INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS
Int. J. Commun. Syst. (2012)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/dac.2468

Security flaws in two improved remote user authentication schemes using smart cards

Chun-Guang Ma[1], Ding Wang[1,2,*,†] and Sen-Dong Zhao[1]

[1]*College of Computer Science and Technology, Harbin Engineering University, Harbin City 150001, China*
[2]*Department of Training, Automobile Management Institute of PLA, Bengbu City 233011, China*

SUMMARY

Understanding security failures of cryptographic protocols is the key to both patching existing protocols and designing future schemes. In this paper, we analyze two recent proposals in the area of password-based remote user authentication using smart cards. First, we point out that the scheme of Chen *et al.* cannot achieve all the claimed security goals and report its following flaws: (i) it is vulnerable to offline password guessing attack under their nontamper resistance assumption of the smart cards; and (ii) it fails to provide forward secrecy. Then, we analyze an efficient dynamic ID-based scheme without public-key operations introduced by Wen and Li in 2012. This proposal attempts to overcome many of the well-known security and efficiency shortcomings of previous schemes and supports more functionalities than its counterparts. Nevertheless, Wen–Li's protocol is vulnerable to offline password guessing attack and denial of service attack, and fails to provide forward secrecy and to preserve user anonymity. Furthermore, with the security analysis of these two schemes and our previous protocol design experience, we put forward three general principles that are vital for designing secure smart-card-based password authentication schemes: (i) public-key techniques are indispensable to resist against offline password guessing attack and to preserve user anonymity under the nontamper resistance assumption of the smart card; (ii) there is an unavoidable trade-off when fulfilling the goals of local password update and resistance to smart card loss attack; and (iii) at least two exponentiation (respectively elliptic curve point multiplication) operations conducted on the server side are necessary for achieving forward secrecy. The cryptanalysis results discourage any practical use of the two investigated schemes and are important for security engineers to make their choices correctly, whereas the proposed three principles are valuable to protocol designers for advancing more robust schemes. Copyright © 2012 John Wiley & Sons, Ltd.

Received 7 September 2012; Accepted 15 October 2012

KEY WORDS: cryptanalysis; authentication protocol; smart card; nontamper resistant; dynamic ID; offline password guessing attack

1. INTRODUCTION

With the rapid development of distributed computer networks, more and more services and resources are shared among the user terminals, and more and more electronic transactions are accomplished in the cyber world. Owing to the openness of distributed networks, robust system security and strong privacy protection have become essential requirements for any application systems. Accordingly, user authentication becomes a crucial security mechanism for these systems to distinguish legitimate users from malicious adversaries.

In 1981, Lamport [1] proposed the first remote user authentication scheme using only human-memorable passwords. Because of its simplicity and convenience, this scheme has gained much

*Correspondence to: Ding Wang, Room #106, Student Apartment #15, Harbin Engineering University, Harbin City 150001, China.
†E-mail: wangdingg@mail.nankai.edu.cn

popularity shortly after being advanced, and it was later refined and adopted in various application systems. However, there are some prominent issues in such password-based schemes, such as the cost of protecting and maintaining the verifier table on the remote server and the vulnerability to password guessing attack. To overcome these pitfalls and further enhance the system security, Chang and Wu [2] introduced the first password-based remote user authentication scheme using smart cards in 1993. Owing to the advantages of smart cards, such as low cost, cryptographic capacity, and portability, smart-card-based password authentication has become one of the most widely adopted two-factor authentication mechanisms [3], and many of this type of schemes were proposed [4–13].

The participants of such schemes mainly involve an authentication server S and a client U. At first, the user U submits her self-chosen personal information (the identity and the password) to the server S, and then, S securely issues a smart card to U with the smart card being personalized with some security parameters. This phase is called the registration phase and is carried out only once for each client. Later on, U and S authenticate itself to each other through the login phase and the authentication phase. The basic security goal of such schemes is to ensure mutual authentication between U and S. To carry out the smart-card-based password authentication successfully with server S, the client U is required to both have the smart card and know the corresponding password; otherwise, the authentication process will end with a failure. Besides mutual authentication, a practical scheme should also be able to withstand various passive and active attacks [3, 9, 13, 14], such as offline password guessing attack, stolen-verifier attack, replay attack, user impersonation attack, server masquerading attack, denial of service attack, reflection attack, and parallel session attack, whereas a failure of any of these security goals may render the whole system completely insecure and unpractical. Sophisticated schemes also support some desirable functionalities [9, 10, 15], such as local password change, session key agreement, and forward secrecy.

Despite decades of intensive research, how to design an efficient and secure smart-card-based password authentication scheme still remains a challenge. In 2009, Xu *et al.* [16] pointed out that previous schemes are prone to various attacks, such as user impersonation attack and offline password guessing attack, if the secret information stored in the smart card is disclosed by the adversary. The underlying assumption of their observation is indeed practical in consideration of the state-of-the-art side-channel attack techniques [17–19]. Accordingly, Xu *et al.* further proposed a robust scheme that is claimed to be secure under the nontamper resistance assumption of the smart cards. Unfortunately, shortly after the scheme of Xu *et al.* was put forward, Song [20] found it vulnerable to user impersonation attack, which means it even cannot achieve the basic goal of mutual authentication. In 2012, Chen *et al.* [21] demonstrated that all the three schemes proposed by Xu *et al.*, Song, and Sood *et al.* still have various security vulnerabilities being overlooked and further presented an enhanced version to overcome the aforementioned defects. However, in this paper, we demonstrate that the scheme of Chen *et al.* still cannot withstand offline password guessing attack under their nontamper resistance assumption of the smart cards. Moreover, their scheme fails to achieve the claimed security goal of forward secrecy.

