Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Advanced smart card based password authentication protocol

Ronggong Song

Network Information Operation, Defence R&D Canada-Ottawa, Ontario K1A0Z4, Canada

ARTICLE INFO

Article history:
Received 20 November 2009
Received in revised form 13 March 2010
Accepted 19 March 2010
Available online 28 March 2010

Keywords:
Remote access control
Smart card
Authentication
Password

ABSTRACT

Password-based authentication is widely used for systems that control remote access to computer networks. In order to address some of the security and management problems that occur in traditional password authentication protocols, research in recent decades has focused on smart card based password authentication. In this paper, we show that the improved smart card authentication scheme proposed by Xu-Zhu-Feng is vulnerable to internal and impersonation attacks. We propose an improvement of their solution, present a new efficient strong smart card authentication protocol, and demonstrate that the new protocol satisfies the requirements of strong smart card authentication and is more efficient.

Crown Copyright © 2010 Published by Elsevier B.V. All rights reserved.

1. Introduction

Password-based authentication has been a commonly used approach for remote access control systems since Lamport [1] proposed a remote authentication scheme based on the passwords in 1981. Traditional password-based remote authentication (e.g., [1,2]) is based on a password table maintained by a server. This approach suffers not only from password attacks such as offline password dictionary attacks and password table tampering and corruption attacks but it also suffers from the cost of protecting and maintaining the password table.

In order to solve these problems and improve the system security, many smart card based password authentication schemes have been proposed in the last decays (e.g., [3–10]). However, these solutions tend to still be vulnerable to some sophisticated attacks such as offline password dictionary searching, observing power consumption, and physically exposing the chip to extract the data it stores. For instance, Xu–Zhu–Feng [3] point out a forgery attack on Lee–Chiu's scheme [5] and a password dictionary attack on Lee–Kim–Yoo's scheme [6]. Song–Korba–Yee [10] discuss vulnerabilities of the schemes proposed by Awasthi–Lal [7], Kumar [8], and Hwang–Li [9]. In addition, most existing smart card based password authentication technologies (e.g., [4,10]) are vulnerable to physical attacks.

Based on previous research, a strong smart card based password authentication scheme should satisfy the following minimum conditions in order to mitigate the more sophisticated attacks:

1. The interactive authentication messages must not reduce the entropy of the password;
2. The remote authentication server should not need to maintain the user's password;
3. The adversary must not be able to attack and gain access to the system by extracting the data stored on the smart card.

where condition (1) protects the system against offline password dictionary attacks, condition (2) can mitigate the password-related attacks and management on the server side, and condition (3) can protect the system against the physical attacks. In addition, an advanced smart card authentication scheme should also be efficient, support mutual authentication, and establish a secure channel between the user and server during authentication.

To match the above conditions, Xu–Zhu–Feng present an improved smart card based password authentication scheme recently in [3]. However, we have found that an internal user can easily make an impersonation attack on the scheme by using data extracted from her own smart card.

In this paper, we detail the potential attack on Xu–Zhu–Feng's scheme and suggest an improvement to resist it. We also present a new efficient strong smart card based password authentication protocol that satisfies not only the minimum conditions but also advanced requirements like efficiency and mutual authentication.

The remainder of the paper is organized as follows. Section 2 discusses the cryptanalysis of Xu–Zhu–Feng's scheme and suggests an improvement. Section 3 presents our new efficient strong smart card based password authentication protocol. Section 4 analyzes the security of the new authentication protocol. Section 5 compares the performance of the new protocol with Xu–Zhu–Feng's scheme and Lee–Chiu's scheme. Section 6 gives our conclusions.

E-mail address: ronggong.song@drdc-rddc.gc.ca.

0920-5489/$ – see front matter. Crown Copyright © 2010 Published by Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2010.03.008

2. Cryptanalysis of the Xu–Zhu–Feng's scheme

2.1. Terminology and notations

Terminology and notations used in the paper are defined as follows.

