Information Sciences Letters

Volume 3
Issue 1 *Jan. 2014*

Article 5

2014

Cryptanalysis of an Improved Smartcard-based Remote Password Authentication Scheme

SK Hafızul Islam
Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333031, India, hafi786@gmail.com

G. P. Biswas
Department of Computer Science and Engineering, Indian School of Mines, Dhanbad, Jharkhand 826004, India, hafi786@gmail.com

Kim-Kwang Raymond Choo
Information Assurance Research Group, Advanced Computing Research Centre, University of South Australia, Australia, hafi786@gmail.com

Recommended Citation

Hafizul Islam, SK; P. Biswas, G.; and Raymond Choo, Kim-Kwang (2014) "Cryptanalysis of an Improved Smartcard-based Remote Password Authentication Scheme," *Information Sciences Letters*: Vol. 3 : Iss. 1 , Article 5.
Available at: https://digitalcommons.aaru.edu.jo/isl/vol3/iss1/5

Inf. Sci. Lett. **3**, No. 1, 35-40 (2014)

Information Sciences Letters
An International Journal

http://dx.doi.org/10.12785/isl/030105

Cryptanalysis of an Improved Smartcard-based Remote Password Authentication Scheme

SK Hafizul Islam[1,*], *G. P. Biswas*[2] *and Kim-Kwang Raymond Choo*[3]

[1] Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333031, India
[2] Department of Computer Science and Engineering, Indian School of Mines, Dhanbad, Jharkhand 826004, India
[3] Information Assurance Research Group, Advanced Computing Research Centre, University of South Australia, Australia

Received: ..., Revised: ..., Accepted: ...

Abstract: In recent years, several dynamic identity-based two-factor user authentication using password and smartcard have been proposed to provide mutual authentication between the user and server over unreliable networks. However, the design of secure cryptographic schemes is still notoriously hard, and there have been several instances of detected flaws in published schemes. For example in 2010, Hao and Yu demonstrated that Wang et al.'s user authentication scheme is insecure against off-line password guessing and server masquerade attacks, and proposed an improved scheme. Subsequently in 2012, Chao pointed out that the improved scheme of Hao and Yu is, unfortunately, susceptible to off-line password guessing and server masquerade attacks, and prone to password backward security problem; and proposed an enhanced scheme. In this paper, we demonstrated that Chao's enhanced scheme is not secure against user masquerade attack, server masquerade attack, insider attack and off-line password guessing attack in violation of its security claim as well as it fails to achieve users' anonymity.

Keywords: Two-factor authentication, One-way hash function, Password guessing attack, Insider attack, Password, Smartcard

1 Introduction

As the Internet evolves from an academic and research network into a commercial network, more and more organizations and individuals are connecting their internal networks and computers to the Internet. Investment in network expansion by telecommunications companies will see a further expansion in capacity that will result in an increase in bandwidth availability and greater adoption of wireless and mobile technologies. As businesses continue to engage in electronic commerce, they will become increasingly globalised and interconnected. These, and other developments, create not only benefits for the community, but also risks of cybercrime [1]. Cybercriminals, for example, aim to disrupt one or more combinations of the following security notions: data confidentiality, data integrity and data availability. The ability to provide security guarantees is of paramount importance and several initiatives have been proposed to address this concern. Due to the low computation cost and portability of smartcard and easy memorization of user chosen password, two-factor smartcard authentication [2–21] using password is commonly used in Internet-based applications such as remote user/server login, online banking, Pay-TV, electronic voting, secret online order placement.

