Remote Access Control Mechanism Using Rabin Public Key Cryptosystem

Ruhul Amin and G.P. Biswas

Abstract There is no efficient algorithm for factoring a large composite number in polynomial time and the security of the Rabin cryptosystem is based on it. As large number of internet users access the web server everyday through insecure channel, therefore, user authentication along with privacy over the world is very important. In this paper, we first proposed Rabin cryptosystem based remote login authentication protocol without using smart card for accessing the web server securely. This paper not only proposed the authentication protocol, but it also applies well popular BAN logic to analyze the security of the proposed protocol. Additionally, we have presented informal security analysis. The proposed protocol not only contributes strong security, but it also achieves others advantages like mutual authentication property, efficient and user-friendly password change phase and an approach which helps to recover the forgot password securely.

Keywords Authentication · Rabin cryprosystem · BAN logic · Hash function · Security attacks

1 Introduction

In the client-server environment, many password-based user authentication schemes with smart card are widely used to authenticate the user's identity. Smart cards are usually adopted to store the authentication information(s) at the time of registration

R. Amin (✉) · G.P. Biswas
Department of Computer Science and Engineering, Indian School of Mines,
Dhanbad, Jharkhand, India
e-mail: amin_ruhul@live.com

G.P. Biswas
e-mail: gpbiswas@gmail.com

J.K. Mandal et al. (eds.), *Information Systems Design and Intelligent Applications*,
Advances in Intelligent Systems and Computing 339,
DOI 10.1007/978-81-322-2250-7_52

for the user. Smart card based authentication schemes may suffers from stolen smart card attack. In addition, the cost of the necessary infrastructure for smart card-based schemes, such as the cards and readers add substantially to the cost.

In 1981, it was Lamport [1] who proposed an authentication scheme where the server maintains a verification table which is insecure against stolen verifier attack and then many password with smart card based user authentication schemes [2–11] have been proposed in the literature. However, these schemes are not applicable in such environment because of using the smart card. In 2009, Rhee et al. [12] proposed remote user authentication scheme without smart card and claimed that their protocol achieves mutual authentication property. However, it has been observed that their protocol is insecure against impersonation attack and man-in-the-middle attack. To overcome the above security weaknesses, Chen et al. [13] proposed an improvement of the Rhee et al.'s [12] protocol and also claimed that their protocol is highly secure. After that, He et al. pointed out that Chen et al.'s protocol is vulnerable to privileged insider attack and does not support perfect forward secrecy with no key control. On the other hand, Zhu et al. [14] pointed out that Hwang and Yeh [15] protocol suffers from several kinds of attack and proposed an authentication scheme without smart card based on the ECC cryptosystem. They claimed that the attacker cannot launch any security weakness based on the their authentication protocol. However, Islam and Biswas [16] demonstrated that Zhu et al.'s [14] scheme suffers from several security weaknesses such as impersonation attack, clock synchronization problem and no session key agreement. In this paper, we have proposed Rabin cryptosystem based remote access control protocol without smart card for accessing securely the web server.

1.1 Road Map of the Paper

In Sect. 2, we briefly introduces the basic concept of Rabin cryptosystem and related hardness problem. Section 3 addresses our proposed protocol and the security analysis and the discussion are presented in Sect. 5. Finally, the conclusion of this paper is given in Sect. 6.

2 Preliminaries

This section briefly introduces the concept of Rabin cryptosystem and related computationally hardness problem which are presented below:

1. **Rabin Cryptosystem**: It is an asymmetric system, requires a public key and a private key. To generate a key pair, the system chooses two large prime number p, q such that $p, q \equiv 3\, mod\, 4$ and computes $n = pq$ and then declares n is the public key and the private key (p, q) kept secret.

Encryption: Chooses a message m and then computes $C = m^2 \, mod \, n$ is the ciphertext and sends it to the destination location.

Decryption: The decryption algorithm is not deterministic function. It applies Chinese Remainder Theorem and private key pairs for obtaining the plaintext and gets four roots as a output. Finally, the original message can be retrieved from the four roots.

2. **Factorization Problem**: It can be stated as the parameter n is known to anyone where $n = pq$, then factoring p, q is infeasible in polynomial time. The security of the Rabin cryptosystem is based on it.

