On the (in)security of some smart-card-based password authentication schemes for WSN[⋆]

Ding Wang[1,2] and Chunguang Ma[2]

[1] School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China
[2] School of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China
wangdingg@mail.nankai.edu.cn

Abstract. In this study, we investigate a temporal-credential-based password authentication scheme introduced by Xue et al. in 2012. This protocol only involves hash and XOR operations and thus is suitable for the resource-constrained WSN environments where an external user wants to obtain real-time data from the sensor nodes inside WSN. However, notwithstanding their security arguments, we point out that Xue et al.'s protocol is still vulnerable to smart card security breach attack and privileged insider attack, and fails to preserve user anonymity. The proposed cryptanalysis discourages any practical use of the scheme under investigation and reveals some subtleties and challenges in designing this type of schemes. Remarkably, using Xue et al.'s scheme as a case study, we further put forward a principle: public-key techniques are indispensable to password-based authentication schemes using non-tamper-resistant smart cards for WSN. We hope that, by following this principle, similar mistakes repeated in the past can be avoided in the future.

Keywords: Wireless sensor networks, Cryptanalysis, Authentication protocol, Smart card, Non-tamper resistant.

1 Introduction

With the rapid development of micro-electromechanical systems and wireless network technologies, wireless sensor networks (WSN) have attracted increasing interest due to its wide range of applications from battlefield surveillance to civilian applications , e.g., environmental monitoring, real-time traffic control, industrial process monitoring and control, healthcare monitoring and home automation. In many critical applications, external users are generally interested in accessing real-time information from sensor nodes. To enable the external users to access the real-time data directly from the desired nodes inside WSN without involving the base station or gateway node when demanded, it is of great concern to protect the users and systems' security and privacy from malicious adversaries. Accordingly, user authentication becomes an essential security mechanism for the user to be first authorized to the nodes as well as the base station (or the gateway node) before allowing the user to access data. Generally speaking, authentication factors are grouped into three categories [40]: 1) what you have (e.g., tokens, smart card, portable storage devices); 2) what you know (e.g., passwords, PINs, private keys); and 3) who you are (e.g., fingerprints, iris). Among the numerous methods based on one or more of these three types, the combination of the first two factors is one of the most popular and effective approaches for authentication in security-critical applications [4] such as e-commerce, e-banking and e-health services.

[⋆] Part of this work has been submitted to IEEE for possible publication.

In 2009, M.L. Das [7] proposed the first password authentication scheme using smart cards to provides mutual authentication between the external user, gateway node and the sensor node. However, shortly after this two-factor authentication [59] scheme was presented, it is found susceptible to various attacks, such as insider attack, impersonation attacks, offline password-guessing attack, GW-node bypassing attack and node compromise attack, by Khan and Alghathbar [21], Chen and Yeh [5] and He et al. [15], respectively. Accordingly, several improvements over Das's two-factor authentication scheme were proposed, typical ones include [5, 15, 21, 32, 60]. Unfortunately, most of these improvements are demonstrated insecure short after they were put forward [14, 29, 45], which outlines the needs for intensive further research.

In 2012, Xue et al. [58] pointed out that previous authentication schemes for real-time data access in WSN have various security flaws being overlooked, and propose a lightweight temporal-credential-based mutual authentication and key agreement scheme for practical use. As with A.K. Das et al.'s scheme [6], this protocol also only involves hash and XOR operations, with no additional symmetric encryption or asymmetric computations, and thus it is very efficient. Although the scheme has been equipped with a long list of heuristic security arguments, we demonstrate that it still cannot achieve the claimed security goals: 1) it is vulnerable to smart card security breach attack; 1) it is vulnerable to privileged-insider attack; 3) it fails to achieve user anonymity; and 4) the registration phase is insecure for no integrity assurance is provided.

The remainder of this paper is organized as follows: in Section 2, we review Xue et al.'s scheme. Section 3 discusses the practical abilities of the adversary. Section 4 describes the weaknesses of Xue et al.'s scheme. Section 5 discusses the principle learned from the cryptanalysis and Section 6 concludes the paper.

2 Review of Xue et al.'s scheme

In this section, we briefly review the temporal-credential-based two-factor authentication scheme for wireless sensor networks proposed by Xue et al. [58] in 2012. Xue et al.'s protocol also involves three participants, i.e., the user (U_i), the gateway node (GWN) and the sensor node (S_j). It should be noted that GWN is not only responsible for the registration but also involved in the authentication process of U_i and S_j. There are three phases in their protocol: registration, login, authentication and session key agreement. In the following, we employ the notations listed in Table 1 and we will follow the original notations in Xue et al.'s scheme as closely as possible. As we shall see, the descriptions of the scheme are rather tedious, but we manage to go through the jungle of protocol specification and to identify several serious security flaws.

2.1 Registration phase

Before the running of this phase, it is supposed that each user already has a secure password shared with GWN. More precisely, the identity of the user and the hash value of her password have already been stored on GWN side. And each sensor node is also with password preconfigured, the hash of which is stored on GWN side. This phase can be divided into two parts, namely, the user registration and the sensor node registration.