In recent years, several smartcard based password authentication schemes have been published. For example in 2002, Chien et al. [2] proposed one such scheme, but was subsequently found to be vulnerable to reflection and insider attacks [3]. To remove these drawbacks, Ku and Chen [3] designed another improved scheme, but Wang et al. [4] demonstrated that the scheme is insecure against off-line password guessing attack, forgery attack and denial of service (DoS) attack, and proposed another improved scheme. However, Chung et al. [5] revealed that Wang et al.'s scheme [2] is still susceptible to impersonation attack and off-line password guessing attack. In addition, Wang et al.'s scheme is not easily repairable and is unable to provide perfect forward secrecy of the generated session key. Other instances of vulnerabilities in published smartcard-based password authentication schemes include off-line password

---

[*] Corresponding author e-mail: hafi786@gmail.com, hafizul.ism@gmail.com, hafizul@pilani.bits-pilani.ac.in

guessing attack [6–8, 22], impersonation attack [9–11], forgery attack [4, 12–14], DoS attack [4, 7, 18, 23], parallel session attack [4, 9, 10, 18], replay attack [23], stolen/lost smartcard attack [9, 22, 24], observing power consumption [25] and reverse engineering techniques [26, 27].

In this paper, we examine the protocol of Chao [16] whose history is as follows. In 2010, Hao and Yu [17] pointed out that Wang et al.'s scheme [6] is not secure against off-line password guessing attack and server masquerade attack, and proposed an enhanced scheme. Unfortunately, Chao [16] demonstrated that Hao and Yu's scheme [17] is still insecure against off-line password guessing attack and server masquerade attack, and prone to password backward security problem i.e., the scheme must be replaced if the scheme was attacked for one time, in violation of its security claims.

They then designed an improved ID-based scheme. The latter scheme is examined in this paper where we pointed out that this scheme is not secure from insider attack, server masquerade attack and user masquerade attack and user's anonymity problem. Furthermore, the scheme is susceptible to off-line password guessing attacks in which an attacker exhaustively enumerates all possible passwords in an offline manner to find out the correct password on lost/stolen smartcard. Off-line password guessing attacks have been used by both criminals and law enforcement and digital forensics practitioners to enable access to password-protected data (e.g. on smart phones and portable devices based on RIM Black Berry and Apple iOS platforms).

The rest of the paper is structured as follows. Section 2 briefly describes the Chao's smartcard-based user authentication scheme [16], and Section 3 outlines our attacks. The last section concludes the paper.

2 Review of Chao's smartcard-based user authentication scheme

The Chao's scheme consists of four phases: registration phase, login phase, verification phase and password change phase, and the notations used are listed in Table 1.

Table 1: Notations used in Chao's authentication scheme

Notations	Descriptions
U_i	A legitimate user
ID_i	Identity of the user U_i
PW_i	Password of the user U_i
S	Remote server
x	Long-term secret of the remote server S
$h(\cdot)$	Secure one-way hash function (i.e., SHA-1)
$\|$	Concatenation operation
$\oplus$	Bit-wise XOR operation
T_i	Current timestamp of the entity i
ΔT_i	Acceptable time interval

2.1 Registration phase

This phase is executed between user U_i and the remote server S, and consists of the following steps:

Step 1. U_i chooses an identity-password pair (ID_i, PW_i) and then sends it to S through a secure channel.

Step 2. On receiving (ID_i, PW_i), S checks the identity ID_i of U_i, selects a random number r_i and computes $K_i = h(x \| r_i) \oplus h(PW_i)$ and $L_i = h(ID_i \| h(x \| r_i))$.

Step 3. S issues a smartcard and writes the parameters $(K_i, L_i, h(\cdot))$ into it. Then S sent the smartcard to U_i through a secure channel.

2.2 Login phase

In order to login to the remote server S, U_i inserts his smartcard into a card reader and inputs ID_i and PW_i, then the smartcard performs the followings:

Step 1. The smartcard computes $h(x \| r_i)^{'} = K_i \oplus h(PW_i)$ and $L_i^{'} = h(ID_i \| h(x \| r_i)^{'})$, and compares $L_i^{'}$ with L_i and continues to the next step if they are equal, otherwise rejects the login request.