- ID_A: the user A's identity;
- ID_B: the user B's identity;
- PW_A: the user A's password;
- R_A: a one-time random number created by the user A;
- T_A: the user A's timestamp;
- T_S: the server S's timestamp;
- ΔT: the time threshold predefined by the system;
- $h(\cdot)$: a secure one-way hash function;
- $E_K(M)$: a message M encrypted with session key K;
- x mod p: the residue of x divided by p;
- $\oplus$: the bitwise XOR operation;
- $||$: the concatenation operation;
- p and q: two large prime numbers such that $p = 2q + 1$;
- Z_q^*: the multiplicative group of Z_q;
- Z_q: the ring of integers modulo q;

2.2. Review of Xu–Zhu–Feng's scheme

We briefly review Xu–Zhu–Feng's scheme [3]. The scheme, depicted in Fig. 1, consists of four phases: initial, registration, login, and authentication.

2.2.1. Initial phase

The server selects large prime numbers p and q such that $p = 2q + 1$, and chooses its secret key $x \in Z_q^*$ and a one-way hash function $h(\cdot)$: $\{0, 1\}^* \rightarrow Z_q^*$.

2.2.2. Registration phase

The user submits her identity ID and password PW to the server through a secure channel.

The server computes $B = h(ID)^x + h(PW)$ mod p after receiving the registration request message $\{ID, PW\}$, stores the data $\{ID, B, h(\cdot), p, q\}$ into a new smart card, and issues the smart card to the user.

2.2.3. Login phase

The user attaches her smart card to a device reader and inputs her ID and PW. The smart card chooses a random number $w \in Z_q^*$, sets the timestamp T with the current time, and computes:

$$B' = (B - h(PW))^w \bmod p,$$

$$W = h(ID)^w \bmod p,$$

$$C = h\left(T||B'||W||ID\right).$$

It then sends the login message $\{ID, C, W, T\}$ to the server.

In this scheme, the smart card needs to do a modulus exponentiation computation twice during this phase.

2.2.4. Authentication phase

Upon receiving the login message at time T^*, the server first validates the user's identity ID and the timestamp T by comparing $(T^* - T) \leq \Delta T$, where ΔT is the predefined threshold. The server then computes $B'' = W^x$ mod p and checks whether C equals to $h(T||B''||W||ID)$. If the above verifications go through successfully, the user is authenticated and the server continues the following process. Otherwise, it rejects the login request.

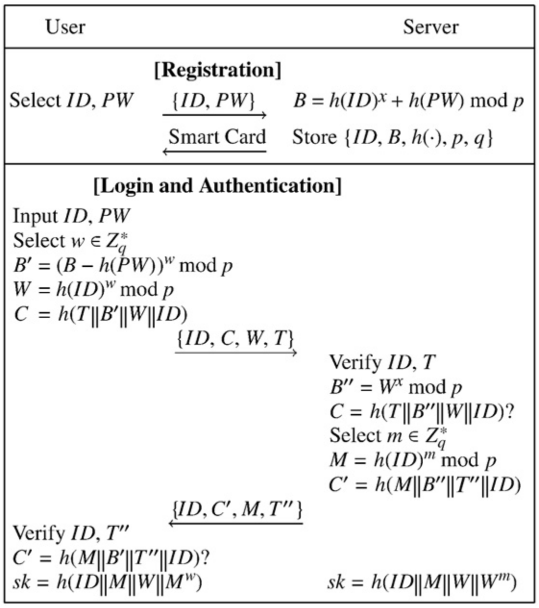
User
Server
[Registration]
Select ID, PW
$\xrightarrow{\{ID,\ PW\}}$
$B = h(ID)^x + h(PW) \bmod p$
$\xleftarrow{\text{Smart Card}}$
Store $\{ID, B, h(\cdot), p, q\}$
[Login and Authentication]
Input ID, PW
Select $w \in Z_q^*$
$B' = (B - h(PW))^w \bmod p$
$W = h(ID)^w \bmod p$
$C = h(T\|B'\|W\|ID)$
$\xrightarrow{\{ID,\ C,\ W,\ T\}}$
Verify ID, T
$B'' = W^x \bmod p$
$C = h(T\|B''\|W\|ID)$?
Select $m \in Z_q^*$
$M = h(ID)^m \bmod p$
$C' = h(M\|B''\|T''\|ID)$
$\xleftarrow{\{ID,\ C',\ M,\ T''\}}$
Verify ID, T''
$C' = h(M\|B'\|T''\|ID)$?
$sk = h(ID\|M\|W\|M^w)$
$sk = h(ID\|M\|W\|W^m)$

