_1, C_2, C_3, C_5, SID_j, ID_{S_y}\}$ exchanged between the parties. $\mathcal{M}$ can figure out U_i's password PW_i as follows:

Step 1. Guesses the value of ID_i to be ID_i^* from dictionary space $\mathcal{D}_{id}$ and the value of PW_i to be PW_i^* from dictionary space $\mathcal{D}_{pw}$;

Step 2. Computes $b_i^* = B_3 \oplus h(ID_i^*)^{PW_i^*}$, where B_3 is revealed from U_i's card;

Step 3. Computes $N_u^* = C_2^* \oplus B_1 \oplus h(PW_i \| b_i^*)$, where C_2 is intercepted from the channel and B_1 is revealed from U_i's card;

Step 4. Computes $C_3^* = h(N_u^*) \oplus ID_i^*$;

Step 5. Verifies the correctness of (ID_i^*, PW_i^*) by checking if C_3^* equals the intercepted C_3;

Step 6. Repeats Step 1∼5 of this procedure until the right value of (ID_i^*, PW_i^*) is found.

The time complexity of the attack is $\mathcal{O}(|\mathcal{D}_{id}| * |\mathcal{D}_{pw}| * 3T_H)$, where T_H is the running time for Hash operation. Recently, it has been found that user-chosen password follow the Zipf's law and the dictionary size is very restricted, e.g., $|\mathcal{D}_{id}| \leq |\mathcal{D}_{pw}| \leq 10^6$ [17]. Further, regarding the timings in Table 5 of [19], $\mathcal{A}$ may figure out the password within 24.6 days on a common PC, or costs \$30.36 and spends 16.37 hours by using the Amazon EC2 `C4.4X-large` cloud computing service [2]. The above attack means that, once the smart card factor is breached, then the password factor will also be compromised. *This indicates that truly two-factor security cannot be achieved in Wu et al.'s scheme.*

Temporary information leakage attack. As session-specific information are generally of large volume and deemed less sensitive than long-term secret keys, the former will be much less well protected than the latter and thus more easily leaked (e.g., through improper erasing, memory leakage or even poor implementations). Therefore, it is desirable that the security impact of the leakage of such session-specific information can be limited to just session-specific secret keys, but not the long-term secret keys.

However, as we show in the following, in Wu et al.'s scheme [21], the leakage of session-specific information will make the long-term secret key dangerous:

Step 1. $\mathcal{M}$ somehow obtains the session-specific info N_u during one session;
Step 2. Computes $B_{01} = C_2 \oplus \oplus N_u = h(PID_i \parallel k_y \parallel ID_{S_y})$.

Note that, $B_{01} = h(PID_i \parallel k_y \parallel ID_{S_y})$ is just U_i's long-term authenticator. After obtaining B_{01}, $\mathcal{M}$ can further guess U_i's passwords (and impersonate U_i):

Step 1. Computes $ID_i = C_3 \oplus h(N_u)$, where C_3 is get from the open channel;
Step 2. Guesses the value of PW_i to be PW_i^* from space $\mathcal{D}_{pw}$;
Step 3. Computes $C_2^* = B_{01} \oplus h(PW_i^* \| b_i^*) \oplus N_u$, where B_{01} is obtained as shown above;
Step 4. Verifies whether PW_i^* is correct by comparing if C_2^* equals the intercepted C_2;
Step 5. Repeats Step 1∼4 until the right value of PW_i^* is found.

The attacking time complexity is $\mathcal{O}(|\mathcal{D}_{pw}| * 2T_H)$, which can be completed in 1.39s on a common PC according to the timings that $T_H \approx 0.693\mu s$ (see Table 5 of [19]). In other words, the leakage of session-specific information will lead to the leakage of user identity and passwords, which is rather dangerous.

5 Cryptanalysis of Leu-Hsieh's scheme

In 2014, Leu-Hsieh [10] pointed out that Lee *et al.*'s scheme [9] actually fails to attain truly two-factor security. In order to overcome the revealed pitfalls, Leu-Hsieh [10] suggested an improved scheme. However, contrary to their claims, we show that it still has serval serious loopholes being overlooked in the following.

Please cite this paper as: Ping Wang, Zijian Zhang, Ding Wang.Revisiting Anonymous Two-Factor Authentication Schemes for Multi-Server Environment. Proc. of the 20th International Conference on Information and Communications Security (ICICS 2018), Springer. Accepted, to appear, 2018.

5.1 Review of Leu-Hsieh's scheme

Due to space constraints, the details of the scheme are referred to [10].