Step 2. The smartcard then computes $M_i = ID_i \oplus h(x \| r_i)^{'} \oplus T_i$ and $CID_i = h(ID_i \| T_i)$, and sends the login message (CID_i, M_i, T_i) to S through an open channel, where T_i is the current timestamp of U_i.

2.3 Verification phase

Assume that S received the message (CID_i, M_i, T_i) at time $T_i^{'}$ and then S does the followings:

Step 1. S checks whether $T_i^{'} - T_i \leq \Delta T_i$ holds, if not, S rejects U_i's login request. Otherwise, S proceeds to the next step.

Step 2. S computes $N_i = h(x \| r_i)$, $ID_i^{'} = M_i \oplus N_i \oplus T_i$ and $CID_i^{'} = h(ID_i^{'} \| T_i)$. S checks whether $CID_i^{'} = CID_i$ holds and terminates the login request if they are not equal. Otherwise, S computes $a = h(T_S \| ID_i^{'} \| N_i)$ and sends the message (a, T_s) to U_i, where T_S is the current timestamp of S.

Step 3. Suppose that U_i receives (a, T_S) at time $T_S^{'}$. Now U_i computes $a^{'} = h(T_S \| ID_i \| h(x \| r_i)^{'})$ and authenticates S if both of the conditions $T_S^{'} - T_S \leq \Delta T_S$ and $a^{'} = a$ hold. U_i terminates the login request if either of the above fails.

2.4 Password change phase

This phase allows U_i to change his old password PW_i to a new password PW_i^{*} with the following operations:

Step 1. U_i inserts his smartcard into the card reader and inputs ID_i and PW_i, then the smartcard computes $h(x \parallel r_i)' = K_i \oplus h(PW_i)$ and $L_i' = h(ID_i \parallel h(x \parallel r_i)')$, and compares L_i' with L_i for valid password change operation. If they are not equal, the smartcard rejects the password change request and asks U_i for exact PW_i and ID_i. Otherwise, the smartcard proceeds to the next step.

Step 2. Smartcard computes $K_i^* = h(PW_i^*) \oplus h(PW_i) \oplus K_i$ and replaces K_i with K_i^*. The secure password change phase is finished.

3 Cryptanalysis of Chao's smartcard-based user authentication scheme

This section demonstrated that Chao's authentication scheme [16] is vulnerable to insider attack, user masquerade attack, server masquerade attack and off-line password guessing attack, as well as it fails to achieve users' anonymity. Before introducing the proposed attacks, we describe the following widely used assumptions about the power of an adversary $\mathscr{A}$ [10, 11, 15, 18, 22, 28, 29].

(A1) $\mathscr{A}$ can sniff the communication media through which U_i and S communicate with each other i.e., $\mathscr{A}$ can intercept, block, inject, remove, or modify, any messages transmitted in the media.

(A2) $\mathscr{A}$ may either (a) steal user's smartcard and extract the stored secrets by monitoring the timing information, power consumption and reverse engineering techniques as mentioned in [25–27] and guess the user's password in off-line manner using the secrets extracted from the smartcard; or (b) obtain a user's password directly by some means. However, the adversary is not allowed to do both (a) and (b) as having the smartcard and knowing the password would be trivial to impersonate the legitimate user.

3.1 Users' anonymity problem

In recent years, many dynamic identity-based remote login schemes [6, 16–21] have been proposed to provide mutual authentication between the user and the remote server. In any dynamic identity-based remote login scheme, users' anonymity [6, 7, 22] is an important security requirement. Now, we show that Chao's scheme [16] fails to achieve the same as follows:

(a) $\mathscr{A}$ intercepts a login message (CID_i, M_i, T_i) of U_i of a previous session, where $M_i = ID_i \oplus h(x \parallel r_i)' \oplus T_i$, $CID_i = h(ID_i \parallel T_i)$ and T_i is the current timestamp.

(b) $\mathscr{A}$ guesses an identity ID_i^* and computes $CID_i^* = h(ID_i^* \parallel T_i)$.