As violation concern of user privacy is promptly raised among individuals and human right organizations, dynamic ID-based schemes that can preserve user anonymity have been a very hot research topic in recent years. In 2012, Wen and Li [22] pointed out that a previous dynamic ID-based scheme proposed by Wang *et al.* [4] in 2009 is still vulnerable to attacks, such as impersonation attack and offline password guessing attack under the nontamper resistance assumption of the smart cards. To cope with these identified defects, Wen and Li proposed an improved scheme to enhance the security of the scheme of Wang *et al.* This proposal attempts to overcome many of the well-known security and efficiency problems of previous schemes and supports more functionalities, such as user eviction mechanism and secret renew mechanism, than its counterparts. In addition, their scheme involves no public-key operations and thus is superior to the previous solutions for implementation in resource-constrained applications, for example, mobile devices. Although Wen–Li's scheme possesses many merits, we find it still cannot achieve the claimed security goals: (i) It cannot withstand offline password attack; (ii) It is prone to denial of service attack; (iii) It fails to preserve user anonymity, which is the most essential goal that a dynamic ID-based scheme is designed to support.

DOI: 10.1002/dac

There have been several papers [23–28] dealing with security vulnerabilities in smart-card-based password authentication schemes. However, in these studies, the authors only present attacks on previous schemes and conclude their paper with a routine summary, such as 'the scheme under study cannot achieve all the claimed security goals' and 'the scheme under investigation is unsuitable for practical applications', while paying little attention to the underlying rationale of the identified security failures. As a result, the same mistakes are repeated over and over again. To ameliorate this situation, in this paper, through the security analysis of the aforementioned two schemes and our past cryptanalysis experience (some of our cryptanalysis results include [10, 13, 15, 29–31]), three principles that are crucial for designing secure smart-card-based password authentication schemes are put forward, in the hope that no similar mistakes are made in the future. By following our principles, one can check whether any of this type of schemes achieves certain security goals within a few seconds.

The remainder of this paper is organized as follows: in Section 2, we review the scheme of Chen *et al.* Section 3 describes the weaknesses of the scheme of Chen *et al.* Wen–Li's scheme is reviewed in Section 4, and the corresponding cryptanalysis is given in Section 5. Section 6 discusses three principles learned from the cryptanalysis, and the conclusion is drawn in Section 7.

2. REVIEW OF THE SCHEME OF CHEN ET AL.

In this section, we briefly illustrate the remote user authentication scheme proposed by Chen *et al.* [21] in 2012. Their scheme consists of four phases – initialization, registration, login, and authentication – and one activity – password change. For ease of presentation, we employ some intuitive abbreviations and notations listed in Table I, and we will follow the notations in the scheme of Chen et al. as closely as possible.

2.1. Initialization phase

In this phase, S selects two large prime numbers p and q such that $p = 2q + 1$, its secret key $x \in Z_q^*$, and an one-way hash function $H(\cdot)$.

2.2. Registration phase

The registration phase involves the following operations:

(1) U_i chooses her identity ID_i and password PW_i.
(2) $U_i \Rightarrow S : \{ID_i, PW_i\}$.
(3) S computes the security parameter $B_i = H(ID_i)^{x+PW_i} \bmod p$.
(4) $S \Rightarrow U_i : A$ smart card containing security parameters $\{B_i, p, q, H(\cdot)\}$.

Table I. Notations.

Symbol	Description
U_i	ith user
S	Remote server
$\mathcal{A}$	The adversary
ID_i	Identity of user U_i
PW_i	Password of user U_i
x	The secret key of remote server S
$H(\cdot)$	Collision free one-way hash function
$\oplus$	The bitwise XOR operation
$\|$	The string concatenation operation
$A \rightarrow B : C$	Message C is transferred through a common channel from A to B
$A \Rightarrow B : C$	Message C is transferred through a secure channel from A to B

DOI: 10.1002/dac

2.3. Login phase

When U_i wants to login to S, the following operations will be performed:

(1) U_i inserts her smart card into a card reader and submits her identity ID_i and password PW_i.
(2) The smart card chooses $\alpha \in_R Z_q^*$, reads the current timestamp T_i, and computes $C_i = B_i / H(ID_i)^{PW_i} \bmod p$, $D_i = H(ID_i)^{\alpha} \bmod p$, $W_i = C_i \cdot D_i \bmod p$, and $M_i = H(ID_i \parallel C_i \parallel D_i \parallel W_i \parallel T_i)$.
(3) $U_i \rightarrow S : \{ID_i, D_i, M_i, T_i\}$.

2.4. Authentication phase

After receiving the login request from user U_i, S performs the following operations:

(1) S checks the validity of ID_i and that $T_i' - T_i \leqslant \Delta T$, where T_i' is the time when the login request was received. If either is invalid, the login request is rejected. Otherwise, S computes $C_i' = H(ID_i)^x \bmod p$, $W_i' = C_i' D_i \bmod p$, and $M_i' = H\left(ID_i \left\| C_i' \right\| D_i \left\| W_i' \right\| T_i\right)$.
(2) S compares M_i' with the received M_i. If they are equal, U_i is authenticated, and the login request is accepted; otherwise, S terminates the session.
(3) S computes $M_s = H\left(ID_i \left\| W_i' \right\| T_s\right)$, where T_s is the current timestamp on server side.
(4) $S \rightarrow U_i : \{ID_i, M_s, T_s\}$.
(5) Upon receiving the response from the server, U_i checks both ID_i and T_s, and compares M_s with $H(ID_i \parallel W_i \parallel T_s)$. If the equality holds, S is authenticated.
(6) After authenticating each other, U_i and S use the same session key $sk = H(W_i) = H\left(W_i'\right)$ to secure ensuing data communications.

2.5. Password change activity

When U_i wants to change the old password PW_i to a new one, this phase will be involved.

(1) U_i inserts her smart card into the card reader and submits her identity ID_i, the original password PW_i, and the new password PW_i^{new}.
(2) The smart card goes through the login and authentication phases to check the validity of PW_i by interacting with S. If PW_i is valid, the smart card replaces B_i with $B_i^{\text{new}} = \left(B_i / H(ID_i)^{PW_i}\right) \cdot H(ID_i)^{PW_i^{\text{new}}} \bmod p$.

3. CRYPTANALYSIS OF THE SCHEME OF CHEN ET AL.

In this section, we will show that the scheme of Chen *et al.* is vulnerable to offline password guessing attack and fails to provide forward secrecy, which invalidates the claims made in [21]. There are three assumptions of the adversary's capabilities explicitly made in the scheme of Chen et al.:

(1) The adversary $\mathcal{A}$ has total control over the communication channel between the user U and the remote server S, which means $\mathcal{A}$ can eavesdrop, block, insert, delete, alter, or intercept any messages transmitted in the channel.
(2) The adversary $\mathcal{A}$ can have temporary access (by stealing or picking up) to the user's smart card to extract the secret values stored in the smart card.
(3) The adversary $\mathcal{A}$ can offline enumerate the password space.