3 Proposed Protocol

This section presents remote access control mechanism without using smart card based on the Rabin cryptosystem for accessing web servers remotely. To achieve mutual authentication and session key agreement, we presented all the process of our proposed protocol in the following as follows:

3.1 System Setup Process

In the system setup phase, the web server chooses two large prime number p, q such that $p, q \equiv 3 \, mod \, 4$ and computes $n = pq$ and finally publishes n as a public parameter and keeps (p, q) as a private key of the system.

3.2 Registration Process

The user initially chooses desired user name ID_i, password PW_i and sends $\langle ID_i, PW_i \rangle$ along with a valid e-mail id/mobile number to the server through secure channel. After receiving it, the web server S computes $V_i = h(ID_i \| p \| q) \oplus PW_i$ and stores ID_i, V_i, along with e-mail id in the verifier Table 1 and sends an acknowledge message to the user that the registration process has been completed successfully.

Table 1 Verifier table

Identity	Parameter	E-mail id/mobile number
ID_1	V_1	abc@gmail.com/9804557
ID_2	V_2	cba@gmail.com/9868754
ID_3	V_3	bca@gmail.com/9878712
.	.	.
.	.	.
ID_n	V_n	bca@gmail.com/9878712

3.3 Login and Authentication Process

This process executes several steps which are presented below:

Step 1: The user carefully provides the identity and password and press the login button on the web page. Then the user/client-end generates a 128 bits random number r_i and computes $L_i = r_i^2 \, mod \, n$, $G_i = h(ID_i \| PW_i \| r_i)$, $M_i = h(r_i)$, $K_i = M_i \oplus h(ID_i \| PW_i)$ and forwards the login message $\langle ID_i, L_i, K_i, G_i \rangle$ to the web server through public channel.

Step 2: After receiving the login message, the web server first checks the existence of the ID_i and if it does not exist, terminates the connection; otherwise, retrieves PW_i^* of the user by computing $PW_i^* = h(ID_i \| p \| q) \oplus V_i$. Then the web server further computes $A_i^* = h(ID_i \| PW_i^*)$, $M_i^* = K_i \oplus A_i^*$ and decrypts the ciphertext L_i by utilizing the Chinese remainder theorem and finally gets the four roots $\langle r_1, r_2, r_3, r_4 \rangle$ as a plaintext. After that, the web server takes four consecutive roots as a input $\langle r_1, r_2, r_3, r_4 \rangle$ and checks the condition whether $M_i^* = h(r_k)$ or not where (k = 1 to 4) and it is confirmed that one of the conditions must match with the M_i^*. The web server then checks the condition whether $G_i^* = G_i$ or not by computing $G_i^* = h(ID_i \| PW_i^* \| r)$. If the condition holds, the web server believes that the U_i is authentic.

Step 3: The web server generates a 128 bits random nonce r_j and computes $C_j = h(ID_i \| ID_s \| r_i \| PW_i^* \| r_j)$, $D_j = r_i \oplus r_j$ and forwards reply message $\langle ID_s, C_j, D_j \rangle$ to the user through public channel.

Step 4: After receiving the reply message, the user/client-end computes $r_j^* = D_i \oplus r_i$, $C_j^* = h(ID_i \| ID_s \| r_i \| PW \|_i r_j^*)$ and checks the correctness whether $C_j^* = C_j$ or not. If it does not hold, terminates the connection; otherwise, the user believes that the web server is authentic as well as the protocol achieves mutual authentication property and both the parties computes the session key $SK = h(ID_i \| ID_s \| r_i \| r_j)$ and starts secure communication.

3.4 Password Change Process

This phase is used rarely and should be provided in any password based authentication system. At the time of changing the password, the user provides the old information along with the new desired password PW_i^{new} and then the web server first authenticates the user based on old informations after executing the step-2 of the authentication process of the proposed protocol. After that, the web server computes $V_i^{new} = V_i \oplus PW_i \oplus PW_i^{new}$ and replaces the new computed value V_i^{new} with the old value V_i of the corresponding ID_i. Thus, the proposed protocol efficiently change the user's password.