(c) $\mathscr{A}$ verifies the correctness of ID_i^* by checking whether the computed CID_i^* and the intercepted CID_i are equal.

(d) $\mathscr{A}$ repeats the steps (b) and (c) until it finds the exact identity ID_i of U_i.

The adversary $\mathscr{A}$ can easily guess the identity ID_i of U_i by checking all possible identities from the search space $|\mathscr{D}_{ID}|$, where $|\cdot|$ indicates the cardinality of $\mathscr{D}_{ID}$. The running time of the aforementioned procedure is $O(|\mathscr{D}_{ID}|) \times (T_c + T_h)$, where T_c and T_h represents the execution time of concatenation and hash operations, respectively. It can be noted that for easy memorization, user generally chooses his identity with low intensity value from the set $\mathscr{D}_{ID}$ having small number of elements. Since $\mathscr{D}_{ID}$ is not large enough in practice, for example, $|\mathscr{D}_{ID}| \leq 10^{-6}$ [30–33] and the time complexities T_c and T_h are also negligible, thus $\mathscr{A}$ can complete the above procedure in polynomial time.

3.2 User masquerade attack

We now demonstrate that Chao's scheme [16] is not secure against user masquerade attack.

(a) $\mathscr{A}$ monitor the communication channel and intercepts a login message (CID_i, M_i, T_i) in a session.

(b) $\mathscr{A}$ finds the exact identity ID_i of U_i by executing steps discussed in section 3.1.

(c) $\mathscr{A}$ selects a valid timestamp $T_i^*(>T_i)$, computes $M_i^* = M_i \oplus T_i \oplus T_i^* = ID_i \oplus h(x \parallel r_i) \oplus T_i^*$, $CID_i^{*\prime} = h(ID_i \parallel T_i^*)$ and then sends the forged message (CID_i^*, M_i^*, T_i^*) to S for login operation.

(d) On receiving (CID_i^*, M_i^*, T_i^*), S will confirm that the timestamp validity condition $T_i^{*\prime} - T_i^* \leq \Delta T_i^*$ is correct, and computes $N_i^* = h(x \parallel r_i)$, $ID_i = M_i^* \oplus N_i \oplus T_i^*$, $CID_i^* = h(ID_i \parallel T_i^*)$ after confirming that $CID_i^{*\prime} = CID_i^*$. With these successful verifications, S accepts the forged login request and allows $\mathscr{A}$ to login to S. Thus, $\mathscr{A}$ impersonates the valid user U_i.

3.3 Server masquerade attack

This section demonstrated that Chao's user scheme [16] is vulnerable to server masquerade attack.

(a) $\mathscr{A}$ intercepts U_i's login message (CID_i, M_i, T_i) of previous session.

(b) $\mathscr{A}$ finds the exact identity ID_i of U_i by executing steps discussed in section 3.1.

(c) $\mathscr{A}$ computes $h(x \parallel r_i) = M_i \oplus ID_i \oplus T_i$, selects a timestamp $T_S^*(>T_S)$, computes a fabricated message (a^*, T_S^*) and sends it to U_i, where $a^* = h(T_S^* \parallel ID_i \parallel h(x \parallel r_i))$.

(d) Upon receiving the message (a^*, T_S^*), U_i found that both the conditions $T_S^{*\prime} - T_S^* \leq \Delta T_S^*$ and $a^{*\prime} = a^*$ are satisfied, where $a^{*\prime} = h(T_S^* \parallel ID_i \parallel h(x \parallel r_i))$ is computed by U_i. Therefore, $\mathscr{A}$ get able to trick the legitimate user U_i to believe that $\mathscr{A}$ is legal server S not an adversary.