Note that these three assumptions, which are also made in the latest works [9, 25–27, 30, 31], are indeed reasonable: (i) Assumption (1) is accordant with the standard distributed computing adversary model; (ii) Assumption (2) is realistic in consideration of the state-of-the-art side-channel attack techniques [17–19]; (iii) Assumption (3) reveals the reality that to be user friendly, most schemes allow the user to choose her own password at will during the password change phase and registration phase, whereas the user is apt to select a password that is easily remembered for her convenience in practice [32], and thus, the human-memorable password tends to be a 'weak password' [33, 34].

On the basis of the aforementioned assumptions, in the following discussions of the security flaws of the scheme of Chen *et al.*, we assume that an attacker can extract the secret values $\{B_i, p, q\}$

DOI: 10.1002/dac

stored in the legitimate user's smart card and that the attacker can also intercept or block the login request $\{ID_i, D_i, M_i, T_i\}$ sent out by the user U_i and the reply message $\{ID_i, M_s, T_s\}$ sent out by the server S.

3.1. Offline password guessing attack

In the offline password guessing attack, the adversary records past communication messages and then goes over the password dictionary and search for a password consistent with the recorded communication, which is the most damaging threat that a sound password-based protocol must be able to thwart [24]. Chen *et al.* showed that Song's scheme [20] is vulnerable to offline password guessing attack once the adversary has extracted the secret parameters stored in the stolen smart card.

Now, let us see how this attack could be successfully launched with the scheme of Chen *et al.* in place. In case a legitimate user U_i's smart card is somehow obtained (stolen or picked up) by an adversary $\mathcal{A}$, the stored secret B_i can be revealed by some means under Assumption (2). With the previously intercepted authentication message $\{ID_i, D_i, M_i, T_i\}$ from the public channel, $\mathcal{A}$ can obtain U_i's password PW_i as follows:

Step 1. Guesses the value of PW_i to be PW_i^* from dictionary space $\mathcal{D}_{pw}$.
Step 2. Computes $C_i^* = B_i / H(ID_i)^{PW_i^*}$, where B_i is revealed from U_i's smart card and ID_i is intercepted from the public channel.
Step 3. Computes $W_i^* = C_i^* \cdot D_i$, where D_i is previously intercepted from the public channel.
Step 4. Computes $M_i^* = H\left(ID_i \left\| C_i^* \right\| D_i \left\| W_i^* \right\| T_i\right)$.
Step 5. Verifies the correctness of PW_i^* by checking if the computed M_i^* is equal to the intercepted M_i.
Step 6. Repeats Steps 1–5 of this procedure until the correct value of PW_i is found.

Let $|\mathcal{D}_{pw}|$ denote the number of passwords in $\mathcal{D}_{pw}$. The running time of the aforementioned attack procedure is $\mathcal{O}(|\mathcal{D}_{pw}| * (T_E + T_I + 2T_H))$, where T_E is the running time for modular exponentiation, T_I is the running time for modular inverse operation, and T_H is the running time for Hash function. Consequently, the time for $\mathcal{A}$ to recover U_i's password is a linear function of the number of passwords in the password space. In practice, the password space is very limited, for example, $|\mathcal{D}| = 10^6$ [33, 34]; $\mathcal{A}$ may recover the password in seconds on a PC.

3.2. Failure to achieve forward secrecy

As noted in [29], forward secrecy is an important property of remote user authentication schemes to limit the effects of eventual failure of the entire system in case the long-term private keys of one or more parties are compromised (leaked or stolen). More precisely, a scheme with forward secrecy assures that the secrecy of previously generated session keys is not affected even if the long-term secrets of one or more entities are exposed.

Let us consider the following scenarios. Suppose the server S's long-time private key x leaks out by accident or is intentionally stolen by an adversary $\mathcal{A}$. Once the value of x is obtained, with previously intercepted D_i^j that was transmitted over the public channel during the legitimate user U_i's jth authentication process, $\mathcal{A}$ can compute the session key of U_i and S's jth encrypted communication as follows:

Step 1. Computes $C_i^j = H(ID_i)^x \bmod p$, where ID_i is previously obtained by eavesdropping on the public channel.
Step 2. Computes $W_i^j = C_i^j \cdot D_i^j$, where D_i^j is previously obtained by eavesdropping on the public channel.
Step 3. Computes the jth session key $SK^j = h\left(W_i^j\right)$.

Once the session key SK^j is obtained, the whole jth session will be completely exposed to $\mathcal{A}$. Therefore, as opposed to the claim of Chen *et al.*, forward secrecy is not provided in their scheme.

DOI: 10.1002/dac

4. REVIEWS OF WEN–LI'S SCHEME

In 2012, Wen and Li proposed an improved version [22] over the dynamic ID-based scheme of Wang *et al.* [4] to remedy the identified defects in the dynamic ID-based scheme of Khan *et al.* [8]. This scheme is composed of four basic phases: registration, login, authentication and key exchange, and mutual authentication and key confirmation. And there are three more advanced phases: revocation phase, offline password change phase, and online secret renew phase. In the following, we employ the notations listed in Table I and follow the descriptions in Wen–Li's scheme as closely as possible.

4.1. Registration phase

When user U_i wants to register to the remote server S, the following operations will be involved:

(1) U_i chooses her identity ID_i and password pw_i.
(2) $U_i \Rightarrow S : \{ID_i, PW_i\}$.
(3) S computes $n_i = h(ID_i \parallel PW_i)$, where n_i is the user's unique ID number and $h(\cdot)$ is a one-way hash function, for example, SHA-1. The unique number n_i is kept by S to check the validity of the smart card, but S does not need to keep the identity or password tables. Then, S computes $m_i = n_i \oplus x$, $N_i = h(ID_i) \oplus h(PW_i) \oplus h(x) \oplus h(m_i)$, where x is the server's master secret key.
(4) $S \Rightarrow U_i : A$ smart card containing security parameters $\{h(\cdot), N_i, n_i\}$.