Fig. 1. Xu–Zhu–Feng's smart card based password authentication scheme.

The server chooses a random number $m \in Z_q^*$, sets the timestamp T'' to be the current time, computes

$$M = h(ID)^m \bmod p,$$

$$C' = h\left(M||B''||T''||ID\right),$$

and sends the message $\{ID, C', M, T''\}$ to the user.

Upon receiving the message, the smart card validates ID and T'', and compares C' with $h(M||B''||T''||ID)$. If they are equal, the server is authenticated.

The user and server compute $sk = h(ID||M||W||M^w) = h(ID||M||W||W^m)$.

2.3. Attack on Xu–Zhu–Feng's scheme

We show that Xu–Zhu–Feng's scheme is vulnerable to the impersonation attack during user authentication phase. Suppose a user A is trying to impersonate a user B with ID_B. First, A extracts the data B_A stored on her own smartcard. With her own password, she can easily recover $h(ID_A)^x$ by $h(ID_A)^x = B_A - h(PW_A)$ mod p. She then chooses a random number $w \in Z_q^*$, sets the timestamp T with the current time, and computes:

$$B_A' = \left(h(ID_A)^x\right)^w \bmod p,$$

$$W = h(ID_A)^w \bmod p,$$

$$C = h\left(T||B_A'||W||ID_B\right).$$

She then sends the login message $\{ID_B, C, W, T\}$ to the server.

Upon receiving the login message, the server checks the user identity ID_B and the timestamp T. The validation of the user identity ID_B and the timestamp T is successful since the user A uses a valid user identity and chooses the current time as the timestamp. The server then computes $B'' = W^x$ mod p and $C'' = h(T||B''||W||ID_B)$, and checks whether $C = C''$. Since $B'' = W^x = (h(ID_A)^w)^x = B_A'$ mod p, the validation of the data C also is successful. Therefore the attacker A, who pretends as the user B, is successfully authenticated by the server.

Although the user A cannot complete the rest of the process to authenticate the server, unlike a legitimate user, as an attacker she really does not need to authenticate server. She is successful as long as the server accepts her login request.

2.4. Improvement of Xu–Zhu–Feng's scheme

The reason user in Xu–Zhu–Feng's scheme is able to mount an impersonation attack is because the user's identity is independent of the secret value B' in the login phase. In order to resist the impersonation attack, the authentication scheme must ensure that the server must use the user's identity in order to recover B'. Therefore, the simplest way to improve Xu–Zhu–Feng's scheme is to change the calculation of B' to $B' = (B - h(PW))^{w+1} \bmod p$. Now, the server needs to recover B'' as $B'' = (W * h(ID))^{x} \bmod p = B'$, i.e., use W combined with the user's identity ID to recover the secret value B'. No further change is required to keep the security and features of the original protocol.

In the improved protocol, we can see that the user A cannot make the same impersonation attack since $B' = (h(ID_A)^{x})^{w+1} \bmod p \neq (h(ID_A)^{w} * h(ID_B))^{x} \bmod p = B''$. The server can check $C = h(T||B'||W||ID_B)$ does not equal to $h(T||B''||W||ID_B)$ and reject the login request.

