On the security of two smart-card-based remote user authentication schemes for WSN*

Ding Wang[1,2] and Chun-guang Ma[1]

[1] Harbin Engineering University, Harbin City 150001, China
[2] Automobile Management Institute of PLA, Bengbu City 233011, China
wangdingg@yeah.net

Abstract. Understanding security failures of cryptographic protocols is the key to both patching existing protocols and designing future schemes. The design of secure and efficient remote user authentication schemes for real-time data access in wireless sensor networks (WSN) is still an open and quite challenging problem, though many schemes have been proposed lately. In this study, we analyze two recent proposals in this research domain. Firstly, Das et al.'s scheme is scrutinized, demonstrating its vulnerabilities to smart card security breach attack and privileged insider attack, which are among the security objectives pursued in their protocol specification. Then, 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 provide identity protection. The proposed cryptanalysis discourages any use of the two schemes under investigation in practice and reveals some subtleties and challenges in designing this type of schemes. Besides reporting the security flaws, we put forward a principle that is vital for designing more robust two-factor authentication schemes for WSN.

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

* The abridged version of this paper has been submitted to WCNC 2013, Oct 10, 2012.

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 [29]: 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 [2] such as e-commerce, e-banking and e-health services.

In 2009, M.L. Das [5] 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 [42] 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 [15], Chen and Yeh [3] and He et al. [11], respectively. Accordingly, several improvements over Das's two-factor authentication scheme were proposed, typical ones include [3, 11, 15, 24, 43]. Unfortunately, most of these improvements are demonstrated insecure short after they were put forward [10, 22, 32], which outlines the needs for intensive further research.

In 2012, Xue et al. [41] 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 [4], 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 preserve 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 A.K. Das et al.'s scheme. Section 3 describes the weaknesses of A.K. Das et al.'s scheme. Xue et al.'s scheme is reviewed in Section 4 and the corresponding cryptanalysis is given in Section 5. Section 6 discusses the principle learned from the cryptanalysis and Section 7 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. [41] 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.

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	a secret information maintained by BS
X_A	a secret information 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
$\rightarrow$	a common communication channel
$\Rightarrow$	a secure communication channel

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 pre-configured, 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 $VI_i = H(TS_1 \| H(PW_i))$

Step RU2. $U_i \rightarrow GWN$: $\{ID_i, TS_1, VI_i\}$.

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. The 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 $PKS_i = K_i \oplus H(TC_i \| TS_4 \| \text{“}000''\text{)}$. 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 $ID_i = DID_i \oplus H(H(K_{GWN-U} \| P_i \| TE_i) \| TS_4)$, $P_i^* = H(ID_i \| TE_i)$, $TC_i = H(K_{GWN-U} \| P_i^* \| TE_i)$ 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 $TC_j = H(K_{GWN-S} \ \| \ SID_j)$, $DID_{GWN} = ID_i \oplus H(DID_i \ \| \ TC_j || TS_5)$, $C_{GWN} = H(ID_i \ \| \ TC_j \ \| \ TS_5)$ and $PKS_{GWN} = K_i \oplus H(TC_j \ \| \ TS_5)$, 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 Cryptanalysis of Xue et al.'s scheme

There are four assumptions explicitly made in A.K. Das et al.'s scheme [4]:

(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 once a legitimate user's smart card is somehow obtained (e.g. picked up or stolen) by $\mathcal{A}$.
(iii) $\mathcal{A}$ has total control over the communication channel among the user U_i, the base station BS and the cluster head CH_j. In other words, the attacker can intercept, block, delete, insert or alter any messages exchanged in the channel.
(iv) The user-memorable identities and passwords are weak, i.e., of low entropy.

Note that the above four assumptions, which are also made in the latest works [3,11,15,21,22,24,43], are indeed reasonable: (1) Assumptions *i* and *ii* are practical when taking the state-of-the-art side-channel attack techniques [13, 19, 28] into consideration; (2) Assumption *iii* is consistent with the common adversary model for distributed computing [39]; and (3) Assumption *iv* reveals the reality that users are allowed to choose their passwords at will during the password change phase and registration phase, and the users are usually apt to choose passwords that are related to their personal life [8], such as meaningful dates, phone numbers or license plate numbers, and the human-memorable passwords tends to be "weak passwords" [7, 14, 18]. 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 (maybe weaker than) user's password.

In the following discussions of the security pitfalls of A.K. Das 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 cannot withstand privileged-insider attack; 4) the registration phase is vulnerable as there is no integrity assurance provided.

3.1 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 [1,26]. 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 [33]. 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" [6, 37]: 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. $|\mathcal{D}_{id}| \leq |\mathcal{D}_{pw}| \leq 10^6$ [7, 18], 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.

3.2 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., $|\mathcal{D}_{pw}| = 10^6$ [7,18], U_m may recover the password in seconds on a PC.

3.3 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 [20]. Therefore, Xue et al.'s scheme is susceptible to privileged-insider attack.

3.4 No integrity assurance in the registration phase

In [41], 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.

4 The public-key principle for two-factor authentication

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., [3–5, 11, 21, 23, 24, 34, 41, 41, 44, 45]) 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 [26, 27, 35–39], 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 [3, 5, 11, 15, 17, 30, 31].

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 [13, 19, 28] 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 [9], 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 the 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 (two-factor authentication [42]) 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 [4, 21, 23, 24, 34, 41, 44, 45], which are only based on symmetric cryptographic primitives (e.g., hash functions, block ciphers and exclusive-OR operations), 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 [23, 34, 44] even have been equipped with a formal security proof. And now the countermeasure is obvious: resorting to public-key techniques like [12, 16, 25, 37, 40, 43].

