International Journal of Security and Its Applications
Vol.9, No.12 (2015), pp.237-244
http://dx.doi.org/10.14257/ijsia.2015.9.12.23

A New Remote User Authentication Scheme based on Graphical Password using Smart Card

Khanjan Ch. Baruah, Subhasish Banerjee, Manash P. Dutta and Chandan T. Bhunia

Department of Computer Science and Engineering
National Institute of Technology, Arunachal Pradesh, India - 791112
khanjan099@yahoo.com, subhasish.cse@nitap.in,
manash.cse@nitap.in, ctbhunia@vsnl.com

Abstract

Remote user authentication schemes provide a system to verify the legitimacy of remote users' login request over insecure communication channel. Since last few years many authentication schemes have been proposed including several new features and ideas. But, due to the advancement of computational process they are suffering from various possible attacks. This is the reason because of which attaining the security becomes a prime issue and major challenge among the researchers. In this paper, we have proposed a new user friendly authentication scheme that can provide the higher security at lower computational cost. This scheme provides extra level of security by adopting the user-defined image for password generation. Finally, the security analysis and performance evaluation are made to proof the efficiency of our scheme.

Keywords: *Mutual Authentication, Multi-server, Dynamic ID*

1. Introduction

Network technology has been widely developed in the recent years. This development brings many new issues of concern. Remote user authentication is one of the fundamental criteria in the network security. Researchers, in the past, devised many authentication schemes. The traditional schemes were based on passwords [1-3], making it vulnerable to simple dictionary attacks. Thereafter, to increase the security, smart card based authentication schemes were introduced [4-6]. But, due to the advancement of computer technology, these schemes are still not capable to withstand various possible attacks [7]. To overcome these weaknesses, later biometrics was also been incorporated as third parameter and make the authentication schemes [8-18] based on three factors namely smartcard, password and biometric. In 2010, Li and Hwang [10] proposed a biometrics-based remote user authentication scheme using smart cards. In their scheme, they eliminated the use of time synchronization by using nonce. Li *et al*. [11], in 2011, analyzed Li and Hwang's [10] scheme and drew various weaknesses. Subsequently, they proposed their improved authentication scheme to overcome drawbacks of Li and Hwang's authentication scheme. Later, in 2011, Das *et al*. [12] showed that Li *et al*.'s [11] scheme failed to locally update user's new password and also failed to provide strong mutual authentication. Thus, they proposed an efficient biometric-based remote user authentication scheme based on smart cards. In 2012, Sekhar *et al*. [13] and An *et al*. [14] analyzed Das *et al*.'s [12] scheme and showed that it was vulnerable to insider attack, impersonation attack, server masquerade attack, Man-in-the-Middle attack, and replay attack. An *et al*. [14] proposed a scheme which was resilient to all the vulnerabilities found in Das *et al*.'s scheme. In 2013, Khan *et al*. [15] showed that An *et al*.'s [14] scheme was not secure enough as they claimed and can suffer from impersonation attack, server masquerade attack, Man in the Middle attack. To overcome from all the mentioned

ISSN: 1738-9976 IJSIA

attacks, they proposed their improved scheme by negotiating the computational cost by adding only two hash operations. In 2014, Chuang and Chen [16] proposed a multi- server authenticated key agreement scheme using smart cards and biometrics. However, both Mishra *et al*. [17] and Maitra and Giri [18] showed their scheme is insecure against stolen smart card attack, impersonation attack, forgery attack and session key discloser attack. Later, Mishra *et al*. [17] proposed an improved biometric based remote user authentication scheme. But, normally human brain is better in recalling images based things rather than remembering complicated large password. So, in this paper, we have proposed a user friendly remote user authentication scheme using smart card. In our proposed scheme, the users need not to remember any complicated alphanumeric password for security concern as because password can be generated automatically by selecting some regions from an image provided by the user itself during registration. The latter half of the paper consists of the security and performance analysis of the proposed scheme.