3.4 Off-line password guessing attack

Assume that if the smartcard of U_i is lost/stolen and it is in the physical possession of $\mathscr{A}$, who then extracts the original contents $(K_i, L_i, h(\cdot))$ by monitoring their timing information [25], power consumption and reverse engineering techniques [26, 27], where $K_i = h(x \parallel r_i) \oplus h(PW_i)$ and $L_i = h(ID_i \parallel h(x \parallel r_i))$. Also we suppose that $\mathscr{A}$ monitors the communication channel and recovers U_i's valid login message (CID_i, M_i, T_i) of a session, where $M_i = ID_i \oplus h(x \parallel r_i) \oplus T_i$, $CID_i = h(ID_i \parallel T_i)$ and T_i is the timestamp. In order to launch an off-line password guessing attack on the stolen smartcard, $\mathscr{A}$ executes the following operations:

(a) $\mathscr{A}$ finds the exact identity ID_i of U_i and $h(x \parallel r_i)$ from the intercepted message (CID_i, M_i, T_i) by executing the steps discussed in section 3.3.
(b) $\mathscr{A}$ computes $X_i = K_i \oplus h(x \parallel r_i) = h(PW_i)$.
(c) $\mathscr{A}$ guesses a PW_i^* and computes $X_i^* = h(PW_i^*)$.
(d) $\mathscr{A}$ verifies the correctness of guessed PW_i^* by checking whether X_i^* and X_i are equal.
(e) $\mathscr{A}$ repeats the steps (c) and (d) until to have the exact password PW_i of U_i.

The running time of the above password guessing attack is $O(|\mathscr{D}_{ID}|) \times (T_c + T_h) + O(|\mathscr{D}_{PW}|) \times (T_c + T_h + T_x)$, where T_x represents the execution time of bit-wise XOR operation. As discussed earlier in section 3.1, the search spaces $\mathscr{D}_{ID}$ and $\mathscr{D}_{PW}$ are unlikely to be large enough (for example, $|\mathscr{D}_{ID}| \leq 10^{-6}$ and $|\mathscr{D}_{PW}| \leq 10^{-6}$ [30–33]), and the time complexities T_c, T_h and T_x all can be executed with negligible amount of time, thus the polynomial time-bounded adversary $\mathscr{A}$ can find the exact password PW_i of U_i easily.

3.5 Insider attack

Studies have demonstrated that users tend to use the same password for different applications [4, 19]. If the adversary, $\mathscr{A}$, is a malicious insider of the remote server S and has learned U_i's password (a trivial exercise as U_i sends his (ID_i, PW_i) in plaintext form to S during the registration phase of Chao's scheme [16]), $\mathscr{A}$ may try to masquerade the user U_i using the password PW_i to access other servers.

4 Conclusion

We examined the identity-based smartcard-based remote password authentication scheme of Chao (2012), and demonstrated that the scheme is susceptible to common attacks, namely user masquerade attack, server masquerade attack, insider attack and off-line password guessing attack.

Acknowledgments

This research work is supported by the Department of Science and Technology (DST), Govt. of India under the **INSPIRE fellowship Ph.D program** (Grant No. IF10247) and the Department of Information Technology (DIT), Ministry of Communication and Information Technology, Govt. of India under the **Information Security Education and Awareness (ISEA) program** (Project No. MIT(2)/2006-08/189/CSE). The authors would also like to express their gratitude and heartiest thanks to the Department of Computer Science and Engineering, Indian School of Mines, Dhanbad-826004, India, for providing their research support, as without such help this work could not be carried out.