5.2 Flaws in Leu-Hsieh's scheme

We now point out the flaws of Leu-Hsieh's dynamic-ID based scheme. Note that the three assumptions about an adversary's capabilities presented in Section 2 are also clearly stated in Leu-Hsieh's work [10] as they analyze Lee *et al.*'s scheme [9] and their owns. However, we find Leu-Hsieh's scheme fails to achieve three important goals: (1) User anonymity; (3) Resistance against smart card loss attack; and (3) Forward secrecy.

No user anonymity. With the concern of user privacy rising rapidly nowadays, user anonymity is becoming a primary feature to be considered in the design of authentication protocols, especially in wireless environments. In Leu-Hsieh's scheme, the exchanged messages are different in every session due to the use of fresh random nonces and user identity is dynamic in every session by hiding the true identity ID_i into shadow identities CID_i. In this way, anonymity service is claimed to be provided in [10] by arguing that an attacker $\mathcal{M}$ "cannot distinguish between different sessions corresponding to a certain user and cannot obtain any clue to the real identity." However, Leu-Hsieh's scheme fails to consider that the attacker $\mathcal{M}$ may be a malicious insider (i.e., a legitimate but malicious user – a type IV attacker, see Sec. 2). In the following we show that such a type IV attacker $\mathcal{M}$ is able to breach U_i's untraceability as follows:

Step 1. $\mathcal{M}$ eavesdrops a login request $\{P_{ij}, N_i\}$ sent by U_i;
Step 2. $\mathcal{M}$ calculates $T_i = P_{ij} \oplus h(h(y)\|N_i\|SID_j)$, where $h(y)$ is shared among all users and service serviers.

Note that, $T_i = h(R_i\|x)$ is specific to U_i and static in all of user U_i's login sessions, and thus it can be used to link the different session participated by U_i, breaching the user untraceability.

The above procedure illustrates that, a type IV attacker (see Section 2) is capable of disclosing the activity of any legitimate user in the system without the sensitive information from user's smart card. Instead, $\mathcal{M}$ only needs the sensitive information from her own knowledge. This is a much weaker condition as compared with the condition that $\mathcal{M}$ needs the sensitive information from U_i's smart card. This is contrary to Leu-Hsieh's claim that $\mathcal{M}$ "cannot obtain any clue to the real identity." Thus, their scheme is incapable of protecting user anonymity and is not a true dynamic-ID based scheme. Our attack highlights the seriousness of threat arising from malicious insiders.

Smart card loss attack I. We show that once $\mathcal{M}$ obtains U_i's smart card, a Type-I attacker $\mathcal{M}$ can obtain U_i's password PW_i as follows:

Step 1. $\mathcal{M}$ extracts $\{V_i, H_i, h(\cdot)\}$ from U_i's smart card by side channel attacks [3, 13].

Step 2. $\mathcal{M}$ picks a candidate PW_i^* from the password dictionary $\mathcal{D}_{pw}$, and a candidate ID_i^* from the identity dictionary $\mathcal{D}_{id}$.
Step 3. $\mathcal{M}$ computes $T_i^* = V_i \oplus h(ID_i^* \| h(b \| PW_i^*))$;
Step 4. $\mathcal{M}$ computes $H_i^* = h(T_i^*)$;
Step 5. $\mathcal{M}$ examines the validity of PW_i^* by comparing if the computed H_i^* is equal to H_i which is extracted from the card memory.
Step 6. $\mathcal{M}$ goes to Step 2 until the right PW_i is obtained.

The time complexity of offline guessing U_i's password is $\mathcal{O}(|\mathcal{D}_{id}| * |\mathcal{D}_{pw}| * (2T_H + T_X))$. Based on the results in [19], this attack is able to be carried out in a few days on a common computer. This attack has been given extensive attention is the literature [18, 19]. As shown in [15], Maitra *et al.*'s scheme [12], an improvement of Leu-Hsieh's scheme [10], suffers exactly the same issue.