Table 1. Notation Used in the Paper

Notations	Meaning
ID_i	Identity of the i^{th} user
RC	Registration center
SID_j	Identity of the j^{th} server
PW_i	Password of the i^{th} user
IMG	Image provided by the user during registration
PSK	Pre-shared key of the servers
X_s	Master secret key maintained by the registration center
h(.)	A one-way hash function
N_i	Random nonce of the i^{th} user
N_j	Random nonce of the j^{th} server
$\oplus$	Exclusive-OR operation
$\|\|$	Message concatenation operation

2. Password Generation

Password is the important factor in authentication scheme. The traditional authentication schemes require the user to input text-based password. However, these passwords are weak or are easily forgotten. It was found that human can remember pictures easier than text.

In our proposed scheme, the user's password is generated by using an image provided by the user. During registration, the user provides an image IMG. The image is reduced to a size of m × m pixels (say 640 × 640 pixels) and converted to greyscale image. The image is then divided into n blocks of l × l size (say 8 × 8 pixels). The user, now selects k number of blocks from the greyscale image. These blocks have individual pixels with each pixel having some value. Now, we add every pixel value to obtain the block value. The block values of the selected k blocks are further added to give us the password of the user. The user can change the image or the password as and when required. Figure 1 graphically represents this process.

$$PW_i = \sum_{j=1}^{k} Block_j$$

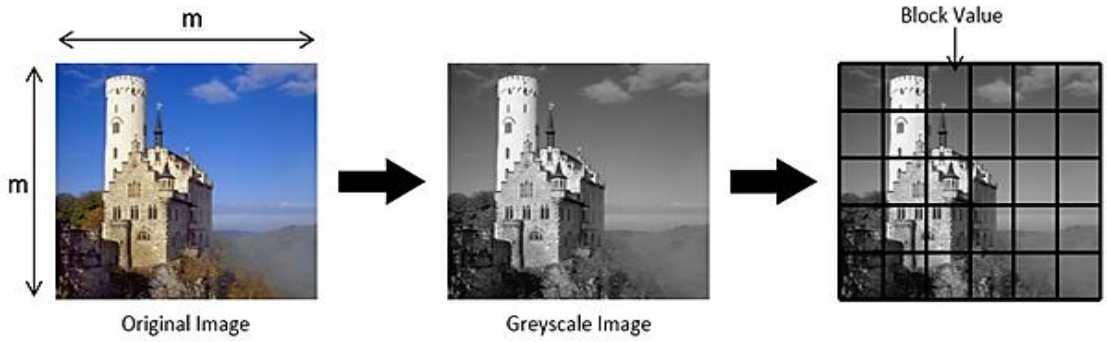

Figure 1. Password Generation from an Image

3. Proposed Scheme

In this section, we have proposed a remote user authentication scheme using smart card. Typically, three participants are involved in the exchange of messages among one another. These participants are: the user (with identity IDi), the server (with identity SID_j) and the registration center (with identity RC). The proposed scheme has been designed to work with the following phases namely registration, login, authentication and password change phase. The notations which have been used throughout this paper are listed in Table 1.

3.1. Registration Phase

The scheme starts with the registration of the users and the service provider servers with the registration center. In this phase, the user performs the following steps to complete his registration:

1) The user, with identity ID_i, selects an image IMG. The password PW_i is generated from this image through the process mentioned in Section II.
2) The user generates a random number R_i and computes $U_1 = h(R_i||PW_i)$ and $U_2 = h(PW_i \oplus ID_i)$. The user sends their ID_i, U_1 and U_2 to the registration center via a secure channel.
3) After receiving the registration request message, registration center, RC, computes
   $A_i = h(ID_i||X_s)$
   $B_i = A_i \oplus U_2$
   $C_i = PSK \oplus h(U_1||ID_i)$
   and generates the smart card containing information B_i and C_i. The smart card is then sent to the user.
4) The user, upon receiving the smart card, updates it with $D_i = h(ID_i||PW_i)$, IMG and R_i. Finally, the smart card will be updated by $\{B_i, C_i, D_i, IMG, R_i\}$.