1) **User registration**

Step RU1. U_i gets the current timestamp TS_1, and computes $VI_i = H(TS_1 \parallel H(PW_i))$
Step RU2. $U_i \rightarrow GWN$: $\{ID_i, TS_1, VI_i\}$.

Table 1. Notations

Symbol	Description
U_i	i^{th} user
BS	Base station
$\mathcal{A}$	the adversary
CH_j	cluster head in the j-th cluster
ID_i	identity of user U_i
PW_i	password of user U_i
ID_{CH_j}	identity of cluster head CH_j
GWN	the gateway node
S_j	j^{th} sensor node
SID_j	identity of sensor node S_j
K_{GWN-U}	secret parameter only known to GWN
K_{GWN-S}	secret parameter only known to GWN
E/D	symmetric key encryption/decryption algorithm
X_s	secret parameter maintained by BS
X_A	secret parameter shared between the user and BS
y	a secret random number only known to the user
$\oplus$	the bitwise XOR operation
$\|\|$	the string concatenation operation
$h(\cdot)$	collision free one-way hash function
$A \rightarrow B : C$	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

Step RU3. After receiving the registration request, GWN checks the validity of TS_1. If $T^*_{GWN} - TS_1 > \Delta T$, GWN rejects and sends a "REJ" message back to U_i, where T^*_{GWN} denotes the timestamp on GWN side and ΔT is the predefined admissible time-interval. GWN continues to extract $H(PW_i)$ corresponding to ID_i from its background database, then computes $VI_i^* = H(TS_1||H(PW_i))$ and checks whether $VI_i^* \stackrel{?}{=} VI_i$. If the equality does not hold, GWN rejects; otherwise, GWN further computes $P_i = H(ID_i||TE_i)$, $TC_i = H(K_{GWN-U})||P_i||TE_i$ and $PTC_i = TC_i \oplus H(PW_i)$, where TE_i is the expiration time of the temporal credential set by GWN or the trust third party (TTP), K_{GWN-U} is GWN's private key and TC_i is the temporal credential for U_i issued by GWN. At last, GWN personalizes the smart card for U_i with the parameters $\{H(\cdot), ID_i, H(H(PW_i)), TE_i, PTC_i\}$.

Step RU4. $GWN \rightarrow U_i$: A smart card containing security parameters $\{H(\cdot), ID_i, H(H(PW_i)), TE_i, TC_i\}$.

2) **Sensor node registration**

Before the deployment, each sensor node S_j is configured with its identity SID_j and its random password PW_j. After the deployment, the following steps are performed:

Step RS1. Sensor node S_j gets its current timestamp TS_2 and computes $VI_j = H(TS_2||H(PW_j))$.

Step RS2. $S_j \rightarrow GWN : \{SID_j, TS_2, VI_j\}$.

Step RS3. After receiving the registration request, GWN checks whether the transmission delay is within the allowed time interval ΔT. If $T^*_{GWN} - TS_2 > \Delta T$, GWN sends a "REJ" message back to S_j, where T^*_{GWN} is the current timestamp on GWN side. Otherwise, GWN continues to extract $H(PW_j)$ corresponding to SID_j from its background database. Then, GWN computes $VI_j^* = H(TS_2||H(PW_j))$ and verifies whether $VI_j^* \stackrel{?}{=} VI_j$. If the equality does not hold, GWN rejects; otherwise, GWN

further computes $TC_j = H(K_{GWN-S}||SID_j)$, $REG_j = H(H(PW_j)||TS_3) \oplus TC_j$, where TS_3 is the current timestamp on GWN side, K_{GWN-S} is GWN's private key and TC_j is the temporal credential for S_j issued by GWN. Then GWN sends TS_3 and REG_j to the sensor node S_j.

Step RS4. $GWN \rightarrow S_j : \{TS_3, REG_j\}$.

Step RS5. After receiving the response from GWN, S_j first checks the validity of TS_3 and then computes its temporal credential $TC_j = REG_j \oplus H(H(PW_j)||TS_3)$, and stores TC_j in its memory.

2.2 Login phase

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

Step L1. U_i inserts her smart card into a card reader and inputs her identity ID_i^* and password PW_i^*.

Step L2. The smart card verifies whether the input ID_i^* equals the stored ID_i and whether $h(PW_i^*)$ equals the stored $h(PW_i)$. If both verifications hold, it indicates that U_i is a legal card holder. Then, the smart card computes $TC_i = PTC_i \oplus H(PW_i)$.

2.3 Authentication and session key agreement phase

This phase aims to achieve the goal of mutual authentication among U_i, GWN and S_j. Meanwhile, a session key is negotiated between U_i and S_j.

Step A1. U_i gets the current timestamp TS_4 and chooses a random number K_i. Then U_i computes $DID_i = ID_i \oplus H(TC_i \| TS_4)$, $C_i = H(H(ID_i \| TS_4) \oplus TC_i)$ and $PKS_i = K_i \oplus H(TC_i \| TS_4 \| ``000'')$. It should be noted that $H(TC_i \| TS_4 \| ''000'')$ is different from $H(TC_i \| TS_4)$, which is ensured by the feature of hash function.

Step A2. $U_i \rightarrow GWN$: $\{DID_i, C_i, PKS_i, TS_4, TE_i, P_i\}$.