3.5 Recovering Forgot Password Process

It is the common problem of many internet users that they forgot their password due to either accessing several number of web server or rarely used. Therefore, it is very important to provide their forgotten password securely. Initially, the user sends the user name and the e-mail id/mobile number to the web server and then checks whether the e-mail id/mobile number is registered or not by using the verification table. If the condition holds, it retrieves the password $PW_i = h(ID_i \| p \| q) \oplus V_i$ and sends it to the e-mail id/mobile number through secure channel with an acknowledge message to the user for checking their registered e-mail id/mobile number. Thus, our proposed protocol retrieves the forgot password of the user.

4 Authentication Proof Based on BAN Logic

This section addresses the security analysis of our proposed protocol using Burrows-Abadi-Needham logic [17, 18], generally called as BAN logic. The BAN logic is well-known formal model used to analyze the security of authentication and key distribution protocols in the literature. Some preliminaries and notations of the BAN logic are described in Table 2.

In order to prove the proposed protocol secure, the proposed protocol must satisfy the following goals based on the BAN logic which are given as follows:

- **Goal 1**: $U_i \mid\equiv U_i \overset{SK}{\leftrightarrow} S$
- **Goal 2**: $U_i \mid\equiv S \mid\equiv U_i \overset{SK}{\leftrightarrow} S$
- **Goal 3**: $S \mid\equiv S \overset{SK}{\leftrightarrow} U_i$
- **Goal 4**: $S \mid\equiv U_i \mid\equiv S \overset{SK}{\leftrightarrow} U_i$

First the proposed protocol is transformed into idealized form:

$$M_1 : U_i \rightarrow S : ID_i, L_i, K_i, G_i : \langle r_i \rangle_{PW_i}$$

$$M_2 : \ S \rightarrow U_i : ID_s, D_j, C_j : \langle r_j \rangle_{PW_i}$$

Second, the following assumptions about the initial state of the protocol are made to analyze the proposed protocol:

$$\begin{array}{ll} A_1 : U_i \mid\equiv \#(r_i) & A_4 : S \mid\equiv S \overset{PW_i}{\leftrightarrow} U_i \\ A_2 : RS \mid\equiv \#(r_j) & A_5 : \ S \mid\equiv U_i \Rightarrow r_i \\ A_3 : \ U_i \mid\equiv U_i \overset{PW_i}{\leftrightarrow} S & A_6 : \ U_i \mid\equiv S \Rightarrow r_j \end{array}$$

Table 2 List of notations used

Symbol	Description
U_i	User/client
n	The product of two large prime number p and q
S	Web server
ID_i	Identity of user U_i
PW_i	User’s password
(p, q)	The secret key of the server S
r_i	The random number of generated by the user
r_j	The random number selected by the web server
$\oplus$	The bitwise exclusive or operation
$\Vert$	The concatenation operation
$h(\cdot)$	One-way hash function, $h : (0, 1)^* \rightarrow (0, 1)^n$
$P \mid\equiv X$	P believes X
$P \lhd X$	P sees X
$P \mid \sim X$	P once said X
$P \Rightarrow X$	P has jurisdiction over X
$\#(X)$	The message X is fresh
$\langle X \rangle_Y$	The formulae X combined with the formulae Y
$\{X\}_K$	The formulae X is encrypted under the key K
$P \overset{K}{\leftrightarrow} Q$	Principals P and Q communicate via shared key K
$P \overset{X}{\rightleftharpoons} Q]$	The formula X is a secret known only to P and Q
SK	The session key used in the current session
$\frac{P \mid\equiv P \overset{K}{\rightleftharpoons} Q, P \lhd \langle X \rangle_K}{P \mid\equiv Q \mid \sim X}$	Message-meaning rule
$\frac{P \mid\equiv (X), P \mid\equiv Y}{P \mid\equiv (X,Y)}$	Belief rule
$\frac{P \mid\equiv \#(X), P \mid\equiv Q \mid \sim X}{P \mid\equiv Q \mid\equiv X}$	Nonce-verification rule
$\frac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$	Jurisdiction rule
$\frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\equiv X}{P \mid\equiv P \overset{K}{\leftrightarrow} Q}$	Session keys rule

Third, the idealized form of the proposed protocol is analyzed based on the BAN logic rules and the assumptions. The main proofs are stated as follows:

$$M_1 : U_i \rightarrow S : ID_i, L_i, K_i, G_i : \langle r_i \rangle_{PW_i}$$

According to seeing rule, we get $S1 : S \lhd ID_i, L_i, K_i, G_i : \langle r_i \rangle_{PW_i}$.