Similarly, the server, who wants to provide his services, need to register itself to the registration center, RC, to become an authorized server. It sends a join request to RC along with its identity SID_j. The RC replies with $h(SID_j||PSK)$ and X_s, which the server uses to authenticate users.

3.2. Login Phase

This phase will be invoked whenever a registered user wants to access the registered service provider server. The complete description of this phase is defined below:

1) The user ID_i inserts his/her smart card SC_i into the card reader and provides his/her identity ID_i. The system displays the image IMG stored in the smart card and prompts the user to select the blocks.
2) The user now selects specific blocks from IMG. Then, the terminal computes the password using the corresponding pixel value of the blocks as defined in the Section II.
3) The smart card computes the value $h(ID_i||PW_i)$ and verifies it with D_i. If the verification fails, the process terminates. Otherwise, the smart card computes
   $U_1 = h(R_i||PW_i)$
   $U_2 = h(PW_i \oplus ID_i)$
   The smart card extracts PSK and A_i from C_i and B_i respectively by computing
   $PSK = C_i \oplus h(U_1||ID_i)$
   $A_i = B_i \oplus U_2$
4) Using the PSK, it computes $h(SID_j||PSK)$, where SID_j is the server's identity to which it is trying to communicate. A message, using $h(SID_j||PSK)$ and ID_i, is generated as : $M_1 = ID_i \oplus h(SID_j||PSK)$.
5) A random number N_i is generated by the smart card and it is sent to the server as: $M_2 = N_i \oplus A_i$. A message for verification is also generated as $M_v = h(SID_j||N_i||A_i)$.
6) The smart card transmits the login request messages $\{M_1, M_2, M_v\}$ to the server SID_j via an insecure channel.

3.3. Authentication Phase

The server SID_j, upon receiving the authentication messages, $\{M_1, M_2, M_v\}$, performs the following operations to validate the user and mutually generate the session key.

1). The server extracts the identity ID_i of the user from message M_1:
   $ID_i = M_1 \oplus h(SID_j||PSK)$
2). The server now uses the user's identity, ID_i and its shared secret X_s to compute A_i. This is further used to extract the user random number N_i from the received message M_2.
   $A_i = h(ID_i||X_s)$
   $N_i = M_2 \oplus A_i$
3). Then the server verifies whether $h(SID_j||N_i||A_i)$ is matched with received message M_v or not.
4). If verification fails, the server simply rejects the login request otherwise it computes the session key for further communication after generating the nonce N_j.
   $SK_{ji} = h(A_i||SID_j||N_i||N_j)$
5). The server information must be communicated to the actual user for the establishment of the session key agreement on the user side. So, the server generates the message M_3. The server verifies its authenticity to the user through the message M_4.
   $M_3 = N_j \oplus h(ID_i \oplus N_i)$
   $M_4 = h(SK_{ji}||N_j||N_i)$
6). These messages M_3 and M_4 are forwarded to the user through an insecure channel.
7). After receiving the message $\{M_3, M_4\}$, the user extracts the server's random number N_j from M_3.
   $N_j = M_3 \oplus h(ID_i \oplus N_i)$
8). The user computes the session key
   $SK_{ij} = h(A_i||SID_j||N_i||N_j)$.
9). The user verifies the server's authenticity by computing $h(SK_{ji}||N_j||N_i)$ and comparing it with M_4. If successful, the user can conclude that the server is authentic and both of them have the same session key.

3.4. Password Change Phase

The password change phase is a significant part of any authentication scheme. The password change mechanism can be performed locally without contacting the registration center.