Step A3. GWN first checks the validity of TS_4 and computes $ID_i = DID_i \oplus H(H(K_{GWN-U} \| P_i \| TE_i) \| TS_4), P_i^* = H(ID_i \| TE_i)$, $TC_i = H(K_{GWN-U} \parallel P_i^* \| TE_i)$ and $C_i^* = H(H(ID_i^*)||TS_4) \oplus TC_i^*$.

Step A4. GWN checks whether $C_i^* \neq C_i$ or $P_i^* \neq P_i$. If either check holds, the authentication request is rejected. Otherwise, GWN accepts U_i's login request and computes $K_i = PKS \oplus H(TC_i||TS_4||''000'')$.

Step A5. GWN chooses a nearby suitable sensor node as the accessed sensor node, say S_j, whose identity is SID_j, and computes $TC_j = H(K_{GWN-S} \parallel SID_j)$, $DID_{GWN} = ID_i \oplus H(DID_i \parallel TC_j||TS_5)$, $C_{GWN} = H(ID_i \parallel TC_j \parallel TS_5)$ and $PKS_{GWN} = K_i \oplus H(TC_j \parallel TS_5)$, where TS_5 is the current timestamp.

Step A6. $GWN \rightarrow S_j : \{TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}\}$

Step A7. After receiving the message from GWN, S_j checks the validity of TS_5. If it is not valid, the session is terminated. Otherwise, S_j computes $ID_i = DID_{GWN} \oplus H(DID_i||TC_j||TS_5)$ and $C_{GWN}^* = H(ID_i||TC_j\| TS_5)$. If $C_{GWN}^* \neq C_{GWN}$, S_j rejects. Otherwise, S_j is confirmed that the received message is from the legitimate GWN, and computes $K_i = PKS_{GWN} \oplus H(TC_j||TS_5)$. Then S_j gets the current timestamp TS_6 and chooses a random number K_j. Then S_j computes $C_j = H(K_j||D_i||SID_j||TS_6)$ and $PKS_j = K_j \oplus H(K_i||TS_6)$.

Step A8. $S_j \rightarrow U_i, GWN : \{SID_j, TS_6, C_j, PKS_j\}$

Step A9. After receiving the response from S_j and checking the validity of TS_6, U_i and GWN can separately compute $K_j = PKS_j \oplus H(K_i||TS_6)$ and $C_j^* = H(K_j||ID_i||SID_j||TS_6)$. For GWN, if $C_j^* = C_j$, it is confirmed that S_j is a legitimate sensor node. For the user U_i, if $C_j^* = C_j$, she is confirmed that both S_j and GWN are legitimate. U_i and S_j can separately compute the shared session key $KEY_{ij} = H(K_i \oplus K_j)$.

Finally, the user U_i and the sensor node S_j agree on a common session key $SK = H(K_i \oplus K_j)$ for securing ensuing data communications.

3 Discussions on the adversary's capabilities

There are four assumptions explicitly made in Xue et al.'s scheme [6]:

(i) The sensitive data stored in the sensor nodes as well as cluster heads can be revealed once they are captured by an adversary $\mathcal{A}$.

(ii) The secret parameters stored in the smart card can be revealed when $\mathcal{A}$ somehow (e.g. picking up, stealing) gets (temporary) access to a legitimate user's smart card.

(iii) $\mathcal{A}$ has total control over the communication channel among the user U_i, the gateway node GWN and the sensor node S_j. In other words, the attacker can intercept, block, delete, insert or alter any messages exchanged in the channel. However, $\mathcal{A}$ is restricted from breaking the cryptographic primitives (e.g., encryption, Hash).

(iv) The user-memorable passwords (and identities) are weak (i.e., of low entropy), and drawn from a space which can be offline enumerated by $\mathcal{A}$.

Some remarks. It is worth noting that the above four assumptions, which are also made in most existing schemes [6, 11, 21, 28, 30, 47, 61], are indeed reasonable:

1) Assumptions *i* is practical, for nodes and cluster heads are usually not equipped with tamper-resistant hardware due to cost constraints, and hence once a node is captured by an attacker, all the stored sensitive parameters can be revealed by $\mathcal{A}$ [3]. However, we assume that the gateway node (or the so called base station) is a trusted authority, which in any case will not be compromised by $\mathcal{A}$.

2) Assumptions *ii* seems quite contrary to the popular belief, but it is reasonable when taking into consideration of the state-of-the-art side-channel attack techniques for contact smart cards [24,35–37] (or for contactless smart cards [18,19]), reverse engineering [1,39] and software attacks (launched on software-supported card, e.g., Java Card) [31]. To make matters worse, users, it seems, are apt to lose their smart card! Some recent studies [38,41] on the usability of real-life two-factor authentication systems reported that, more than 50% users have lost their smart card in the card reader at least once during an investigation period of merely several weeks. Consequently, it is more prudent and desirable to assume that, once the smart card is lost, the sensitive data in its memory is revealed, even though the extraction of data from smart cards is beyond the reach of an amateur. Note that, this does not necessarily suggest that smart cards are completely non-tamper resistant as the common USB sticks. Rather, we mean smart cards are sometimes, i.e. when lost, non-tamper resistant, while in other less catastrophic situations, they could not be tampered. Interestingly, some studies like [44, 59] even go the extreme to claim that "we put aside any special security feature that could be supported by the smart card".