According to A3, S1 and message meaning rule, we get $S2 : S \mid\equiv U_i \mid \sim r_i$.

According to A2, S2 and freshness-conjuncatenation rule and nonce verification rule is applied, we get $S3 : S \mid\equiv U_i \mid \equiv r_i$, where r_i is the necessary parameter of the session key of the proposed protocol.

According to A5, S3 and the jurisdiction rule is applied, we get $S4 : S\,|{\equiv}\, r_i$.

According to A2, S3 and the session key rule is applied, we get $S5 : S\,|{\equiv}\, S \overset{SK}{\leftrightarrow} U_i \quad (\mathbf{Goal\,3})$.

According to A2, S5 and the nonce verification rule is applied, we get $S6 : S\,|{\equiv}\, U_i\,|{\equiv}\, S \overset{SK}{\leftrightarrow} U_i \quad (\mathbf{Goal\,4})$

$$M_2 : S \rightarrow U_i : ID_s, D_j, C_j : \langle r_j \rangle_{PW_i}$$

According to seeing rule, we get $S7 : U_i \triangleleft ID_s, D_j, C_j : \langle r_j \rangle_{PW_i}$.

According to A4, S7 and the message meaning rule, we get $S8 : U_i| \equiv S| \sim r_j$.

According to A1, S8 and freshness-conjuncatenation rule and nonce verification rule is applied, we get $S9 : U_i\,|{\equiv}\, S\,|{\equiv}\, r_j$, where r_j is the necessary parameter of the session key of the proposed protocol.

According to A6, S9 and the jurisdiction rule is applied, we get $S10 : U_i\,|{\equiv}\, r_j$.

According to A1, S9 and the session key rule is applied, we get $S11 : U_i\,|{\equiv}\, U_i \overset{SK}{\leftrightarrow} S \quad (\mathbf{Goal\,1})$.

According to A1, S11 and nonce verification rule is applied, we get $S12 : U_i\,|{\equiv}\, S\,|{\equiv}\, U_i \overset{SK}{\leftrightarrow} S \quad (\mathbf{Goal\,2})$.

The above discussion proves our objectives mentioned above using BAN logic and it is clear that the U_i and the S performs mutual authentication and key agreement property securely.

5 Security Analysis and Discussion of the Proposed Protocol

In wireless communication system, it is our assumption that an attacker has maximum power or capabilities over the insecure communication such as (1) the login-reply messages of the proposed protocol passes through the attacker, so the attacker can trap, delete, re-generate, re-route the login-reply message and try to authenticate him/herself to the server or user for retrieving the confidential information(s). The following subsections present the security strength of the proposed protocol:

5.1 Strong Security Protection on the Password

It is our assumption that the proposed protocol uses the low entropy password which is guessable in off-line mode in polynomial time, in spite of that the attacker cannot derive or guess the password. We assume that the attacker traps the login-reply message of the protocol and tries to find out the password from the $\langle G_i, K_i, C_j \rangle$ parameters. It is very clear that the attacker cannot derive the password from the known parameters, as all the parameters are protected by the non-invertible cryptographic one-way hash function. As mentioned in [19], the probability of guessing the user's password composed of exactly n character is $\frac{1}{2^{6n}}$. Therefore, the probability of guessing the password from the G_i, K_i and C_j are $\frac{1}{2^{6n+128}}$ and $\frac{1}{2^{6n+256}}$ respectively which are enormously negligible and infeasible in polynomial time.

5.2 Strong Security Protection on Login-Reply Message

In the protocol, the login parameter G_i is dependent on the user's password, random number and it is possible that an attacker can generate a random number easily. As the login parameters are dependent on the user's password, therefore the attacker fails to forge the valid login message and the same case is also applicable for the reply message. Thus, we can claim that our proposed protocol provides strong security protection on the login-reply message.

5.3 Strong Security Protection on Session Key

The session key of the authentication protocol must be different for each authentication cycle and if it is disclosed, an attacker can decrypt the ciphertext and will obtain the confidential information. As the attacker cannot retrieve the random numbers from the login-reply messages, he/she fails to compute the session key. If an attacker tries to guess it, the probability of guessing is $\frac{1}{2^{256}}$, which is dreadfully hard in polynomial time.