4.2. Login phase

When user U_i wants to login to S, he or she inserts his or her smart card into the terminal and keys ID_i with PW_i. The smart card performs the following steps:

(1) The smart card computes $A_i = h(ID_i) \oplus h(PW_i)$, $B_i = N_i \oplus h(ID_i) \oplus h(PW_i) = h(x) \oplus h(m_i)$, and $CID_i = h(A_i) \oplus h(h(n_i) \oplus B_i \oplus h(N_i) \oplus T)$, where T is the current timestamp.
(2) $U_i \rightarrow S : M_1 = \{CID_i, n_i, N_i, T\}$.

4.3. Authentication and key exchange phase

Upon receiving the login request at time T', S performs the following steps:

(1) Checks whether $T' - T \leqslant \Delta T$ and n_i are in the registered list; if either fails, S terminates.
(2) Computes $m_i = n_i \oplus x$, $B_i = h(x) \oplus h(m_i)$, and $A_i = N_i \oplus B_i = h(ID_i) \oplus h(PW_i)$.
(3) Verifies whether the equation $CID_i \oplus h(A_i) = h(B_i \oplus h(N_i) \oplus h(n_i) \oplus T)$ holds. If the equality does hold, S continues to compute $C_i' = h(A_i \oplus T' \oplus h(n_i))$, the session key $SK = h(A_i \parallel T \parallel B_i \parallel T')$, and the key confirmation message $KC' = h(B_i \parallel SK \parallel T')$.
(4) $S \rightarrow U_i : \left\{M_2 = \left\{C_i', KC', T'\right\}\right.$.

4.4. Mutual authentication and key confirmation phase

Upon receiving the response at timeT'', U_i performs the following steps:

(1) U_i checks $T' - T \leqslant \Delta T$ and $C_i' \stackrel{?}{=} h(A_i \oplus T' \oplus h(n_i))$. If either is invalid, the login request is rejected. Otherwise, U_i computes $SK = h(A_i \parallel T \parallel B_i \parallel T')$.
(2) U_i checks $KC' \stackrel{?}{=} h(B_i \| SK \| T')$. If the verification holds, U_i proceeds to compute $KC = h(A_i \parallel SK \parallel T'')$.
(3) $U_i \rightarrow S : M_3 = \{KC, T''\}$.
(4) S verifies the last key confirmation message; if the equation $KC = h(A_i \parallel SK \parallel T'')$ holds, the authenticity of U_i is confirmed, and this accomplishes the authentication process.

DOI: 10.1002/dac

4.5. Revocation phase

In case of loss of smart card or theft, U_i could request S for revocation. S verifies U_i's credentials by checking whether $n_i = H(ID_i \parallel PW_i)$ is stored in the registration table. Then, U_i can re-register to the server S through the registration phase.

4.6. Offline password change phase

When the user wants to change her password, he or she inserts the smart card into the terminal and keys ID_i with PW_i, and then, the smart card computes $N_i^{\text{new}} = N_i \oplus h(PW_i) \oplus h\left(PW_i^{\text{new}}\right)$, where PW_i^{new} is U's new password. Then, the smart card replaces N_i with N_i^{new}.

4.7. Online secret renew phase

When the remote server wants to renew its secret key x to enhance the security of the system, S can interact with its clients to first authenticate each other and then to update the corresponding parameters within the session-key encrypted channel. Because this phase has little relevance with our discussions, it is omitted here.

5. CRYPTANALYSIS OF WEN–LI'S SCHEME

The three assumptions presented in Section 3 are also explicitly made in Wen–Li's paper [22] when they analyze the security of the scheme of Wang *et al.* [4]. Naturally, our following cryptanalysis also relies on these three assumptions.

Although Wen–Li's scheme has many attractive properties, such as the provision of local password change, advanced functional phases, and only involving very few computationally efficient hash operations, it fails to achieve many of the claimed security goals. In the following, we will demonstrate that Wen–Li's scheme still cannot preserve user anonymity, which is the most crucial goal of a dynamic ID-based scheme. Besides, we also observe that Wen–Li's scheme is susceptible to offline password guessing attack, which is an inherent vulnerability existing in the scheme. Furthermore, we point out that Wen–Li's scheme fails to provide forward secrecy and is prone to smart card loss attack, which seriously impairs the practicality of the scheme in real applications.

5.1. No provision of user anonymity

A protocol with user anonymity protects an individual's sensitive personal information, such as preferences, lifestyles, social circle, shopping patterns, and so on, from being acquired by an adversary through analyzing the login information, the resources, or the services being accessed [35]. Additionally, in mobile environments, the leakage of user-specific information may facilitate an unauthorized entity to track the user's login history and current location [36]. Hence, user anonymity is a highly desirable property of remote user authentication schemes.

To provide user anonymity, the common practice is to employ the 'dynamic ID technique' [37]: a user's real identity is concealed in the session-variant pseudo-identities. Authentication schemes that employ this technique are so-called 'dynamic-ID' schemes. And Wen–Li's scheme falls into this category. However, Wen–Li's scheme actually fails to preserve user anonymity, which is the most essential feature that a dynamic-ID scheme is designed to support.

In each login request, user U_i will send the message $\{CID_i, n_i, N_i, T\}$ to the remote server. Among the request data, the values n_i and N_i are kept the same and specific to each user until the password is updated to a new one. Either n_i or N_i can be seen as user U_i's identification. An adversary could not be aware of the real identity of the user but may know whether two conversations are originating from the same (unknown) party. The adversary can, therefore, use n_i or N_i to identify and trace U_i's login requests and activities. Consequently, the scheme fails to preserve user anonymity.

Note that in this user-anonymity violation attack, the adversary only needs to keep an eye over the public channel and does not involve any cryptographic operations. In this regard, it is very practical

DOI: 10.1002/dac

and effective. On the other hand, the limitation of our attack is also obvious: the adversary manages to trace user activity but fails to know the real identity of the user. Unfortunately, a dedicated adversary can still figure out the real identity of victim user U_i through the offline identity guessing attack. We elaborate on this in what follows.