Here we argue that, our "conditional" tamper-resistance assumption of smart cards is more practical and reasonable than such an extreme assumption made in [44, 59]. Firstly, we give a concrete example. A victim's password may be exposed easily when she inserts her card into a malicious card reader, however, the secret data in her card shall not be extracted on the same occasion, because the adversary can not employ the special tools and/or setup professional platforms that are required to launch a side-channel attack while the user is at the scene. Secondly and what's most crucial, if the extreme assumption holds, now one question may naturally arise: As the smart cards are deemed completely non-tamper resistant, what's the advantage of using smart cards as compared to using cheap USB memory cards?

Having justified the reasonableness of our "conditional" non-tamper resistance assumption of the smart cards, we proceed to answer the above question in the following. As tamper resistance is part of the core feature of smart cards, though the countermeasures to defer the side-channel/reverse-engineering attempts may not be so satisfactory, they can prevent the common non-invasive attacks, e.g., unauthorized read/write attempts of a trojan. Hence, even deployed in completely un-trusted environments, a well-designed smart-card-based scheme may not be endangered, such as the two general two-factor authentication schemes [49, 56]. In contrast, since a memory card does not have its own CPU and cannot conduct cryptographic operations, the user has to insert it into a trusted computer; Otherwise, the malicious computer could just intercept the password and copy the content on the memory stick and masquerade the user in future [54]. As far as we know, this is the first in-depth investigation that well explains why most two-factor schemes [6, 11, 16, 17, 33] prefer smart cards rather than cheap USB memory sticks, even if the adversary is assumed to be able to reveal the secret information from a lost smart card.

3) Assumption *iii* is consistent with the common adversary model for distributed computing, called the standard model or the Dolev-Yao model [10]. In reality, the capabilities of $\mathcal{A}$ are powerful but not omnipotent, it is often called "a feasible attacker" [13].

4) Assumption *iv* reflects the reality that users are allowed to choose their passwords at will during the password change phase and the registration phase, and they are usually apt to choose passwords that are related to their personal life [12], such as meaningful dates, phone numbers or license plate numbers. In other words, the user-chosen human-memorable passwords tend to be "weak passwords" [4, 9, 57]. Moreover, although password-composition policies can aid to increase password strength, it has been reported that the effectiveness of these policy mechanisms is not very satisfactory [20,55]: it is often hampered by inconsistent and even contradictory requirements across systems and web sites, or by circumvention strategies employed by the users. The user's identity, chosen in the way with the password, is often confined to a predefined format and kept static in its entire life-cycle, and thus it is as weak as (probably weaker than) user's password. Moreover, a determined attacker can probably learn the victim user's identity if she knows some information about the victim or gets access to the victim's smart card. In a nutshell, both user identity and password are human-memorable short strings but not high entropy cryptographic keys, and they fall into two corresponding dictionaries of small size.

4 Cryptanalysis of Xue et al.'s scheme

In the following discussions of the security pitfalls of Xue et al.'s scheme, based on the above four assumptions, we assume that an adversary can extract the secret parameters $\{H(\cdot), ID_i, H(H(PW_i)), TE_i, TC_i\}$ stored in the legitimate user's smart card, and could also intercept or block the exchanged messages $\{DID_i, C_i, PKS_i, TS_4, TE_i, P_i, TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}\}$ during the login and authentication processes. Although Xue et al.'s scheme has many attractive properties, such as provision of mutual authentication between the external user, gateway node and sensor node, high efficiency and key agreement, it fails to achieve many of the claimed security goals: 1) it cannot provide identity protection; 2) it is susceptible to smart card security breach attack (stolen smart card attack); 3) it fails to achieve user anonymity; 4) the registration phase is vulnerable as there is no integrity assurance provided.

4.1 No provision of identity protection

A protocol with identity protection protects an individual's sensitive personal information, such as social circle, preferences, lifestyles, shopping patterns, etc., from being acquired by an adversary through analyzing the login information, the services or the resources being accessed [2,53]. Moreover, in mobile environments, the leakage of user-specific information may facilitate an unauthorized entity to track the user's current location and login history [46]. Hence, identity protection is a highly admired feature of remote user authentication schemes.

To provide identity protection, a feasible approach is to adopt the "dynamic ID technique" [8, 51]: a user's real identity is concealed in the session-variant pseudo-identities. Authentication schemes that employ this technique are the so-called "dynamic-ID" schemes. And Xue et al.'s scheme falls into this category. However, the following offline identity guessing attack demonstrates that this scheme actually cannot provide identity protection.

Step 1. Intercepts a login request message, say $\{DID_i,\ C_i, PKS_i, TS_4, TE_i,\ P_i\}$, sent by U_i;
Step 2. Guesses the value of ID_i to be ID_i^* from a dictionary space $\mathcal{D}_{id}$.
Step 3. Computes $P_i^* = h(ID_i^* \| TE_i)$, where TE_i is intercepted as in Step 1.
Step 4. Verifies the correctness of ID_i^* by checking if the computed P_i^* is equal to the intercepted P_i.
Step 5. Repeats the above steps until the correct value of ID_i is found.

