4th International Conference on Eco-friendly Computing and Communication Systems

RSA Based Two-Factor Remote User Authentication Scheme with User Anonymity

Preeti Chandrakar\textsuperscript{a} and Hari Om\textsuperscript{b}

\textsuperscript{a, b}Department of Computer Science and Engineering
Indian School of Mines, Dhanbad, Jharkhand -826004, India

Abstract

Remote user authentication is one of the most commonly used mechanisms to verify the legitimacy of a remote user over insecure communication channel. In remote user authentication, the server and the user mutually authenticate each other and establish a common session key for future communication. In this paper, we propose a secure and effective two-factor remote user authentication scheme based on RSA, which achieves mutual authentication and user anonymity properties. Informal security analysis ensures that the proposed scheme is secure against various malicious attacks and its security is based on the one-way hash function, smart card, and RSA algorithm. Performance comparison shows that the proposed scheme is efficient in terms of communication and computation overhead. Furthermore we demonstrate the validity of our proposed through BAN logic, which confirm that the proposed scheme achieve mutual authentication and session key agreement securely.

Keywords: Authentication, BAN logic, RSA cryptosystem, Smart card, User anonymity;

1. Introduction

One of the most convenient and well popular two factor authentication scheme is based on smart card and password. It has been extensively used in different types of applications such as remote host login, e-banking, online
pay-TV, e-commerce, online bill payment, e-mail, etc. In order to access these application servers, a mutual authentication and key agreement scheme is needed, in which the remote server and the user mutually authenticate each other and generate a common session key. In 1981, Lamport proposed the first remote authentication scheme based on smart card [1]. However, in their scheme the server must store a password list and consequently cannot resist the interpolation attack. After that, many password authentication schemes have been proposed to improve the scheme security and enhance their functionality [2-8].

In 1999 Yang et al. proposed an authentication scheme based on RSA cryptosystem [5]. However, Chan et al. [6] show that Yang et al. scheme is not secure and vulnerable to impersonation attack. In 2002, Fan et al. [7] also prove that Yang et al. scheme could not withstand user impersonation attack and proposed a slight modification to resist this attack. In 2003, Shen et al. [8] proposed a modified Yang et al. scheme to enhance security. This scheme could withstand the impersonation attack and also provide mutual authentication. In recent years, many RSA based authentication scheme have been proposed by researcher [9-12]. The security of RSA cryptosystem is based on the difficulty of factoring large prime integers. In this paper, we propose a two-factor remote user authentication scheme with user anonymity based on RSA that provides mutual authentication with key agreement. In addition, we use BAN logic to demonstrate the validity of the proposed scheme. Our scheme precisely comprises of the following merits: (1) It has an efficient login phase, where an incorrect input can be quickly detected. (2) It has an efficient and user friendly password change phase where user can change his password without server assistant. (3) It provides user anonymity. (4) It supports mutual authentication and session key agreement. (5) The computation cost and communication cost are comparable with other relevant schemes. (6) It satisfies all desired security attributes.

The rest of paper is organized as follows: In section 2, we describe our proposed scheme. The formal and informal security analysis is presented in section 3. The functionality and performance comparison among the proposed scheme and other relevant schemes demonstrate in section 4. Finally the conclusion of our proposed scheme is described in section 5.

2. Proposed Scheme

Our scheme has five phases: initialization phase, registration phase, login phase, authentication and key agreement phase, and password change phase.

2.1 Initialization Phase

In this phase, the remote server S chooses the system parameters. For this purpose, the remote server S generates two large prime numbers p and q and compute n = p×q. The public key e is chosen randomly such that 1 < e < \( \phi(n) \) and gcd \( (e, \phi(n)) = 1 \), where \( \phi(n) = (p-1) \times (q-1) \). The private key is computed as \( d = e^{-1} \mod \phi(n) \) where d is multiplicative inverse of e \( \mod \phi(n) \). The remote server publishes \{e, n\} as public key and \{d, p, q\} as private key.

2.2 Registration Phase

When a new user \( U_i \) wants to register or re-registers in the remote server, he/she chooses identity \( ID_i \), password \( PW_i \) and generates a random number r and computes \( RPW = h(PW_i || r) \). Then the user sends registration request message \( (ID_i, RPW) \) to the server S via a secure channel. After receiving the registration request message from the user \( U_i \), the server S computes \( MK = h(ID_i || d) \), \( L = MK \oplus RPW \), \( B = h(MK || RPW) \), \( J = ID_i^e \mod n \) and \( Y = J \oplus B \). Then the server sends a smart card containing the information \{Y, L, h(\cdot), n, e\} to the user \( U_i \) through secure channel. After receiving the smart card securely from the server S, the user stores a random number r in the memory of the smart card. Finally the smart card contains \{Y, L, h(\cdot), n, e, r\} and the registration phase is successfully completed.

2.3 Login Phase

Whenever a new user wants to access the remote servers, he/she inserts the smart card into the smart card reader and enters his ID, and PW. Smart card computes \( RPW = h(PW || r) \). The server S verifies the entered ID and password and checks whether \( Y \) equals to entered ID or not. If they are not equal, the session is terminated by the smart card. Otherwise, the user is legal owner of smart card. Then the smart card generates a random nonce \( R_i \), computes \( AID = ID_i \oplus h(R_i || MK) \), \( C_i = h(R_i || MK || Y) \), \( V_i = h(ID_i || C_i || R_i || MK)^e \mod n \), \( R'_i = R_i \oplus h(MK || ID_i) \) and sends the login request message \{AID, C_i, V_i, R'_i\} to the server S through a public channel.
2.4 Authentication and Key agreement Phase

In this phase, the server and user authenticate each other and generate a session key for future communication by performing the following steps.