3. Our proposed efficient strong smart card based password authentication protocol

As we mentioned, an advanced smart card based password authentication scheme should not only have strong security but also be efficient. However, many existent strong smart card based password authentication schemes such as Hwang–Li's [9], Kumar's [8], Xu–Zhu–Feng's [3], and Lee–Chiu's [5] are based on the famous discrete logarithm problem (DLP) [11] and are very inefficient since they rely on smart cards with severely limited computation capabilities. In order to improve the efficiency and security of the existing smart card based password authentication schemes, we propose an advanced smart card based password authentication protocol as detailed in Fig. 2, which, like Xu–Zhu–Feng's scheme, consists of four phases: initial, registration, login, and authentication.

3.1. Initial phase

The server selects large prime numbers p and q such that $p = 2q + 1$, and chooses its secret key $x \in Z_q^*$, a one-way hash function $h(\cdot)$, and a symmetric key cryptography algorithm with encryption $E(\cdot)$ and decryption $D(\cdot)$ operations. The server keeps both p and x secret.

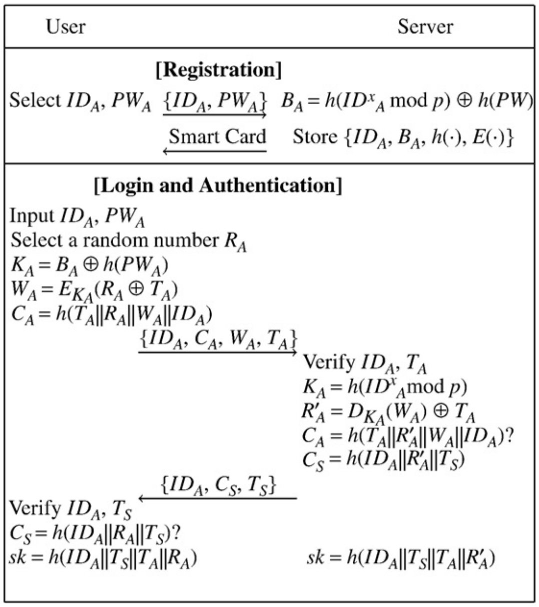
User
Server
[Registration]
Select ID_A, PW_A
$\{ID_A, PW_A\}$
$B_A = h(ID^x{}_A \bmod p) \oplus h(PW)$
Smart Card
Store $\{ID_A, B_A, h(\cdot), E(\cdot)\}$
[Login and Authentication]
Input ID_A, PW_A
Select a random number R_A
$K_A = B_A \oplus h(PW_A)$
$W_A = E_{K_A}(R_A \oplus T_A)$
$C_A = h(T_A||R_A||W_A||ID_A)$
$\{ID_A, C_A, W_A, T_A\}$
Verify ID_A, T_A
$K_A = h(ID^x{}_A \bmod p)$
$R'_A = D_{K_A}(W_A) \oplus T_A$
$C_A = h(T_A||R'_A||W_A||ID_A)$?
$C_S = h(ID_A||R'_A||T_S)$
$\{ID_A, C_S, T_S\}$
Verify ID_A, T_S
$C_S = h(ID_A||R_A||T_S)$?
$sk = h(ID_A||T_S||T_A||R_A)$
$sk = h(ID_A||T_S||T_A||R'_A)$

Fig. 2. Our proposed smart card based password authentication scheme.

3.2. Registration phase

The user A submits her identity ID_A and password PW_A to the server through a secure channel.

After receiving the registration request message $\{ID_A, PW_A\}$, the server computes $B_A = h(ID_A^x \bmod p) \oplus h(PW_A)$, stores the data $\{ID_A, B_A, h(\cdot), E(\cdot)\}$ on a new smart card, and issues the smart card to the user.

3.3. Login phase

The user attaches her smart card to a device reader and inputs ID_A and PW_A. The smart card chooses a random number R_A, sets the timestamp T_A with the user's current system time, and computes:

$$K_A = B_A \oplus h(PW_A),$$

$$W_A = E_{K_A}(R_A \oplus T_A),$$

$$C_A = h(T_A\,|\,|R_A\,|\,|W_A\,|\,|ID_A),$$

where E_{K_A} is the symmetric key encryption operation with the secret key K_A, and the length of R_A should be equal or bigger than the length of the hash function digest in order to not reduce the security of the hash function.