Let $|\mathcal{D}_{id}|$ denotes the number of identities in $\mathcal{D}_{id}$. The running time of the above attack procedure is $\mathcal{O}(|\mathcal{D}_{id}| * T_H)$, where T_H is the running time for Hash operation. Since users' identities are human-memorable short strings but not high-entropy keys, that is to say, they are often drawn from a dictionary of small size. What's more, user's identity is static and often confined to a predefined format, and it is more easily guessed than user's password. As $|\mathcal{D}_{id}|$ is very limited in practice, e.g. $|\mathcal{D}_{id}| \leq |\mathcal{D}_{pw}| \leq 10^6$ [9, 25], the above attack can be completed in polynomial time. Note that, in this user-identity breach attack, the adversary only needs to keep an eye over the public channel and it does not involve any special cryptographic operations (e.g., power analysis). In this regard, the proposed attack is very practical and effective.

4.2 Smart card security breach attack

Let us consider the following scenarios. In case a legitimate user U_i's smart card is stolen by the adversary $\mathcal{A}$, and the stored secret parameters $H(\cdot), ID_i$ and $H(H(PW_i))$ can be extracted. Note that this assumption is reasonable as described in Assumption *ii* and it is also explicitly made in Xue et al.'s scheme. With the extracted $H(H(PW_i))$, $\mathcal{A}$ can successfully guess the password of U_i as follows:

Step 1. Guesses the value of PW_i to be PW_i^* from a dictionary space $\mathcal{D}_{pw}$.
Step 2. Computes $HK^* = H(H(PW_i^*))$.
Step 3. Verifies the correctness of PW_i^* by checking if the computed HK^* is equal to the received $H(H(PW_i))$.
Step 4. Repeats the above steps until the correct value of PW_i is found.

Let $|\mathcal{D}_{pw}|$ denote the number of passwords in the password space $\mathcal{D}_{pw}$. Then the running time of the attacker $\mathcal{A}$ is $\mathcal{O}(|\mathcal{D}_{pw}| * 2T_H)$, where T_H is the running time for Hash operation. So, the time for $\mathcal{A}$ to recover U_i's password is a linear function of the number of passwords in the password space. Since the password space is limited in practice, e.g., $|\mathcal{D}_{pw}| = 10^6$ [9, 25], U_m may recover the password in seconds on a PC.

4.3 Privileged-insider attack

As U_i simply submits the hashed value of her password, i.e. $H(H(PW_i))$, to the gateway node GWN in the registration phase, a privileged-insider of GWN can easily derive U_i's password PW_i using the same attack procedure with above smart card security breach attack.

Now, if U_i uses this PW_i to access other systems for her convenience, the malicious insider can impersonate U_i to login by abusing the legitimate users password and thus gets access to other systems [27]. Therefore, Xue et al.'s scheme is susceptible to privileged-insider attack.

4.4 No integrity assurance in the registration phase

In [58], Xue et al. explicitly stated that, in the registration phase, U_i and S_j communicate with GWN " in an open and public environment." In the light of this statement, we find there is no integrity assurance in the registration phase: take Step RS4 for example, what will happen if an attacker intercepts $\{TS_3, REG_j\}$ and substitutes REG_j with a random value X? It is not difficult to see that, on receiving $\{TS_3, X\}$, S_j will find no abnormality for there is no integrity check. As a result, S_j will unwittingly compute and store the wrong TC_j, and the subsequent authentication involving S_j will never succeed.

5 The public-key principle for two-factor authentication in WSN

Since sensor nodes and smart cards are typically resource-constrained devices, the protocol designers are faced with the hard task of reconciling security, efficiency and functionality requirements, and often must make design decisions that are seemingly well motivated but may have unintended consequences. As it is widely accepted that the traditional certificate-based authentication schemes are not suitable for WSN and asymmetric cryptographic operations (e.g., modular exponentiation and Elliptic Curve point multiplication) are comparatively expensive, most two-factor authentication schemes for WSN (e.g., [5–7, 15, 28, 30, 32, 47, 58, 58, 61, 62]) swing to the other extreme: they attempt to only adopt non-public-key techniques (e.g., hash functions, symmetric encryptions, XOR operations, MAC operations) to reduce the computational complexity, communication cost and storage overhead while fulfilling the stringent security requirements. However, according to our protocol cryptanalysis experience, this strategy is inviable under the non-tamper resistance assumption of the smart cards.

We have analyzed more than eighty recently proposed smart-cards-based password authentication schemes (some of our cryptanalysis results include [34,48–53], and observed that schemes that do not employ public-key techniques are definitely vulnerable to the smart card security breach attack when the smart cards are assumed to be non-tamper resistant. In other words, all these schemes that only employ non-public-key techniques but claim to be secure against smart card security breach attack are found problematic, some quite recent typical examples include [5, 7, 15, 21, 23, 42, 43].