5.2. *Offline password (and identity) guessing attack*

Just with one previously eavesdropped message $\{CID_i, n_i, N_i, T\}$, an adversary $\mathcal{A}$ can successfully guess the password (and the identity) of U_i as follows:

Step 1. Randomly chooses a pair $\left(ID_i^*, PW_i^*\right)$ from the Cartesian product $\mathcal{D}_{id} \times \mathcal{D}_{pw}$, where $\mathcal{D}_{id}$ denotes the identity space and $\mathcal{D}_{pw}$ denotes the password space.
Step 2. Computes $n_i^* = h\left(ID_i^* \| PW_i^*\right)$.
Step 3. Verifies the correctness of PW_i^* and ID_i^* by checking if n_i^* equals the received n_i. If n_i^* does not equal n_i, go back to Step 1.
Step 4. Repeat Steps 1–3 until the correct value of (ID_i, PW_i) pair is found.

Let $|\mathcal{D}_{id}|$ and $|\mathcal{D}_{pw}|$ denote the number of identities in $\mathcal{D}_{id}$ and the number of passwords in $\mathcal{D}_{pw}$, respectively. The running time of the aforementioned attack procedure is $\mathcal{O}(|\mathcal{D}_{id}| * |\mathcal{D}_{pw}| * T_H)$, where T_H is the running time for Hash, because both password and identity are human-memorable short strings but not high-entropy keys, that is to say, they are often chosen from two corresponding dictionaries of small size. As $|\mathcal{D}_{id}|$ and $|\mathcal{D}_{pw}|$ are very limited in practice, for example, $|\mathcal{D}_{id}| \leqslant |\mathcal{D}_{pw}| \leqslant 10^6$ [33, 38, 39], the aforementioned attack can be completed in polynomial time.

It is worth noting that, as with the user anonymity violation attack presented in Section 5.1, in this attack, the adversary $\mathcal{A}$ only needs to be a passive eavesdropping attacker. From this point of view, our attack is rather effective and practical.

5.3. *Smart card loss attack*

The password change phase of Wen–Li's scheme is completely insecure because there is no validation of the authenticity of the old password before the new password update. If an adversary manages to gain temporary access to legitimate user U_i's smart card (this is a quite realistic assumption), he or she can easily launch a kind of denial of service attack as follows:

Step 1. Inserts U_i's smart card into a card reader and initiates a password change request.
Step 2. Submits a random string X as U_i's original password and a new string PW_i^{new}as the targeting new password.
Step 3. The smart card computes $N_i^{\text{new}} = N_i \oplus h(PW_i) \oplus h\left(PW_i^{\text{new}}\right)$ and updates N_i with N_i^{new}.

Once the value of N_i is updated, legitimate user U_i cannot login successfully even after obtaining his/her smart card back because $N_i^{\text{new}} \oplus h(PW_i) \oplus h(ID_i) \neq h(x) \oplus h(m_i)$, and since then, U_i's login requests will be denied by the server S during the authentication and key exchange phase until U_i re-register to the server S. Consequently, denial of service attack can be launched successfully.

An important point to realize here is that although the aforementioned attack seems rather simple, how to cope with it is quite tricky. And it will be further discussed later in this paper.

5.4. *No provision of forward secrecy*

Let us consider the following scenarios. Suppose the server S's long-time private key x is leaked out by accident or intentionally stolen by an adversary $\mathcal{A}$. Once the value of x is obtained, with previously intercepted login message $\left\{CID_i^j, n_i^j, N_i^j, T^j\right\}$ that was transmitted over the public channel during the legitimate user U_i's jth authentication process, $\mathcal{A}$ can compute the session key of U_i and S's jth encrypted communication as follows:

Step 1. Computes $m_i^j = n_i^j \oplus x$, where n_i^j is previously obtained by eavesdropping on the public channel.
Step 2. Computes $B_i^j = h(x) \oplus h\left(m_i^j\right)$.

DOI: 10.1002/dac

Step 3. Computes $A_i^j = N_i^j \oplus B_i^j$.
Step 4. Computes the jth session key $SK^j = h\left(A_i^j \| T^j \| B_i^j \| T'^j\right)$.

Once the session key SK^j is obtained, the whole jth session will be completely exposed to $\mathcal{A}$. Therefore, Wen–Li's scheme cannot achieve forward secrecy.

6. THREE PRINCIPLES FOR DESIGNING MORE ROBUST SCHEMES

There are hundreds of papers dealing with smart-card-based password authentication; some quite recent ones include [4, 6–13, 29, 40]. Moreover, several papers [23–28] have focused on the security vulnerabilities in previous schemes. Yet, relatively little rationale has been given for the specific design choices in the protocol, and similar (sometimes even the same) mistakes are repeated over and over again (some problematic schemes, e.g., [6, 7, 16, 41], even provide a formal security proof). For example, the scheme proposed by Wang *et al.* [4] has been found vulnerable to offline password guessing attack and smart card loss attack (denial of service attack) by Ahmed *et al.* in 2009 [42] and to user anonymity violation attack by He *et al.* in 2010 [43]. However, precisely the same vulnerabilities still exist in its several improved versions [6, 8, 9], whereas the authors in [6, 8, 9] are clearly aware of these security flaws of the scheme of Wang *et al.* [4], which once again proves that a cryptanalysis may be of little value if little (or no) underlying rationale of the security vulnerabilities is uncovered.

To mitigate this situation, through the security analyses of the schemes of Chen *et al.* and Wen–Li and on the basis of our past cryptanalysis experience (some of our cryptanalysis results include [10, 11, 13, 15, 30, 31]), we present three principles that are important for designing secure two-factor authentication schemes.

6.1. The public-key technique principle

We have reviewed more than 70 recently proposed smart-card-based password authentication schemes for single-server environment and 20 schemes for multiserver architecture, and find, under the nontamper resistance assumption of the smart cards, these schemes (no matter for single-server environment or multiserver architecture) that do not employ public-key technique definitely susceptible to offline password guessing attack and user anonymity violation attack. In other words, all these schemes that do not employ public-key techniques but claim to be secure against offline password guessing attack and to preserve user anonymity under the nontamper resistance assumption of the smart cards are found problematic; some quite recent typical examples include [8, 9, 40, 44].