5.4 Strong Security Protection on Stolen-Verifier Attack

After hacking the verifier table, the attacker tries to extract confidential information (s) from it. As the computation $h(ID_i||p||q)$ depends upon the secret key of the server, he/she cannot extract the user's password from the V_i parameter. Therefore, the protocol provides strong security protection on it.

6 Conclusion

This paper contributes an efficient remote access control protocol without using smart card usable for client-server environment and the well popular BAN logic proves that the proposed protocol agreement a session key in each authentication cycle securely. The informal security analysis are also made and it confirms that the proposed protocol has strong security protection on the user's password, login-reply message, session key and verifier-table. This paper not only provides strong security protection on the authentication protocol, but it also contributes (1) an efficient password change phase, (2) retrieving forgot password procedure, (3) mutual authentication property, and (4) session key agreement etc.

References

1. Lamport, L.: Password authentication with insecure communication. Commun ACM **24**(11), 770–772 (1981)
2. Khan, M.K., Zhang, J.S.: Improving the security of a flexible biometrics remote user authentication scheme. Comput. Stand. Interface **29**(1), 82–85 (2007)
3. Liu, J.Y., Zhou, A.M., Gao, M.X.: A new mutual authentication scheme based on nonce and smart cards. Comput. Commun. **31**(10), 2205–2209 (2008)
4. Li, C.T., Lee, C.C.: A robust remote user authentication scheme using smart card. Inf. Technol. Control **40**(3), 236–245 (2011)
5. Li, X., Qiu, W., Zheng, D., Chen, K., Li, J.: Anonymity enhancement on robust and efficient password authenticated key agreement using smartcards. IEEE Trans. Industr. Electron. **57**(2), 43–48 (2010)
6. Amin, R.: Cryptanalysis and an efficient secure ID-based remote user authentication scheme using smart card. IJCA **75**(13), 1149–1157 (2013)
7. He, D., Chen, Y., Chen, J.: Cryptanalysis and improvement of an extended chaotic maps based key agreement protocol. Nonlinear Dyn **69**(3), 37–42 (2012)
8. Amin, R., Maitra, T., Rana, S.: An improvement of Wang. et. al.'s remote user authentication scheme against smart card security breach. IJCA **75**(13), 405–410 (2013)
9. He, D., Chen, J., Hu, J.: Improvement on a smart card based authentication scheme. J. Internet Technol. **13**(3), 236–248 (2012)
10. Wu, S., Zhu, Y., Pu, Q.: Robast smart card based user authentication scheme with user anonymity. Secur. Commun. Netw **5**(2), 181–185 (2012)
11. Goriparthi, T., Das, M.L., Saxsena, A.: An improved bilinearing pairing based remote client authentication protocol. Comput. Stand. Interface **31**(1), 181–185 (2009)
12. Rhee, H.S., Kwon, J.O., Lee, D.H.: A remote user authentication scheme without using smart cards. Comput Stand. Interface **31**(1), 6–13 (2009)
13. Chen, B., Kuo, W., Wuu, L.: A secure password based remote user authentication scheme without using smart cards. Inf. Technol. Control **41**(1), 53–59 (2012)
14. Zhu, L., Yu, S., Zhang, X.: Improvement upon mutual password authentication scheme. Inter. Semin. Bus. Inf. Manage. **1**, 400–403 (2008)
15. Hwang, J.J., Yeh, T.C.: Improvement on Peyravian-Zunic's password authentication schemes. IEICE Trans. Commun. **E85-B**(4), 823–825 (2002)
16. Islam, S.K., Biswas, G.P.: Improved remote login scheme based on ECC. IEEE-Inter. Conf. Recent Trends Inf. Technol. ICRTIT, pp. 6–13 (2011)
17. Burrows, M., Abadi, M., Needham, R.: A logic of authentication. ACM Trans. Comput. Syst. **8**(1), 1836 (1990)
18. Tsai, J.-L., Wu, T.-C., Tsai, K.-Y.: New dynamic ID authentication scheme using smart cards. Int. J. Commun. Syst. **23**, 1449–1462 (2010)
19. Chang, Y.-F., Yu, S.-H., Shiao, D.-R.: An uniqueness-and anonymity-preserving remote user authentication scheme for connected health care. J. Med. Syst. **37**, 9902 (2013)