It then sends the login message $\{ID_A, C_A, W_A, T_A\}$ to the server.

In this scheme, the smart card performs one symmetric key encryption computation and two hash computations during this phase, which is more efficient when compared to the modulus exponentiation computations the smart card is required to perform in Xu–Zhu–Feng's scheme.

3.4. Authentication phase

3.4.1. User authentication

Upon receiving the login message at time T^*, the server first validates the user's identity ID_A and the timestamp T_A by comparing $(T^* - T_A) \leq \Delta T$. The server then computes $K_A = h(ID_A^x \bmod p)$ and $R'_A = D_{K_A}(W_A) \oplus T_A$, and checks whether C equals to $h(T_A||R'_A||W_A||ID_A)$, where D_{K_A} is the symmetric key decryption operation with the secret key K_A. If the above verifications go through successfully, the user is authenticated and the server sends the message $\{ID_A, C_S, T_S\}$ to the user, where $C_S = h(ID_A||R'_A||T_S)$ computed by the server and T_S is the server's current system time.

3.4.2. Server authentication

Upon receiving the message, the smart card validates ID_A and T_S, and checks whether C_S equals to $h(ID_A||R_A||T_S)$. If they are equal, the server is authenticated.

3.4.3. Session key establishment

The user and server then compute a shared secret session key $sk = h(ID_A||T_S||T_A||R_A) = h(ID_A||T_S||T_A||R'_A)$.

3.5. Password change

In the new protocol, if the user wants to change her password, she needs to go through the above authentication procedure and let the server authenticate her first with her old password PW_A. After receiving the successful authentication confirmation from the server, the smart card then lets the user input the new password PW'_A and replaces the old B_A with the new $B'_A = B_A \oplus PW_A \oplus PW'_A$.

4. Security analysis of the new protocol

In this section, we analyze the security of the new protocol and demonstrate its strength in terms of security.

4.1. Security of the system secrets

The security of most strong smart card based password authentication schemes (e.g., [3–10]) relies on their system secrets. In the new authentication protocol, only the server contains the system secrets p and x, and the users know nothing about them. It is difficult for an attacker to re-compute or recover the system secrets p and x based solely on the authentication messages. For a user A, even if she extracts the data B_A from her smart card and recovers her secret key K_A with her password, she still needs to solve the famous discrete logarithm problem (DLP) and break the hash function in order to recover the system secrets p and x since $K_A = h(ID_A^x \bmod p)$. Furthermore, even if she breaks the hash function and finds a collision (e.g., w) such that $K_A = h(w)$, it is still difficult for her to know whether $w = ID_A^x \bmod p$ especially without knowing the value p. This property makes it even harder for the attackers to break the system secrets.

4.2. Security of the stored data

In the new authentication protocol, the only secret data stored on the smart card is B_A. The data B_A extracted from the user's smart card does not help an attacker without the user's password PW_A recover the user's secret key K_A since $K_A = B_A \oplus h(PW_A)$. If an attacker is trying to recover K_A by combining offline password dictionary attacks with the extracted data B_A, she needs to find both PW_A and R_A to match $W_A = E_{K_A}(R_A \oplus T_A)$. Since, from the protocol, we know that the only available information is W_A that means the attacker has to process two kinds of attacks—an offline password dictionary attack or a brute force attack to recover the password PW_A and an exhaustive search attack to recover the random number R_A since R_A is a secret random number. If the size of the random number R_A is bigger than the secret key K_A, the attack is no better than just randomly guessing the user's secret key.

4.3. Security of the password

From the new authentication protocol, we can see that the authentication messages $\{ID_A, C_A, W_A, T_A\}$ and $\{ID_A, C_S, T_S\}$ only contain information about $K_A = h(ID_A^x \bmod p)$, ID_A, R_A, T_A, C_S, and T_S. They do not contain any information about the password, satisfying condition (1) from the introduction of not reducing the entropy of the password. Therefore the mutual information of the interactive authentication messages (M) and password (PW) equals to zero in the new authentication protocol, i.e., $I(PW, M) = 0$, meaning that the password and the messages are completely independent. This separation can protect the system against offline attacks such as offline password dictionary searching.