We show that this is no accident. Under the nontamper resistance assumption of the smart cards, it is important to see that all the security parameters stored in the smart card can be revealed, and thus, the smart-card-based password authentication scheme is downgraded to a traditional one-factor password authentication scheme; that is, the security of the scheme only relies on the security of the password. And a related work performed by Halevi and Krawczyk [45] provides very strong evidence (with the probability of $\boldsymbol{P} \neq \boldsymbol{NP}$) that, under the common distributed computing adversary model, no password protocol (the traditional one-factor password authentication) can be free from offline password guessing attack if the public-key techniques are not used. As user identities are usually as weak as passwords, it is not difficult to see that user identity can also be offline guessed by $\mathcal{A}$ using the same method as guessing user's password. Accordingly, we conjecture that under the nontamper resistance assumption of the smart cards, no smart-card-based password protocol (two-factor authentication [3]) can be free from offline password guessing attack and user anonymity violation if the public-key techniques are not employed. By following this principle, one can easily identify that all these schemes [8, 9, 22, 40, 44], which are only based on symmetric cryptographic primitives (e.g., hash functions, block ciphers and exclusive-OR operations), are inherently unable to withstand offline password guessing attack and to provide user anonymity. And now the countermeasure is obvious: resorting to public-key techniques like [10, 12, 15].

DOI: 10.1002/dac

6.2. The security-usability trade-off principle

In Section 5.3, we have shown that Wen–Li's scheme is susceptible to smart card loss attack. In their scheme, the password change phase seems to be very problematic because it does not provide the smart card with any explicit way to check whether the user-keyed password is correct or not. In other words, the password in the smart card can be changed even without knowledge of the correct current password. It is worth noting that although this vulnerability seems too basic to merit discussion, it cannot be well coped just with minor revisions. To eliminate this defect while achieving the usability goal of local password update, a verification of the validity of the original password before updating the value of parameters stored in the smart card is crucial. Accordingly, the provision of such a means inevitably requires a password verifier to be stored in the smart card, which may introduce new vulnerabilities [15], such as offline guessing attack and user impersonation attack.

To gain more insights into this problem, we take Wen–Li's scheme [22] as an example. Suppose a password verifier is also stored in U_i's smart card (actually, there already exists such a verifier in Wen–Li's original scheme, i.e., n_i). Now, whenever U_i wants to change her password, he or she first keys ID_i and the original password PW_i; the smart card then validate the correctness of PW_i by checking $n_i \stackrel{?}{=} h(ID_i \| PW_i)$. If the check fails, the password change request is denied. Through this way, the identified smart card loss attack can be thwarted in Wen–Li's scheme. Unfortunately, now it is trivial to see that once n_i is revealed by $\mathcal{A}$, an offline password guessing attack will be successfully launched by exhaustively checking whether $n_i \stackrel{?}{=} h\left(ID_i^* \| PW_i^*\right)$, where ID_i^* and PW_i^*) are the guessed identity and password.

This subtlety has also been noticed by Nam *et al.* [23] in 2007; unfortunately, they left it as an open problem. Most subsequent works simply overlook this issue [3, 4, 7, 8, 12, 22, 41] or choose not to provide local user password change [5, 16, 21, 46], whereas the few rest [6, 9, 40, 44, 47] that are ambitious to achieve both goals (i.e., resistance to smart card loss attack and support for local password change) are all found vulnerable to offline password guessing attack. Luckily, this problem seems to have been well resolved with a technique of 'fuzzy verifier' in a recent work [15], in which the authors observed that there is an avoidable trade-off between the security requirement of resistance to smart card loss attack and the usability goal of local password change. And they further introduced a novel 'fuzzy verifier' to cope with this issue. Readers may refer to [15] for more details.

6.3. The forward secrecy principle

Forward secrecy is a desirable security feature of key establishment protocols and concerns the dependency of a session key upon long-term secret keys (symmetric or asymmetric) [48]. More precisely, a scheme providing forward secrecy guarantees that the secrecy of previously generated session keys is not affected even if the long-term secret(s) of one or more entities are compromised. Naturally, most schemes attempt to satisfy this admired feature, but it turns out that many of them fall short of delivering this feature. Quite recent examples include [7, 8, 20, 21, 47, 49], all of which definitely aim at achieving this feature but later found disappointing [12, 25, 29, 43]. As far as we know, in the area of smart-card-based password authentication, no rationale for achieving forward secrecy has ever been uncovered, which may explicate why similar failure occurs again and again. And we try to give some light on this failure in the following.

Because a session key is generally computed with both user-specific parameters and session-specific transients, the secrecy of the session key is up to the secrecy of these two kinds of values. As it is widely accepted that no sensitive (or secret) user-specific parameters shall be stored in the authentication server to avoid insider attack and modified password-verifier attack [4], recent schemes seldom store sensitive user-specific parameters on the server side. That is to say, the servers only store some nonsensitive user-specific parameters or even do not store any user-specific parameters, such as these two schemes just analyzed in this study. In such a situation, no secret user-specific values except those transmitted during the authentication process contribute to the formation of a session key. As a result, an adversary $\mathcal{A}$ with the exact long-term private key of the server S can find all the user-specific values that are necessary for the computation of the session key in the same

DOI: 10.1002/dac

way with S. Now, it is clear that the secrecy of previous session keys will only rely on the transient (i.e., session-specific) secret values, and thus, we can deal with this issue in the broad sense of key establishment protocols, where only session-specific secret values are concerned.

In a seminal work [48], Park *et al.* investigated the basic principle for achieving forward secrecy in key establishment protocols. They presented two general prototypes to realize this feature: one is based on the classic Diffie–Hellman key exchange technique, and the other is based on the confidentiality of a random nonce chosen by the responder (i.e., the server in the case of smart-card-based password authentication). Furthermore, Park *et al.* conjectured that forward secrecy can only be achieved by protocols that either have similar algebraic properties as modular exponentiation (i.e., the prototype one, in which at least two exponential operations are conducted on the server side) or use trapdoor one-way functions underlying any public-key cryptosystem (i.e., the prototype two, in which at least two exponential operations are conducted on the server side). Readers are referred to [48] for more details about these two prototypes. On the basis of the findings of Park *et al.*, it is sufficient to infer that (i) forward secrecy can only be achieved with the help of public-key techniques, which explains the failure of [8,47], and (ii) forward secrecy can only be achieved with at least two exponential operations conducted on the server side, which explains the failure of [7,20,21,49].