The user inserts his/her smart card and inputs identity ID_i. The system prompts the user to select the *k* blocks from the image, IMG, stored in the smart card. The card verifies the information entered using D_i. The user has two options either to input a new image or to select new blocks. The user selects the blocks and the password is generated as mentioned in Section II. The new password PW_i^{new} is generated and the card computes:

$U_1 = h(R_i \| PW_i)$
$U_2 = h(PW_i \oplus ID_i)$
$U_1^{new} = h(R_i \| PW_i^{new})$
$U_2^{new} = h(PW_i^{new} \oplus ID_i)$
$B_i^{new} = B_i \oplus U_2 \oplus U_2^{new}$
$C_i^{new} = C_i \oplus h(U_1 \| ID_i) \oplus h(U_1^{new} \| ID_i)$
$D_i^{new} = h(ID_i \| PW_i^{new})$

The smart card replaces the old B_i, C_i, D_i with the newly computed values, B_i^{new}, C_i^{new}, D_i^{new}. Thus the updated smart card $SC_i = \{ B_i^{new}, C_i^{new}, D_i^{new}, IMG, R_i \}$

4. Security Analysis of the Proposed Scheme

In this section, we have analyzed the security features of our proposed scheme.

- ✓ **Stolen smart card Attack:** An adversary may get a lost or stolen smart card of a user and may extract the information, $\{B_i, C_i, D_i, IMG, R_i\}$, stored in it. However, the adversary will not be able to extract the relevant information A_i from B_i as it is protected with password PW_i and identity ID_i of the user.
  $B_i = A_i \oplus U_2$, where $U_2 = h(PW_i \oplus ID_i)$.
  The shared secret PSK, used for generating authentication message, is also well protected. The adversary without PSK and A_i will not be able to generate any login message. If the adversary attempts to generate the session key, they will not succeed as A_i is required.
- ✓ **Impersonation Attack:** To impersonate as a legal user, the adversary must be able to generate the login messages $\{M_1, M_2, M_v\}$. The adversary must possess the user information A_i, ID_i, PSK. A registered but malicious user can use its PSK for login message generation but A_i is unknown to it. Also, in the smart card, A_i is protected with the user password and the identity, $B_i = A_i \oplus U_2$, where $U_2 = h(PW_i \oplus ID_i)$.
- ✓ **Server Masquerade Attack:** The server identity SID_j is publicly known, so the probability of server masquerading increases. An adversary may intercept all the messages intended for the server SID_j. However, the adversary, a malicious server, will not be able to extract any information from the captured messages, as they will not have the server secret $h(SID_j \| PSK)$. Moreover, if the adversary is a registered user, they can generate $h(SID_j \| PSK)$ but they will not have any knowledge about X_s.
- ✓ **Offline password guessing attack:** The adversary may use a stolen smart card to extract all the information, $SC_i = \{B_i, C_i, D_i, IMG, R_i\}$, stored in it. Now the adversary try to guess the password by selecting the blocks of image IMG. But the adversary is unaware of the number of blocks to select from the image.
- ✓ **Man-in-the-middle attack:** In this attack, an adversary eavesdrops a communication and tries to extract the information to generate the session key. The adversary intercepts the user's login messages, $\{ M_1, M_2, M_v \}$, and attempts to extract the parameters for session key generation. However, this will not be successful as the adversary is unaware of the server secrets $h(SID_j \| PSK)$ and X_s, which are required to

extract ID_i from M_1. Without the ID_i, the adversary will not be able to compute A_i, N_i, used in session key.

- ✓ **Replay Attack:** The adversary may eavesdrop an ongoing communication and stores the login messages, $\{M_1, M_2, M_v\}$. They can, in future, use these message for performing replay attack. However, this will not be successful, as the adversary will not be able to generate a valid authentication message.
- ✓ **Insider Attack:** The user during registration does not provide the password in its original form. The password is hashed with a random number R_i for U_1 and for U_2, it is hashed with the user's identity ID_i as: $U_1 = h(R_i||PW_i)$ and $U_2 = h(PW_i \oplus ID_i)$. Hence, making the proposed scheme resistant against this attack.