References

[1] Choo, K-K. R.: The cyber threat landscape: Challenges and future research directions, Computers & Security, **30**, 719-731, (2011).
[2] Chien, H. Y., Jan, J. K., and Tseng, Y. M.: An efficient and practical solution to remote authentication: smart card, Computers & Security, **21**, 372-375 (2002).
[3] Ku, W-C., and Chen, S-M.: Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, **50**, 204-207 (2004).
[4] Wang, X. M., Zhang, W. F., Zhang, J. S., and Khan, M. K.: Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards, Computer Standards & Interfaces, **29**, 507-512 (2007).
[5] Chung, H-R. , Ku, W-C. , and Tsaur, M-J.: Weaknesses and improvement of Wang et al.'s remote user password authentication scheme for resource-limited environments, Computer Standards & Interfaces, **31**, 863-868 (2009).
[6] Wang, Y-Y., Liu, J-Y., Xiao, F-X., and Dan, J.: A more efficient and secure dynamic ID-based remote user authentication scheme, Computer Communications, **32**, 583-585 (2009).
[7] Wang, D., Ma, C-G., Zhao, S., and Zhou, C.: Secure password-based remote user authentication scheme with non-tamper resistant smart cards, In Proceedings of the 9th IFIP International Conference on Network and Parallel Computing (NPC 2012), LNCS, **7513**, 110-118 (2012).
[8] Wang, D., and 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, **19**, 104-114 (2012).
[9] Xie, Q.: Improvement of a security enhanced one-time two-factor authentication and key agreement scheme, Scientia Iranica, Transactions D: Computer Science & Engineering and Electrical Engineering, (2012).
[10] Chen, T-H., Hsiang, H-C., and Shih, W-K.: Security enhancement on an improvement on two remote user authentication schemes using smart cards, Future Generation Computer Systems, **27**, 377-380 (2011).
[11] Song, R.: Advanced smart card based password authentication protocol, Computer Standards & Interfaces, **32**, 321-325 (2010).

[12] Liu, J. Y., Zhou, A. M., and Gao, M. X.: A new mutual authentication scheme based on nonce and smart cards, Computer Communications, **31**, 2205-2209 (2008).

[13] Holbl, M., Welzer, T., and Brumen, B.: Attacks and improvement of an efficient remote mutual authentication and key agreement scheme, Cryptologia, **34**, 52-59 (2010).

[14] Awasthi, A. K., Srivastava, K., and Mittal, R. C.: An improved timestamp-based remote user authentication scheme, Computers & Electrical Engineering, **37**, 869-874 (2011).

[15] Xu, J., Zhu, W-T., Feng, D-G.: An improved smartcard based password authentication scheme withprovable security, Computer Standards & Interfaces, **31**, 723-728 (2009).

[16] Chao, J.: An Improved remote password authentication scheme with smartcard, Journal of Electronics, **26**, 550-555 (2012).

[17] Hao, Z., and Yu, N.H.: A security enhanced remote password authentication scheme using smart card, In Proceedings of the 2nd International Symposium on Data, Privacy and E-Commerce, 56-60 (2010).

[18] Hsiang, H-C., and Shih, W-K.: Improvement of the secure dynamic ID-based remote user authentication scheme for multi-server environment, Computer Standards & Interfaces, **31**, 1118-1123 (2009).

[19] Wen, F., and Li,X.: An improved dynamic ID-based remote user authentication with key agreement scheme, Computers & Electrical Engineering, **38**, 381-387 (2012).

[20] Das, M. L., Saxena, A, and Gulati, V. P.: A dynamic ID-based remote user authentication scheme, IEEE Transactions on Consumer Electronics, **50**, 629-631 (2004).

[21] Khan, M. K., Kim, S-K., Alghathbar, K.: Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme', Computer Communications, **34**, 305-309 (2011).

[22] Ma, C-G., Wang, D, and Zhao, S-D.: Security flaws in two improved remote user authentication schemes using smart cards, International Journal of Communication Systems, (2012).

[23] Xiang, T., Wong, K. W., and Liao, X.: Cryptanalysis of a password authentication scheme over insecure networks, Journal of Computer and System Sciences, **74**, 657-661 (2008).

[24] Li, C. T., Lee, C. C., Liu, C. J., and Lee, C. W.: A Robust Remote User Authentication Scheme against Smart Card Security Breach. In Proceedings of the DBSec'11, LNCS, **6818**, 231-238 (2011).