Note that the aforementioned two conclusions can be further summarized as follows: at least two exponentiation operations conducted on the server side are necessary for achieving forward secrecy. It is also worth noting that in the aforementioned analysis, we do not take the elliptic curve cryptosystem into consideration, but it is trivial to see that our principle can be directly applied to schemes based on elliptic curve cryptosystem, as the elliptic curve point multiplication is analogous to the modular exponentiation in discrete logarithm-based schemes.

7. CONCLUSION

Smart-card-based password authentication technology has been widely deployed in various kinds of security-critical applications because of its portability, efficiency, and two-factor security, but designing a secure and practical scheme has been demonstrated not to be an easy task. Although there have been ample of works on the security analysis of this type of schemes, little (or even no) rationale is given, and thus, similar mistakes are repeated over and over again. In this paper, through the cryptanalysis of two quite recent schemes, that is, the schemes of Chen *et al.* and Wen–Li, we put forward three principles that are helpful to explain many of the security failures repeated in the past and important for designing more robust schemes in the future.

ACKNOWLEDGEMENTS

This research was partially supported by the National Natural Science Foundation of China (NSFC) under Grant No. 61170241 and the Specialized Foundation Project for Science and Technology Innovation Talent of Harbin City under Grant No. 2012RFXXG086.

REFERENCES

1. Lamport L. Password authentication with insecure communication. *Communications of the ACM* 1981; **24**(11):770–772.
2. Chang CC, Wu TC. Remote password authentication with smart cards. *IEE Proceedings-Computers and Digital Techniques* 1991; **138**(3):165–168.
3. Yang G, Wong D, Wang H, Deng X. Two-factor mutual authentication based on smart cards and passwords. *Journal of Computer and System Sciences* 2008; **74**(7):1160–1172.
4. Wang Y, Liu J, Xiao F, Dan J. A more efficient and secure dynamic ID-based remote user authentication scheme. *Computer Communications* 2009; **32**(4):583–585.
5. Horng W, Lee C, Peng J. A secure remote authentication scheme preserving user anonymity with non-tamper resistant smart cards. *WSEAS Transactions on Information Science and Applications* 2010; **7**(5):619–628.
6. Yeh KH, Su C, Lo NW, Li Y, Hung YX. Two robust remote user authentication protocols using smart cards. *Journal of Systems and Software* 2010; **83**(12):2556–2565.
7. Tsai J, Wu T, Tsai K. New dynamic ID authentication scheme using smart cards. *International Journal of Communication Systems* 2010; **23**(12):1449–1462.

DOI: 10.1002/dac

8. Khan M, Kim S, Alghathbar K. Cryptanalysis and security enhancement of a more efficient and secure dynamic ID-based remote user authentication scheme'. *Computer Communications* 2011; **34**(3):305–309.
9. Sood SK. Secure dynamic identity-based authentication scheme using smart cards. *Information Security Journal: A Global Perspective* 2011; **20**(2):67–77.
10. Ma CG, Wang D, Zhang QM. Cryptanalysis and improvement of Sood *et al.*'s dynamic ID-based authentication scheme. In *ICDCIT 2012*, Vol. 7154, Ramanujam R, Ramaswamy S (eds), LNCS. Springer: Berlin / Heidelberg, 2012; 141–152.
11. Wang D, Ma CG. Cryptanalysis and security enhancement of a remote user authentication scheme using smart cards. *The Journal of China Universities of Posts and Telecommunications* 2012; **19**(5):104–114.
12. Wu SH, Zhu YF, Pu Q. Robust smart-cards-based user authentication scheme with user anonymity. *Security and Communication Networks* 2012; **5**(2):236–248.
13. Wang D, Ma CG, Wu P. Secure password-based remote user authentication scheme with non-tamper resistant smart cards. In *26th Annual IFIP Conference on Data and Applications Security and Privacy (DBSEC 2012)*, Vol. 7371, Cuppens-Boulahia N, Cuppens F, Garcia-Alfaro J (eds), LNCS. Springer: Berlin / Heidelberg, 2012; 114–121.
14. Tsai C, Lee C, Hwang M. Password authentication schemes: current status and key issues. *International Journal of Network Security* 2006; **3**(2):101–115.
15. Wang D, Ma CG. Robust smart card based password authentication scheme against smart card security breach. Cryptology ePrint Archive. *Report 2012/439*, 2012. (Available from: http://eprint.iacr.org/2012/439.pdf). [Accessed on 21 July 2012].
16. Xu J, Zhu W, Feng D. An improved smart card based password authentication scheme with provable security. *Computer Standards & Interfaces* 2009; **31**(4):723–728.
17. Kocher P, Jaffe J, Jun B. Differential power analysis. In *Advances in Cryptology–CRYPTO 1999*, Vol. 1666, LNCS. Springer: Berlin / Heidelberg, 1999; 789–789.
18. Messerges TS, Dabbish EA, Sloan RH. Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers* 2002; **51**(5):541–552.
19. Kasper T, Oswald D, Paar C. Side-channel analysis of cryptographic rfids with analog demodulation. In *RFIDSEC 2012*, Vol. 7055, Juels A, Paar C (eds), LNCS. Springer: Berlin / Heidelberg, 2012; 61–77.
20. Song R. Advanced smart card based password authentication protocol. *Computer Standards & Interfaces* 2010; **32**(5):321–325.
21. Chen B, Kuo W, Wuu L. Robust smart-card-based remote user password authentication scheme. *International Journal of Communication Systems* 2012. DOI: 10.1002/dac.2368.
22. Wen F, Li X. An improved dynamic ID-based remote user authentication with key agreement scheme. *Computers & Electrical Engineering* 2012; **38**(2):381–387.
23. Nam J, Kim S, Won D. Security analysis of a nonce-based user authentication scheme using smart cards. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 2007; **90**(1):299–302.
24. Xiang T, Wong K, Liao X. Cryptanalysis of a password authentication scheme over insecure networks. *Journal of Computer and system Sciences* 2008; **74**(5):657–661.
25. Tapiador JE, Hernandez-Castro JC, Peris-Lopez P, Clark JA. Cryptanalysis of song's advanced smart card based password authentication protocol. *CoRR* 2011; **abs/1111.2744**.
26. Shim K. Security flaws in three password-based remote user authentication schemes with smart cards. *Cryptologia* 2012; **36**(1):62–69.
27. He D, Wu S. Security flaws in a smart card based authentication scheme for multi-server environment. *Wireless Personal Communications* 2012. DOI: 10.1007/s11277-012-0696-1.
28. Yeh K, Lo N, Li Y. Cryptanalysis of Hsiang-Shih's authentication scheme for multi-server architecture. *International Journal of Communication Systems* 2011; **24**(7):829–836.
29. Ma CG, Wang D, Zhao P, Wang YH. A new dynamic ID-based remote user authentication scheme with forward secrecy. In *APWeb'12*, Vol. 7234, Wang H, Zou L, Huang G, He J, Pang C, Zhang H, Zhao D, Yi Z (eds), LNCS. Springer: Berlin / Heidelberg, 2012; 199–211.
30. Wang D, Ma CG, Zhao S, Zhou C. Cryptanalysis of two dynamic id-based remote user authentication schemes for multi-server architecture. In *Proceedingg of 6th International Conference on Network and System Security (NSS 2012)*, Vol. 7645, Xu L, Bertino E, Mu Y (eds), LNCS. Springer: Berlin / Heidelberg, 2012; 462–475.
31. Wang D, Ma CG, Zhao S, Zhou C. Secure password-based remote user authentication scheme with non-tamper resistant smart cards. In *9th IFIP International Conference on Network and Parallel Computing (NPC 2012)*, Vol. 7513, Park JJ (ed.), LNCS. Springer: Berlin / Heidelberg, 2012; 110–118.
32. Florencio D, Herley C. A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web*. ACM: New York, NY, USA, 2007; 657–666.
33. Klein DV. Foiling the cracker: a survey of, and improvements to, password security. *Proceedings of the 2nd USENIX Security Workshop*, Anaheim, CA, USA. Berkeley, CA, USA: USENIX Association, August 1990; 5–14.
34. Dell'Amico M, Michiardi P, Roudier Y. Password strength: an empirical analysis. *Proceedings of INFOCOM 2010,* IEEE, San Diego, CA, USA, May 2010; 1–9.
35. Bao F, Deng R. Privacy protection for transactions of digital goods. In *ICICS 2001*, Vol. 2229, Qing S, Okamoto T, Zhou J (eds), LNCS. Springer: Berlin / Heidelberg, 2001; 202–213.
36. Tang C, Wu D. Mobile privacy in wireless networks-revisited. *IEEE Transactions on Wireless Communications* March 2008; **7**(3):1035–1042.