5. Performance Analysis

In this section, we have compared the security performance of our scheme with other existing authentication schemes which is shown in the Table 2.

Table 2. Comparison of Security Attributes of Our Proposed Scheme with Existing Scheme

Security Attributes	Proposed scheme	Mishra *et al.* [17]	Chuang and Chen [16]	Li and Hwang [10]
A1	Yes	Yes	Yes	No
A2	Yes	Yes	Yes	Yes
A3	Yes	Yes	Yes	Yes
A4	Yes	Yes	Yes	No
A5	Yes	No	No	No
A6	Yes	No	No	Yes
A7	Yes	No	No	No
A8	Yes	Yes	No	No
A9	Yes	Yes	Yes	No
A10	Yes	Yes	Yes	No

A1: User anonymity; A2: Human Participation; A3: Simple Password Change; A4: Mutual Authentication; A5: Resistance against impersonation attack; A6: Resistance against server spoofing; A7: Resistance against Stolen Smart card attack; A8: Resistance against Man-in-the-middle attack; A9: Resistance against Insider Attack; A10: Session Key verification.

The computational cost of the authentication scheme depends on the hash function and the operations performed. The following notations are used for computing the computational complexity of the proposed scheme:

T_h: time for executing a one-way hash function h(.).
T_x: time for executing exclusive – OR operation.
T_c: time required for executing comparison operation.

Table 3. Performance Comparison with Existing Scheme

Phase	Proposed Scheme	Mishra *et al.* [17]	Chuang and Chen [16]	Li and Hwang [10]
P1	$5T_h+3T_x$	$7T_h+5T_x$	$3T_h+3T_x$	$3T_h+T_x$
P2	$6T_h+5T_x+T_c$	$6T_h+6T_x+T_c$	$4T_h+3T_x+T_c$	$T_h+2T_x+T_c$
P3	$9T_h+6T_x+2T_c$	$12T_h+5T_x+3T_c$	$13T_h+6T_x+3T_c$	$5T_h+4T_x+2T_c$
P4	$8T_h+6T_x+T_c$	$5T_h+3T_x+T_c$	$2T_h+5T_x+T_c$	$3T_h+2T_x+ T_c$
Total	$28T_h+20T_x+4T_c$	$30T_h+19T_x+5T_c$	$22T_h+17T_x+5T_c$	$12T_h+9T_x+4T_c$

P1: Registration Phase; P2: Login Phase; P3: Authentication Phase; P4: Password Change Phase

Table 3 shows that the computational cost of the proposed scheme is relatively lower than Mishra *et al*.'s [17] scheme but with higher security. We can conclude that the security can be enhanced by affording a little bit of extra cost.

6. Conclusion

In this paper, we have proposed a user-friendly authentication scheme using smart card where the users need not to spend any extra effort to remember any alphanumeric complicated password for the assurance of higher security. Our proposed scheme not only uses the graphic-based password but also can provide the security to a quality level at lower cost. Therefore, our scheme is well suited for practical implementation for all kind of users even though they are not expertise in computer.