We show that this is no accident. It is crucial to notice that, under the non-tamper resistance assumption of the smart cards, all the security parameters stored in the smart card can be extracted [19, 26, 37] and thus the smart-card-based password authentication scheme is downgraded to a traditional one-factor (i.e., only password-based) authentication scheme. That is to say, the security of the scheme now only relies on the security of the password. In a seminal work [13], Halevi and Krawczyk investigate the basic principle for constructing secure password-based authentication (the traditional one-factor password authentication) protocols, and provide very strong evidence (with a probability of $\boldsymbol{P} \neq \boldsymbol{NP}$) that, under the common distributed computing adversary model, no password protocol can be free from offline password guessing attack if only symmetric cryptographic primitives are involved. Accordingly, we come to the conjecture that, under the non-tamper resistance assumption of the smart cards, no smart-card-based password protocol (i.e., two-factor authentication [59]) can withstand smart card security breach attack (offline password guessing attack) if the public-key techniques are not employed.

By following this principle, one can easily identify that all these newly proposed two-factor schemes for WSN [6, 28, 30, 32, 47, 58, 61, 62], which are only based on symmetric cryptographic primitives, are inherently unable to withstand smart card security breach attack (offline password guessing attack). To the best of our knowledge, most of these schemes were just made online and have not been cryptanalzed elsewhere. Some of them, like [30, 47, 61] even have been equipped with a formal security proof. And now the countermeasure is obvious: resorting to public-key techniques like [22, 49, 60].

6 Conclusion

In this paper, we have analyzed an efficient password-based authentication scheme using smart cards for WSN without employing any public-key techniques. This scheme is equipped with a claimed proof of security, however, we pointed out that it has various security defects being overlooked. Although there have been ample of works on the security analysis of two-factor authentication schemes for WSN, little (or even no) rationale is given and thus similar mistakes are repeated over and over again. To alleviate this situation, through the cryptanalysis of Xue et al.'s scheme and based on our protocol cryptanalysis experience, we put forward one principle that is helpful to explicate many of the security failures repeated in the past and vital for designing more robust two-factor authentication schemes for WSN in the future.

Acknowledgments. This research was in part supported by the National Natural Science Foundation of China (NSFC) under Grants No. 61170241 and No. 61073042, and the open program of State Key Laboratory of Networking and Switching Technology under Grant No. SKLNST-2009-1-10.

References

1. Amiel, F., Feix, B., Villegas, K.: Power analysis for secret recovering and reverse engineering of public key algorithms. In: SAC 2007. LNCS, vol. 4876, pp. 110–125. Springer (2007)
2. Bao, F., Deng, R.: Privacy protection for transactions of digital goods. In: Qing, S., Okamoto, T., Zhou, J. (eds.) Proceedings of Third International Conference on Information and Communications Security (ICICS 2001), LNCS, vol. 2229, pp. 202–213. Springer Berlin / Heidelberg (2001)
3. Becher, A., Benenson, Z., Dornseif, M.: Tampering with motes: Real-world physical attacks on wireless sensor networks. Springer-Verlag (2006)
4. Bonneau, J.: The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In: 33th IEEE Symposium on Security and Privacy (S&P 2012). pp. 538–552. IEEE Computer Society (2012)
5. Chen, T., Shih, W.: A robust mutual authentication protocol for wireless sensor networks. ETRI journal 32(5), 704–712 (2010)

6. Das, A.K., Sharma, P., Chatterjee, S., Sing, J.K.: A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. Journal of Network and Computer Applications 35(52), 1646–1656 (2012)
7. Das, M.L.: Two-factor user authentication in wireless sensor networks. IEEE Transactions on Wireless Communications 8(3), 1086–1090 (2009)
8. Das, M.L., Saxena, A., Gulati, V.P.: A dynamic id-based remote user authentication scheme. IEEE Transactions on Consumer Electronics 50(2), 629–631 (2004)
9. Dell'Amico, M., Michiardi, P., Roudier, Y.: Password strength: An empirical analysis. In: Proceedings of 29th IEEE Conference on Computer Communications (INFOCOM 2010). pp. 1–9 (march 2010)
10. Dolev, D., Yao, A.: On the security of public key protocols. IEEE Transactions on Information Theory 29(2), 198–208 (1983)
11. Fan, R., He, D., Pan, X., Ping, L.: An efficient and dos-resistant user authentication scheme for two-tiered wireless sensor networks. Journal of Zhejiang University-Science C 12(7), 550–560 (2011)
12. Florencio, D., Herley, C.: A large-scale study of web password habits. In: Proceedings of the Sixteenth International World Wide Web Conference (WWW 2007). pp. 657–666. ACM (2007)
13. Halevi, S., Krawczyk, H.: Public-key cryptography and password protocols. ACM Transactions on Information and System Security 2(3), 230–268 (1999)
14. Han, W.: Weakness of a secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Cryptology ePrint Archive, Report 2011/293 (2011), http://eprint.iacr.org/2011/293
15. He, D., Gao, Y., Chan, S., Chen, C., Bu, J.: An enhanced two-factor user authentication scheme in wireless sensor networks. Ad Hoc & Sensor Wireless Networks 10(4), 361–371 (2010)
16. He, D., Ma, M., Zhang, Y., Chen, C., Bu, J.: A strong user authentication scheme with smart cards for wireless communications. Computer Communications 34(3), 367–374 (2011)
17. Hsieh, W., Leu, J.: Exploiting hash functions to intensify the remote user authentication scheme. Computers & Security 31(6), 791–798 (2012)
18. Hutter, M., Mangard, S., Feldhofer, M.: Power and em attacks on passive 13.56 MHz RFID devices. In: Paillier, P., Verbauwhede, I. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2007, Lecture Notes in Computer Science, vol. 4727, pp. 320–333. Springer Berlin Heidelberg (2007)
19. Kasper, T., Oswald, D., Paar, C.: Side-channel analysis of cryptographic rfids with analog demodulation. In: Juels, A., Paar, C. (eds.) Proceedings of RFIDSec 2012, LNCS, vol. 7055, pp. 61–77. Springer Berlin / Heidelberg (2012)
20. Kelley, P.G., Komanduri, S., Mazurek, M.L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L.F., Lopez, J.: Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In: 33th IEEE Symposium on Security and Privacy (S&P 2012). pp. 523–537. IEEE Computer Society (2012)
21. Khan, M., Alghathbar, K.: Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks. Sensors 10(3), 2450–2459 (2010)
22. Khan, M., He, D.: A new dynamic identity-based authentication protocol for multi-server environment using elliptic curve cryptography. Security and Communication Networks (2012), doi: 10.1002/sec.573
23. Khan, M., Kim, S., Alghathbar, K.: Cryptanalysis and security enhancement of a more efficient & secure dynamic id-based remote user authentication scheme'. Computer Communications 34(3), 305–309 (2011)
24. Kim, T.H., Kim, C., Park, I.: Side channel analysis attacks using am demodulation on commercial smart cards with seed. Journal of Systems and Software 85(12), 2899 – 2908 (2012)
25. Klein, D.V.: Foiling the cracker: A survey of, and improvements to, password security. In: Proceedings of the 2nd USENIX Security Workshop. pp. 5–14 (1990)
26. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) Proceedings of Advances in Cryptology–CRYPTO 1999, LNCS, vol. 1666, pp. 388–397. Springer Berlin / Heidelberg (1999)
27. Ku, W., Chen, S.: Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics 50(1), 204–207 (2004)