DOI: 10.1002/dac

37. Das M, Saxena A, Gulati V. A dynamic ID-based remote user authentication scheme. *IEEE Transactions on Consumer Electronics* 2004; **50**(2):629–631.
38. Wu T. A real-world analysis of kerberos password security. *Proceedings of NDSS'99,* Internet Soc., San Diego, CA, USA, March 1998; 1–14.
39. Bonneau J. The science of guessing: analyzing an anonymized corpus of 70 million passwords. *33th IEEE Symposium on Security and Privacy (S&P 2012),* IEEE Computer Society, San Francisco, CA, USA, May 2012; 538–552.
40. Li X, Xiong Y, Ma J, Wang W. An enhanced and security dynamic identity based authentication protocol for multi-server architecture using smart cards. *Journal of Network and Computer Applications* 2012; **35**(2):763–769.
41. Wang RC, Juang WS, Lei CL. Robust authentication and key agreement scheme preserving the privacy of secret key. *Computer Communications* 2011; **34**(3):274–280.
42. Ahmed M, Lakshmi D, Sattar S. Cryptanalysis of a more efficient and secure dynamic ID-based remote user authentication scheme. *International Journal of Network Security & Its Applications* 2009; **1**(3):32–37.
43. He D, Chen J, Zhang R. Weaknesses of a dynamic id-based remote user authentication scheme. *International Journal of Electronic Security and Digital Forensics* 2010; **3**(4):355–362.
44. Sood S, Sarje A, Singh K. A secure dynamic identity based authentication protocol for multi-server architecture. *Journal of Network and Computer Applications* 2011; **34**(2):609–618.
45. Halevi S, Krawczyk H. Public-key cryptography and password protocols. *ACM Transactions on Information and System Security (TISSEC)* 1999; **2**(3):230–268.
46. Li X, Qiu W, Zheng D, Chen K, Li J. Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards. *IEEE Transactions on Industrial Electronics* 2010; **57**(2):793–800.
47. Chen T, Hsiang H, Shih W. Security enhancement on an improvement on two remote user authentication schemes using smart cards. *Future Generation Computer Systems* 2011; **27**(4):377–380.
48. Park D, Boyd C, Moon SJ. Forward secrecy and its application to future mobile communications security. In *PKC 2000*, Vol. 1751, Imai H, Zheng Y (eds), LNCS. Springer: Berlin / Heidelberg, 2000; 433–445.
49. Kim J, Choi H, Copeland J. Further improved remote user authentication scheme. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 2011; **94**(6):1426–1433.

AUTHORS' BIOGRAPHIES

Chun-Guang Ma received his PhD degree in cryptography from Beijing University of Posts and Telecommunications in 2005. Currently, he is a full-time Professor and a PhD candidate supervisor in the Department of Computer Science and Technology, Harbin Engineering University and a director of Chinese Association for Cryptographic Research. His research interests include cryptography, information security, and wireless sensor networks.

Ding Wang received his BS Degree in Information Security from Nankai University, China, in 2008. And then he went to Information Engineering University of PLA to work toward Information Security Engineering. Currently, he is under the supervision of Prof. Chun-Guang Ma. He has published more than 20 research papers in refereed international journals and conferences. His research interests include cryptographic protocols, provable security, and wireless network security.

Sen-Dong Zhao received his BS Degree in Computer Science from Northeast Dianli University, China, in 2009. Then, he joined Baidu Inc., the largest Chinese language search platform, and served as an R&D engineer. Currently, he is pursuing an MS degree in Information Security from Harbin Engineering University, China. His research interests include information security and information retrieval.

DOI: 10.1002/dac