Smart card loss attack II. We further show that a Type-I attacker $\mathcal{M}$ can obtain U_i's password PW_i via another attacking procedure as follows:

Step 1. $\mathcal{M}$ extracts $\{B_i, Z_i, V_i, b, h(\cdot)\}$ from U_i's smart card by side channel attacks [3, 13].
Step 2. $\mathcal{M}$ picks a candidate PW_i^* from the password dictionary $\mathcal{D}_{pw}$, and a candidate ID_i^* from the identity dictionary $\mathcal{D}_{id}$.
Step 3. $\mathcal{M}$ computes $R_i^* = Z_i \oplus ID_i^* \oplus h(b \| PW_i^*)$;
Step 4. $\mathcal{M}$ computes $O_i^* = h(b \| PW_i^*) \oplus ID_i^* \oplus R_i^*$;
Step 5. $\mathcal{M}$ computes $A_i^* = h(T_i \| h(y) \| N_i)$, where N_i is got from the open channel and $h(y)$ comes from a legitimate yet curious user/service server;
Step 6. $\mathcal{M}$ computes $Q_i^* = h(O_i^* \| A_i^* \| N_i)$;
Step 7. $\mathcal{M}$ examines the validity of PW_i^* by comparing if the computed Q_i^* is equal to Q_i which is intercepted from the open channel.
Step 8. $\mathcal{M}$ goes to Step 2 until the right PW_i is obtained.

The time complexity of the above procedure is $\mathcal{O}(|\mathcal{D}_{id}| * |\mathcal{D}_{pw}| * (4T_H + 3T_X))$. It can be carried out in a few days on a common computer according to the timings in [19]. Note that, our attack involves the parameter $h(y)$ but not $h(x \| y)$, which is different from Maitra et al.'s attack (see Sec. 6.3 of [12]). When compared with the above "smart card loss attack I", this attack is less effective as it requires that $\mathcal{M}$ colludes with a malicious insider. Still, this attack invalidates the claim of achieving truly two-factor security in [10].

No forward secrecy. When analyzing their scheme, Leu and Hsieh do not consider (mention) forward secrecy. We now show that this desirable property cannot be preserved: Supposing an attacker $\mathcal{M}$ manages to obtain the long-term keys $h(y)$ and $h(x \| y)$ from a compromised/malicious service server and eavesdropped the messages $\{CID_i, P_{ij}, Q_i, N_i, N_j\}$ exchanged during U_i and S authentication process from the public channel. For convenience of presentation, assume it is U_i's mth login. $\mathcal{M}$ can calculate U_i and S's session key during the jth communication as follows:

Please cite this paper as: Ping Wang, Zijian Zhang, Ding Wang.Revisiting Anonymous Two-Factor Authentication Schemes for Multi-Server Environment. Proc. of the 20th International Conference on Information and Communications Security (ICICS 2018), Springer. Accepted, to appear, 2018.

Step 1. $\mathcal{M}$ calculates $T_i = P_{ij} \oplus h(h(y)\|N_i\|SID_j)$, $A_i = h(T_i\|h(y)\|N_i))$, where $\{P_{ij}, N_i\}$ come from the open channel;

Step 2. $\mathcal{M}$ computes $h(b \oplus PW_i \oplus R_i) = CID_i \oplus h(T_i\|A_i\|N_i)$ and $O_i = h(h(b \oplus PW_i \oplus R_i)\|h(x\|y))$, where $\{CID_i, N_i\}$ is from the open channel;

Step 3. $\mathcal{M}$ calculates $SK^m = h(O_i\|N_i\|N_j\|A_i\|SID_j)$, where $\{N_i, N_j\}$ is from the open channel;

Once the session key SK^m is procured, the entire mth communication will be leaked to $\mathcal{M}$. Maitra *et al.*'s scheme [12] suffers exactly the same issue.

6 Conclusion

Considerable efforts have been spent on designing an efficient, secure and privacy-preserving two-factor authentication scheme for multi-server environments, yet this still remains an open challenge when assuming that smart cards can be extracted. Very recently, Xu *et al.*, Wu *et al.* and Leu-Hsieh made three new attempts. However, in this paper, through systematic evaluation we reveal that all of them are still subject to various serious defects. Most importantly, our results underscore some new challenges (e.g., attacks arising from the leakage of session-specific information and from malicious insiders) in devising a practical two-factor authentication scheme for multi-server environments.

Acknowledgment

We are grateful to the anonymous reviewers for their invaluable comments. This research was in part supported by the National Key Research and Development Plan under Grants Nos. 2016YFB0800600 and 2017YFB1200700, and by the National Natural Science Foundation of China (NSFC) under Grant No.61472016.