28. Kumar, P., Choudhury, A.J., Sain, M., Lee, S.M., Lee, H.J.: Ruasn: A robust user authentication framework for wireless sensor networks. Sensors 11(5), 5020–5046 (2011)
29. Kumar, P., Lee, H.: Cryptanalysis on two user authentication protocols using smart card for wireless sensor networks. In: Wireless Advanced, 2011. pp. 241–245. IEEE (2011)
30. Kumar, P., Lee, S.G., Lee, H.J.: E-sap: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. Sensors 12(2), 1625–1647 (2012)
31. Leroy, X.: Smart card security from a programming language and static analysis perspective. INRIA Rocquencourt & trusted logic, Tecnical Report (2013), available at `http://pauillac.inria.fr/~xleroy/talks/language-security-etaps03.pdf`
32. Li, C., Lee, C., Wang, L., Liu, C.: A secure billing service with two-factor user authentication in wireless sensor networks. International Journal of Innovative Computing, Information and Control 7(8), 4821–4832 (2011)
33. Liao, Y.P., Hsiao, C.M.: A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients. Future Generation Computer Systems 29(3), 886–900 (2013)
34. Ma, C.G., Wang, D., Zhang, Q.M.: Cryptanalysis and improvement of sood et al.s dynamic id-based authentication scheme. In: Ramanujam, R., Ramaswamy, S. (eds.) Proceedings of ICDCIT'12, LNCS, vol. 7154, pp. 141–152. Springer-Verlag (2012)
35. Mangard, S., Oswald, E., Popp, T.: Power analysis attacks: Revealing the secrets of smart cards. Springer-Verlag (2007)
36. Markantonakis, K., Tunstall, M., Hancke, G., Askoxylakis, I., Mayes, K.: Attacking smart card systems: Theory and practice. Information Security Technical Report 14(2), 46–56 (2009)
37. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Examining smart-card security under the threat of power analysis attacks. IEEE Transactions on Computers 51(5), 541–552 (2002)
38. Morse, E., Theofanos, M., Choong, Y., Paul, C., Zhang, A.: NIST-IR-7867 usability of piv smartcards for logical access. Tech. rep., National Institute of Standards and Technology, McLean, VA (2012), doi:`http://dx.doi.org/10.6028/NIST.IR.7867`
39. Nohl, K., Evans, D., Starbug, S., Plötz, H.: Reverse-engineering a cryptographic RFID tag. In: Proceedings of the 17th USENIX Security symposium (USENIX Security 2008). pp. 185–193. USENIX Association (2008)
40. O'Gorman, L.: Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE 91(12), 2021–2040 (2003)
41. Paul, C., Morse, E., Zhang, A., Choong, Y.Y., Theofanos, M.: A field study of user behavior and perceptions in smartcard authentication. In: Campos, P., Graham, N., Jorge, J., Palanque, P., Winckler, M. (eds.) Human-Computer Interaction–INTERACT 2011, LNCS, vol. 6949, pp. 1–17. Springer Berlin Heidelberg (2011)
42. Sood, S.K.: Secure dynamic identity-based authentication scheme using smart cards. Information Security Journal: A Global Perspective 20(2), 67–77 (2011)
43. Sood, S., Sarje, A., Singh, K.: A secure dynamic identity based authentication protocol for multi-server architecture. Journal of Network and Computer Applications 34(2), 609–618 (2011)
44. Sun, D.Z., Huai, J.P., Sun, J.Z., Li, J.X., Zhang, J.W., Feng, Z.Y.: Improvements of juang et al.'s password-authenticated key agreement scheme using smart cards. IEEE Transactions on Industrial Electronics 56(6), 2284–2291 (2009)
45. Sun, D., Li, J., Feng, Z., Cao, Z., Xu, G.: On the security and improvement of a two-factor user authentication scheme in wireless sensor networks. Personal and Ubiquitous Computing (2012), doi: 10.1007/s00779-012-0540-3
46. Tang, C., Wu, D.: Mobile privacy in wireless networks-revisited. IEEE Transactions on Wireless Communications 7(3), 1035 –1042 (march 2008)
47. Vaidya, B., Makrakis, D., Mouftah, H.: Two-factor mutual authentication with key agreement in wireless sensor networks. Security and Communication Networks (2012), doi: 10.1002/sec.517
48. Wang, D., Ma, C.G.: Cryptanalysis and security enhancement of a remote user authentication scheme using smart cards. The Journal of China Universities of Posts and Telecommunications (Elsevier) 19(5), 104–114 (2012)
49. Wang, D., Ma, C.G., Chen, Z., Wang, P.: Robust smart card based password authentication scheme against smart card security breach. Cryptology ePrint Archive, Report 2012/439 (2012), `http://eprint.iacr.org/2012/439.pdf`