In addition, after registration, the server does not need to retain the user's password for later authentication and password changes. From the password change process, we can see that the server never finds out the user's new password. This property makes the system stronger against some insider attacks and avoids traditional password management issues.

4.4. General online attacks

General online attacks for a smart card based password authentication protocol include impersonation, replay, modify, parallel, and so on.

4.4.1. Impersonation attack

The new authentication protocol can protect the system against impersonation attacks on both the user and the server side. First, on the user side, it is difficult for an attacker to create a correct W_A without the user's secret key K_A. In order to re-compute or recover the user's secret key K_A, the attacker must know the system secrets p and x, or extract the secret data B_A from the user's smart card and know the user's password. As we know, there is no way to prevent the attacker from masquerading as the user if the attacker gets both of the user's smart card and password. Otherwise, it is difficult for the attacker to get the user's secret key K_A. On the server side, the attacker cannot recover the random number without the user's secret key K_A, which means the attacker cannot compute a correct hash value C_S in order to impersonate the server.

4.4.2. Replay attack

The login request message of our proposed protocol uses a random number combined with the timestamp to protect against replay attacks. Unlike in Xu–Zhu–Feng's scheme, even if the attacker recovers the old secret by some means (e.g., B' in Xu–Zhu–Feng's scheme and R_A in the new protocol), she still cannot make a replay attack on the new authentication protocol since W_A combines R_A with the timestamp T_A. The server can easily discover the replay attack by checking the timestamp. For the server authentication message, the user can easily discover the replay attack by checking C_S with current random number and timestamp if the attacker replays an old message from the server side since the user chooses a new random number for each new login request.

4.4.3. Modification attack

As we mentioned, in the new protocol, each authentication message is protected with the hash value and the hash value combines a new secret random number and the timestamp. Without the secret random number, an attacker cannot calculate the correct hash value for the authentication message thus making the successful modification of a message extremely difficult. Any legitimate user or server can easily detect an incorrect hash value just by comparing the new calculated hash value with the received hash value, i.e., the hash value links all the parts of the authentication message together to make a modification attack very hard.

4.4.4. Parallel attack

The new authentication protocol uses the secret random number as a nonce and combines it with the timestamp and hash value to protect the authentication message against parallel attack.

4.5. Secure channel

In the new authentication protocol, with a successful authentication, the user and server establish a shared secret session key and create a secure channel between them.

For security, even if an attacker finds a collision (e.g., w) such that both $C_A = h(T_A||w||W_A||ID_A)$ and $C_S = h(ID_A||w||T_S)$ (finding such a collision is not easy), the attacker still cannot recover the secret session key *phsk* for the secure channel since w may not equal to R_A especially when R_A is large (e.g., bigger than 256 bit), which means that $sk = h(ID_A||T_S||T_A||R_A) \neq h(ID_A||T_S||T_A||w)$.

4.6. Mutual authentication

In our proposed protocol, the user also authenticates the server at the same time the server authenticates the user. The mutual authentication protects against server side impersonation.

5. Performance of our proposed protocol

In order to evaluate the performance of the proposed smart card based password authentication protocol, we compare it with Xu–Zhu–Feng's scheme [3] and Lee–Chiu's scheme [5]. Table 1 gives a brief review of their performance, where the computational

Table 1
Performance comparison of the smart card based password authentication protocols.