References

1. All Data Breach Sources (May 2018), https://breachalarm.com/all-sources
2. Amazon elastic compute cloud (Amazon EC2) (2018), `https://aws.amazon.com/ec2/pricing/`
3. Amiel, F., Feix, B., Villegas, K.: Power analysis for secret recovering and reverse engineering of public key algorithms. In: Proc. SAC 2007. pp. 110–125
4. Amin, R., Islam, S., Khan, M.K., Karati, A., Giri, D., Kumari, S.: A two-factor rsa-based robust authentication system for multiserver environments. Secur. Commun. Netw. (2017), doi:10.1155/2017/5989151
5. Chang, C.C., Wu, T.C.: Remote password authentication with smart cards. IEE Proceedings-Computers and Digital Techniques 138(3), 165–168 (1991)
6. Huang, X., Chen, X., Li, J., Xiang, Yang ang Xu, L.: Further observations on smart-card-based password-authenticated key agreement in distributed systems. IEEE Trans. Para. Distrib. Syst. 25(7), 1767–1775 (2014)
7. Irshad, A., Ahmad, H.F., Alzahrani, B.A., Sher, M., Chaudhry, S.A.: An efficient and anonymous chaotic map based authenticated key agreement for multi-server architecture. KSII Trans. Internet Inf. Syst. 10(12), 5572–5595 (2016)

8. Kumari, S., Khan, M.K., Li, X.: An improved remote user authentication scheme with key agreement. Computers & Electrical Engineering 40(6), 97–112 (2014)
9. Lee, C.C., Lin, T.H., Chang, R.X.: A secure dynamic id based remote user authentication scheme for multi-server environment using smart cards. Expert Syst. Appl. 38(11), 13863–13870 (2011)
10. Leu, J.S., Hsieh, W.B.: Efficient and secure dynamic id-based remote user authentication scheme for distributed systems using smart cards. IET Inform. Secur. 8(2), 104–113 (2014)
11. Ma, C., Wang, D., Zhao, S.D.: Security flaws in two improved remote user authentication schemes using smart cards. Int. J. Commun. Syst. 27(10), 2215–2227 (2014)
12. Maitra, T., Islam, S.H., Amin, R., Giri, D., Khan, M.K., Kumar, N.: An enhanced multi-server authentication protocol using password and smart-card: cryptanalysis and design. Secur. Commun. Netw. 9(17), 4615–4638 (2016)
13. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Examining smart-card security under the threat of power analysis attacks. IEEE Trans. Comput. 51(5), 541–552 (2002)
14. Stobert, E., Biddle, R.: The password life cycle. ACM Trans. Priva. Secur. 21(3), 13 (2018)
15. Wang, C., Xu, G., Li, W.: A secure and anonymous two-factor authentication protocol in multiserver environment. Secur. Commun. Netw. (2018), doi: 10.1155/2018/9062675
16. Wang, D., Wang, P.: Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE Trans. Depend. Secur. Comput. 15(4), 708–772 (2018)
17. Wang, D., Cheng, H., Wang, P., Huang, X., Jian, G.: Zipf's law in passwords. IEEE Trans. Inform. Foren. Secur. 12(11), 2776–2791 (2017)
18. Wang, D., Gu, Q., Cheng, H., Wang, P.: The request for better measurement: A comparative evaluation of two-factor authentication schemes. In: Proc. ACM ASIACCS 2016. pp. 475–486
19. Wang, D., He, D., Wang, P., Chu, C.H.: Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. IEEE Trans. Depend. Secur. Comput. 12(4), 428–442 (2015)
20. Wang, Y.G.: Password protected smart card and memory stick authentication against off-line dictionary attacks. In: Proc. SEC 2012, pp. 489–500
21. Wu, F., Xu, L., Li, X.: A new chaotic map-based authentication and key agreement scheme with user anonymity for multi-server environment. In: Proc. FC 2017. pp. 335–344
22. Xie, Q., Wong, D.S., Wang, G., et al.: Provably secure dynamic id-based anonymous two-factor authenticated key exchange protocol with extended security model. IEEE Trans. Inform. Foren. Secur. 12(6), 1382–1392 (2017)
23. Xu, J., Zhu, W., Feng, D.: An improved smart card based password authentication scheme with provable security. Comput. Stand. Inter. 31(4), 723–728 (2009)
24. Xu, Z., He, D., Huang, X.: Secure and efficient two-factor authentication protocol using rsa signature for multi-server environments. In: ICICS 2017. pp. 595–605
25. Yang, G.M., Wong, D.S., Wang, H.X., Deng, X.T.: Two-factor mutual authentication based on smart cards and passwords. J. Comput. Syst. Sci. 74(7), 1160–1172 (2008)
26. Zhu, H.: Flexible and password-authenticated key agreement scheme based on chaotic maps for multiple servers to server architecture. Wirel. Personal Commun. 82(3), 1697–1718 (2015)