References

[1] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, no. 11, pp. 770–772, **1981**.
[2] N. M. Haller, "The S/KEY one-time password system," RFC1760, February **1995**.
[3] G. Horng, "Password authentication without using a password table," Information Processing Letters, vol. 55, no. 5, pp. 247–250, **1995**.
[4] M.-S. Hwang and L.-H. Li, "A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 46, no.1, pp. 28–30, **2000**.
[5] C.-T. Li, C.-C. Lee, C.-J. Liu, and C.-W. Lee, "A robust remote user authentication scheme against smart card security breach," Proceedings of Data and Applications Security and Privacy XXV, vol. 6818, pp. 231–238, **2011**.
[6] S. S. Sonwanshi, R. R. Ahirwal, and Y. K. Jain, "An efficient smart card based remote user authentication scheme using hash function," in Proceedings of the IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS '12), pp.1–4, March **2012**.
[7] R. Madhusudhan, R. C. Mittal, "Dynamic Id-based remote user password authentication schemes using smart cards: A review", Journal of Network and Computer Application, vol. 35, no. 4, pp. 1235-1248, **2012**.
[8] J.-Y. Liu, A.-M. Zhou, and M.-X. Gao, "A new mutual authentication scheme based on nonce and smart cards," Computer Communications, vol. 31, no. 10, pp. 2205–2209, **2008**.
[9] M. K. Khan, "Fingerprint biometric-based self-authentication and deniable authentication schemes for the electronic world," IETE Technical Review, vol. 26, no. 3, pp. 191–195, **2009**.
[10] C.-T. Li and M.-S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," Journal of Network and Computer Applications, vol.33, no.1, pp.1–5, **2010**.
[11] X. Li, J.W. Niu, J. Ma, W.D. Wang, and C.L. Liu, "Cryptanalysis and improvement of a biometric-based remote authentication scheme using smart cards". Journal of Network and Computer Applications, vol. 34, pp. 73–79, **2011**.
[12] A.K Das, "Analysis and improvement on an efficient biometric based remote user authentication scheme using smart cards". IET Information Security, vol. 5, no. 3, pp. 145-151, **2011**.
[13] V.C Sekhar, and Mrudula.S. "Secure and Efficient Biometric Based Remote User Authentication Scheme Using Smart Cards" ICECIT, Dec 21, SRIT, India, **2012**.
[14] Y. An, "Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards," Journal of Biomedicine and Biotechnology, vol. 2012, **2012**.
[15] M. K. Khan, and S. Kumari, "An Improved Biometrics-Based Remote User Authentication Scheme with User Anonymity", BioMed Research International, Hindawi Publishing Corporation, **2013**.
[16] M.-C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics." Experts Systems with Applications, Vol. 41, No. 4, pp. 1411-1418, **2014**.
[17] D. Mishra, A. K. Das and S. Mukhopadhyay, "A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards.", Expert Systems with Applications, vol. 41, no. 18, pp. 8129-8143, **2014**.
[18] T. Maitra, D. Giri, "An Efficient Biometric and Password-Based Remote User Authentication using Smart Card for Telecare Medical Information Systems in Multi-Server Environment." Journal of Medical Systems, vol. 38, no. 12, **2014**

Authors

Khanjan Changmai Baruah, he received his B.Tech in Computer Science and Engineering from Tezpur University, Assam, India in 2013. Currently, he completed M.Tech degree in Mobile Communication and Computing from National Institute of Technology, Arunachal Pradesh. His research interests are Network Security, Wireless Ad hoc Network and Green computing.

Subhasish Banerjee, he received his M.Tech degree in Computer Application from Indian School of Mines, Dhanbad, India in 2012. Currently he is pursuing his Ph.D. and also working as Assistant Professor in the Department of Computer Science and Engineering in National Institute of Technology, Arunachal Pradesh. His research activities are mainly focused on cryptography and information security.

Manash Pratim Dutta, he received his M.Tech degree in Information Technology from Sikkim Manipal University, Sikkim, India in 2012. Currently, he is working as Assistant Professor in the Department of Computer Science and Engineering in National Institute of Technology, Arunachal Pradesh. His research activities are mainly focused on cryptography.

Chandan Tilak Bhunia, he did his B. Tech. in Radiophysics and Electronics in 1983 from Calcutta University. He received his M. Tech. in Radiophysics and Electronics in 1985 and then joined North Bengal University as a lecturer of Computer Science & Applications in 1988. He became Assistant Professor of ECE at NERIST, Govt. of India in 1990. He got P. hd. in Computer Science & Engineering from Jadavpur University. He became a full Professor in 1997 at NERIST. Currently, he is working as a Director of National Institute of Technology, Arunachal Pradesh. He has published around 150 research papers in various national and international journals of repute. Under his supervision, five Ph.D. scholars got awarded and nine scholars are currently working in various fields.