50. Wang, D., Ma, C.G., Gu, D.L., Cui, Z.S.: Cryptanalysis of two dynamic id-based remote user authentication schemes for multi-server architecture. In: Xu, L., Mu, Y. (eds.) Proceedings of 6th International Conference on Network and System Security (NSS 2012), LNCS, vol. 7645, pp. 462–475. Springer Berlin / Heidelberg (2012)
51. Wang, D., Ma, C.G., P., W.: Secure password-based remote user authentication scheme with non-tamper resistant smart cards. In: Cuppens-Boulahia, N., Cuppens, F., Garcia-Alfaro, J. (eds.) Proceedings of 26th Annual IFIP Conference on Data and Applications Security and Privacy (DBSec 2012), LNCS, vol. 7371, pp. 114–121. Springer Berlin / Heidelberg (2012)
52. Wang, D., Ma, C.G., Zhao, S., Zhou, C.: Breaking a robust remote user authentication scheme using smart cards. In: Park, J.J. (ed.) Proceedings of the 9th IFIP International Conference on Network and Parallel Computing (NPC 2012), LNCS, vol. 7513, pp. 110–118. Springer Berlin / Heidelberg (2012)
53. Wang, D., Ma, C., Shi, L., Wang, Y.H.: On the security of an improved password authentication scheme based on ecc. In: Liu, B., Ma, M., Chang, J. (eds.) Proceedings of ICICA'12, LNCS, vol. 7473, pp. 181–188. Springer Berlin / Heidelberg (2012)
54. Wang, Y.G.: Password protected smart card and memory stick authentication against off-line dictionary attacks. In: Gritzalis, D., Furnell, S., M., T. (eds.) Proceedings of the 27th IFIP International Information Security and Privacy Conference (SEC 2012), IFIP AICT, vol. 376, pp. 489–500. Springer Boston (2012)
55. Weir, M., Aggarwal, S., Collins, M., Stern, H.: Testing metrics for password creation policies by attacking large sets of revealed passwords. In: Proceedings of the 17th ACM conference on Computer and communications security (CCS 2010). pp. 162–175. ACM (2010)
56. Wu, S.H., Zhu, Y.F., Pu, Q.: Robust smart-cards-based user authentication scheme with user anonymity. Security and Communication Networks 5(2), 236–248 (2012)
57. Wu, T.: A real-world analysis of kerberos password security. In: Proceedings of the 1999 ISOC Network and Distributed System Security Symposium (NDSS 1999). pp. 1–14. Internet Soc. (1999)
58. Xue, K., Ma, C., Hong, P., Ding, R.: A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. Journal of Network and Computer Applications 36(1), 316–323 (2013)
59. Yang, G.M., Wong, D.S., Wang, H.X., Deng, X.T.: Two-factor mutual authentication based on smart cards and passwords. Journal of Computer and System Sciences 74(7), 1160–1172 (2008)
60. Yeh, H., Chen, T., Liu, P., Kim, T., Wei, H.: A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors 11(5), 4767–4779 (2011)
61. Yoo, S.G., Park, K.Y., Kim, J.: A security-performance-balanced user authentication scheme for wireless sensor networks. International Journal of Distributed Sensor Networks (2012), doi: http://dx.doi.org/10.1155/2012/382810
62. Zhang, J., Shankaran, R., Orgun, M.A., Sattar, A., Varadharajan, V.: A dynamic authentication scheme for hierarchical wireless sensor networks. In: Snac, P., Ott, M. (eds.) MobiQuitous 2012, LNICST, vol. 73, pp. 186–197. Springer Berlin Heidelberg (2012)