5 Conclusion

In this paper, we have analyzed two efficient password-based authentication schemes using smart cards for WSN without employing public-key techniques. The two schemes are equipped with a claimed proof of security, however, we pointed out that both protocols have 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. In this paper, through the cryptanalysis of two quite recent schemes, i.e. A.K. Das et al.' and Xue et al.'s schemes, 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 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. Bao, F., Deng, R.: Privacy protection for transactions of digital goods. In: Qing, S., Okamoto, T., Zhou, J. (eds.) ICICS'01, LNCS, vol. 2229, pp. 202–213. Springer Berlin / Heidelberg (2001)
2. Bonneau, J., Herley, C., Oorschot, P., Stajano, F.: The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: 33th IEEE Symposium on Security and Privacy (IEEE S&P 2012). IEEE (2012)
3. Chen, T., Shih, W.: A robust mutual authentication protocol for wireless sensor networks. ETRI journal 32(5), 704–712 (2010)
4. 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 (2012), dio:10.1016/j.jnca.2012.03.011
5. Das, M.L.: Two-factor user authentication in wireless sensor networks. Wireless Communications, IEEE Transactions on 8(3), 1086–1090 (2009)
6. 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)
7. Dell'Amico, M., Michiardi, P., Roudier, Y.: Password strength: An empirical analysis. In: 29th IEEE Conference on Computer Communications (INFOCOM 2010). pp. 1–9 (march 2010)
8. Florencio, D., Herley, C.: A large-scale study of web password habits. In: Proceedings of the 16th international conference on World Wide Web (WWW). pp. 657–666. ACM (2007)
9. Halevi, S., Krawczyk, H.: Public-key cryptography and password protocols. ACM Transactions on Information and System Security (TISSEC) 2(3), 230–268 (1999)
10. 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.pdf
11. 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)
12. He, D.: An efficient remote user authentication and key agreement protocol for mobile clientcserver environment from pairings. Ad Hoc Networks 10(6), 1009–1016 (2012)

13. Kasper, T., Oswald, D., Paar, C.: Side-channel analysis of cryptographic rfids with analog demodulation. In: Juels, A., Paar, C. (eds.) RFIDSec 2012, LNCS, vol. 7055, pp. 61–77. Springer Berlin / Heidelberg (2012)
14. Katz, J., Ostrovsky, R., Yung, M.: Efficient and secure authenticated key exchange using weak passwords. Journal of the ACM 57(1), 1–39 (2009)
15. Khan, M., Alghathbar, K.: Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks. Sensors 10(3), 2450–2459 (2010)
16. 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
17. 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)
18. 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)
19. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) Advances in Cryptology–CRYPTO 1999, LNCS, vol. 1666, pp. 388–397. Springer Berlin / Heidelberg (1999)
20. 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)
21. 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)
22. 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)
23. 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)
24. 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)
25. Li, X., Zhang, Y.: A simple and robust anonymous two-factor authenticated key exchange protocol. Security and Communication Networks (2012), doi: 10.1002/sec.605
26. Liu, B., Ma, M., Chang, J. (eds.): LNCS, vol. 7473. Springer Berlin / Heidelberg (2012)
27. 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.) ICDCIT 2012, LNCS, vol. 7154, pp. 141–152. Springer-Verlag (2012)
28. 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)
29. O'Gorman, L.: Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE 91(12), 2021–2040 (2003)
30. Sood, S.K.: Secure dynamic identity-based authentication scheme using smart cards. Information Security Journal: A Global Perspective 20(2), 67–77 (2011)
31. 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)

32. 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
33. Tang, C., Wu, D.: Mobile privacy in wireless networks-revisited. IEEE Transactions on Wireless Communications 7(3), 1035 –1042 (march 2008)
34. Vaidya, B., M.D., Mouftah, H.: Two-factor mutual authentication with key agreement in wireless sensor networks. Security and Communication Networks (2012), doi: 10.1002/sec.517
35. 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)
36. Wang, D., Ma, C.G.: Robust smart card based password authentication scheme against smart card loss problem. Cryptology ePrint Archive, Report 2012/439 (2012), http://eprint.iacr.org/2012/439.pdf
37. 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.) 26th Annual IFIP Conference on Data and Applications Security and Privacy (DBSec 2012), LNCS, vol. 7371, pp. 114–121. Springer Berlin / Heidelberg (2012)
38. Wang, D., Ma, C.G., Zhao, S., Zhou, C.: Cryptanalysis of two dynamic id-based remote user authentication schemes for multi-server architecture. In: Xu, L., Bertino, E., Mu, Y. (eds.) Proceedingg of 6th International Conference on Network and System Security (NSS 2012), LNCS, vol. 7645, pp. 462–475. Springer Berlin / Heidelberg (2012)
39. Wang, D., Ma, C.G., Zhao, S., Zhou, C.: Secure password-based remote user authentication scheme with non-tamper resistant smart cards. In: Park, J.J. (ed.) 9th IFIP International Conference on Network and Parallel Computing (NPC 2012), LNCS, vol. 7513, pp. 110–118. Springer Berlin / Heidelberg (2012)
40. 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)
41. 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 (2012), doi:10.1016/j.jnca.2012.05.010
42. 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)
43. 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)
44. 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:10.1155/2012/382810
45. 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., Seneviratne, A., Akan, O., Bellavista, P., Cao, J., Dressler, F., Ferrari, D., Gerla, M., Kobayashi, H., Palazzo, S., Sahni, S., Shen, X.S., Stan, M., Xiaohua, J., Zomaya, A., Coulson, G. (eds.) MobiQuitous 2012, LNICST, vol. 73, pp. 186–197. Springer Berlin Heidelberg (2012)