[25] Joye, M., and Olivier, F.: Side-channel analysis, Encyclopedia of Cryptography and Security, Kluwer Academic Publishers, 571-576 (2005).

[26] Kocher, P., Jaffe, J., and Jun, B.: Differential power analysis, in: Proceedings of Advances in Cryptology- Crypto'99, LNCS, 388-397 (1999).

[27] Messerges, T. S., Dabbish, E. A, and Sloan, R. H.: Examining smart-card security under the threat of power analysis attacks, IEEE Transactions on Computers, **51**, 541-552 (2002).

[28] Shim, K.: Security flaws in three password-based remote user authentication schemes with smart cards, Cryptologia, **36**, 62-69 (2012).

[29] Wang D., Ma, C-G., Zhao, S., and Zhou, C.: Cryptanalysis of two dynamic id-based remote user authentication schemes for multi-server architecture, In Proceeding of the 6th International Conference on Network and System Security (NSS 2012), LNCS, **7645**, 462-475 (2012) .

[30] Florencio, D., and Herley, C.: A large-scale study of web password habits, In Proceedings of the 16th International Conference on World Wide Web, 657-666 (2007).

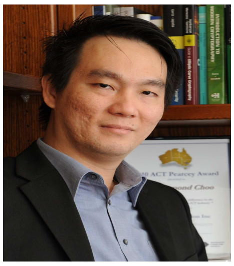
[31] Klein, D.V.: Foiling the cracker: a survey of, and improvements to, password security, In Proceedings of the 2nd USENIXSecurity Workshop, 5-14 (1990).

[32] Wu, T., A real-world analysis of kerberos password security, In: Proceedings of the NDSS'98, 1-14 (1998).

[33] Bonneau, J.: The science of guessing: analyzing an anonymized corpus of 70 million passwords, In Proceedings of the 33th IEEE Symposiumon Security and Privacy, 538-552 (2012).

SK Hafizul Islam completed his Ph.D in Computer Science and Engineering from Indian School of Mines, Dhanbad, India, under the prestigious INSPIRE Fellowship Ph.D Program (funded by DST, Govt. of India) and Information Security Education and Awareness (ISEA) program (funded by Department of Information Technology (DIT), Ministry of Communication and Information Technology, Govt. of India, No. MIT (2)/2006-08/189/CSE). Dr. Islam received his B.Sc (Hons.) in Mathematics and M.Sc in Applied Mathematics from Vidyasagar University, West Bengal, India in 2004 and 2006, and M.Tech from Indian School of Mines, Dhanbad in 2009, respectively. Dr. Islam is currently holding the position of Assistant Professor in the Department of Computer Science & Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333031, India. His research interest includes Cryptography, Network/Information Security and Computer Networks.

G. P. Biswas received B.Sc (Engg.) and M.Sc (Engg.) degrees in Electrical & Electronics Engineering and Computer Science & Engineering, respectively. He completed his PhD degree in Computer Science & Engineering from Indian Institute of Technology, Kharagpur, India. He is currently working as a Professor in the Department of Computer Science & Engineering, Indian school of Mines, Dhanbad, Jharkhand, India. His main research interests include Cryptography, Computer Network and Security, Cellular Automata, VLSI Design.



Kim-Kwang Raymond Choo received the Ph.D in Information Security from Queensland University of Technology in 2006. He has (co-)authored a number of publications including a book published in Springers “Advances in Information Security” book series and six refereed monographs; and is the recipient of the 2010 ACT Pearcey Award, 2009 Fulbright Scholarship, 2008 Australia Day Achievement Medallion, British Computer Society’s Wilkes Award for the best paper published in the 2007 volume of The Computer Journal, 2007 Queensland University of Technology Faculty of Information Technology Executive Deans outstanding Ph.D. thesis commendation, and the 2005 Australasian Conference on Information Security and Privacy Best Student Paper Award.