Protocols performance	New authen. protocol	Xu et al. authen. protocol	Lee et al. authen. protocol
Registration			
User side	–	–	–
Server side	$t_{ME}+2t_h$	$t_{ME}+2t_h$	$t_{ME}+2t_h$
Authentication			
User side	t_s+3t_h	$2t_{ME}+4t_h$	$2t_{ME}+2t_h$
Server side	$t_{ME}+t_s+3t_h$	$2t_{ME}+3t_h$	$t_{ME}+2t_h$

• t_s is symmetric key computation.
• t_h is hash computation.
• t_{ME} is modulus exponentiation computation.
Note: The computation cost of the symmetric key operations is similar to the hash operations.

complexity of the symmetric key operations t_s is similar to the hash operations t_h (e.g., Feldhofer and Rechberger claim that AES [12] is even more efficient than SHA-256 [13] in resource-constrained devices such as RFID tags based on their testing [14]), the modulus exponentiation operations t_{ME} have much higher computational complexity than the symmetric key and hash operations.

From Table 1, we can see that the new authentication protocol does not require modulus exponentiation computation on the smart card. Its performance is much better than Xu–Zhu–Feng's scheme and Lee–Chiu's scheme in the user side, and also better than Xu–Zhu–Feng's scheme in the server side.

6. Conclusion

In this paper, we analyzed Xu–Zhu–Feng's smart card based password authentication scheme. Our research showed that Xu–Zhu–Feng's scheme is vulnerable to the impersonation attack provided by an internal user. We proposed a simple improvement for Xu–Zhu–Feng's scheme. Moreover, we presented a new efficient strong smart card based password authentication protocol and analyzed its security. We demonstrated that the new protocol has much better security features and performance when compared to Xu–Zhu–Feng's scheme and Lee–Chiu's scheme.

Acknowledgement

We would like to thank Matthew Kellett and Peter C. Mason for their helpful comments and review. We are also grateful to the anonymous referees for helpful comments.

References

[1] L. Lamport, Password authentication with insecure communication, Communications of the ACM 24 (11) (1981) 770–772.
[2] N. Haller, The s/key one-time password system, Proceedings of the Internet Society Symposium on Network and Distributed Systems, 1994, pp. 151–157.
[3] J. Xu, W.T. Zhu, D.G. Feng, An improved smart card based password authentication scheme with provable security, Computer Standards & Interfaces 31 (4) (2009) 723–728.
[4] M.L. Das, Two-factor user authentication in wireless sensor networks, IEEE Transactions on Wireless Communications 8 (3) (2009) 1086–1090.
[5] N.Y. Lee, Y.C. Chiu, Improved remote authentication scheme with smart card, Computer Standards & Interfaces 27 (2) (2005) 177–180.
[6] S.W. Lee, H.S. Kim, K.Y. Yoo, Improvement of Chien et al'.s remote user authentication scheme using smart cards, Computer Standards & Interfaces 27 (2) (2005) 181–183.
[7] A.K. Awasthi, S. Lal, An enhanced remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 50 (2) (2004) 583–586.
[8] M. Kumar, New remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 50 (2) (2004) 597–600.
[9] M.S. Hwang, L.H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (1) (2000) 28–30.
[10] R. Song, L. Korba, G. Yee, Analysis of smart card-based remote user authentication schemes, Proceedings of the 2007 International Conference on Security and Management, 2007, pp. 323–329.
[11] S.V.A. Menezes, P. van Oorschot, Handbook of Applied Cryptography, CRC Press Inc, 1997.
[12] M. Feldhofer, J. Wolkerstorfer, V. Rijmen, Aes implementation on a grain of sand, IEE Proceedings on Information Security 152 (1) (2005) 13–20.
[13] L. Dadda, M. Macchetti, J. Owen, The design of a high speed asic unit for the hash function Sha-256 (384, 512), Proceedings of the conference on Design, automation and test in Europe (DATE'04), Vol. 3, IEEE Computer Society, Paris, France, 2004, pp. 70–75.
[14] M. Feldhofer, C. Rechberger, A case against currently used hash functions in rfid protocols, Lecture Notes in Computer Science, Vol. 4277, Springer, 2006, pp. 372–381.

Ronggong Song is a research officer with the Institute for Information Technology of National Research Council of Canada (NRC/IIT). He is currently assigned to Defence R&D Canada-Ottawa on research of security in MANETs and WSNs. His research interests include information security, network security, privacy protection, and trust management. He is a Senior Member of IEEE.