1. After receiving the login request message \{AID, C_i, V_i, R_i\}, the server computes \(R_i = R_i \oplus h(MK || ID_i)\), \(ID_i = AID \oplus h(R_i || MK)\), \(C_i = h(R_i || MK || Y_i)\), \(V_i = h(ID_i || C_i || R_i || MK) \mod n\) and \(V_i = h(ID_i || C_i || R_i || MK)\). Then server matches \(ID_i\) with the stored \(ID\). \(V_i = V_i\) and \(C_i = C_i\). If it does not hold, this phase is terminated immediately, otherwise, the server believes that the user is legitimate entity and it generates a random nonce \(R_i\) and computes \(E_i = h(R_i || MK || Y)\), \(R_j = R_j \oplus h(MK || ID_j)\), \(V_j = h(ID_j || E_i || R_j || MK)\). Then server sends \((E_i, R_j, V_j)\) to the user \(U_i\).

2. After receiving the authentication message \{\(E_i, R_j, V_j\)\} from the server, the user \(U_i\) computes \(R_j \oplus h(MK || ID_i)\), \(E_i = h(R_j || MK || Y)\) and \(V_j = h(ID_i || E_i || R_i || MK)\). Then the user matches \(E_i = E_i\) and \(V_j = V_j\). If matched, the user is authenticated to the server and mutual authentication holds good.

3. Finally the server \(S\) and the user \(U\) agree upon a common secret session key \(SK = h(R_i || MK || R_j || Y)\).

2.5 Password Change Phase

This phase is invoked when the user wants to change the password, the user inserts his/her smart card into smart card reader and keys in \{\(ID_i\), \(PW_i\)\}. The smart card computes \(RPW = h(PW_i || r)\), \(MK' = L \oplus RPW\), \(B' = h(MK' || RPW')\), \(Y' = J \oplus B \oplus B'\), \(Y = J^s \mod n\) and checks whether \(Y'\) is equal to entered \(ID\) or not. If condition hold, it means the user is legitimate holder of smart card. Now the user enters his new password \(PW_{i, new}\) and smart card computes \(RPW_{i, new} = h(PW_{i, new} || r)\), \(L_{i, new} = L \oplus RPW \oplus RPW_{i, new}\), \(Y_{i, new} = Y \oplus RPW \oplus RPW_{i, new}\). Then the smart card replaces \(Y\) with \(Y_{i, new}\) and \(L\) with \(L_{i, new}\) in its memory. Now the new password successfully updated.

3. Security Analysis of the Proposed Scheme

3.1. Authentication Proof Based on BAN logic

BAN logic [16] is one of the most popular and widely used logics, which ensures that the proposed scheme achieves mutual authentication and session key agreement securely. To implement BAN logic to prove an authentication scheme, the following steps should be performed.

**STEP1:** We show the verification goals of the proposed scheme as follows:

- **Goal 1:** \(U_i \equiv (U_i \xrightarrow{SK} S)\)
- **Goal 2:** \(U_i \equiv S \equiv (U_i \xrightarrow{SK} S)\)
- **Goal 3:** \(S \equiv (U_i \xrightarrow{SK} S)\)
- **Goal 4:** \(U_i \equiv (U_i \xrightarrow{SK} S)\)

**STEP2:** We transform our proposed scheme to the idealised form as follows:

Message 1. \(U_i \rightarrow S:\) \(AID, C_i, V_i; < ID_i, C_i, R_i >_{MK}, R_i\)

Message 2. \(S \rightarrow U_i:\) \(E_i, V_i; < ID_i, E_i, R_i, R_i >_{MK}, R_i\)

**STEP3:** We make the following assumption about the initial state of the scheme to analyze the proposed scheme

\[A_1: U_i \equiv (R_i, R_i)\]

\[A_2: S \equiv (R_i, R_i)\]

\[A_3: U_i \equiv U_i \xrightarrow{MK} S\]
STEP4: Based on the above-mentioned assumptions and rules of BAN logic, we prove the security of the proposed scheme and main procedures of proof as follows: According to the message 1, we obtain:

\[ S_1 : S \xleftarrow{\text{AID}, C_i, V_1} \langle < \text{ID}_u, C_i, R_i \rangle >_{MK}, R_i \rangle \]

According to \( S_1 \), \( A_4 \) and the message meaning rule, we obtain

\[ S_2 : S \equiv U_i |\sim ( \text{ID}_i, C_i, R_i ) \]

According to \( A_2 \), we apply the freshness conjunction rule to obtain

\[ S_3 : S \equiv \#( \text{ID}_i, C_i, R_i ) \]

According to \( S_2 \) and \( S_3 \) we apply the nonce verification rule to obtain

\[ S_4 : S \equiv U_i \equiv ( \text{ID}_i, C_i, R_i ) \]

According to \( S_4 \), \( A_5 \) and jurisdiction rule, we obtain

\[ S_5 : S \equiv ( \text{ID}_i, C_i, R_i ) \]

According to \( S_4 \), \( A_2 \) and session key rule, we obtain

\[ S_6 : S \equiv ( U_i \xleftarrow{\text{SK}} S ) \quad \text{Goal 3} \]

According to \( S_6 \), \( A_2 \) and nonce verification rule, we obtain

\[ S_7 : S \equiv U_i \equiv ( U_i \xleftarrow{\text{SK}} S ) \quad \text{Goal 4} \]

According to the message 2, we obtain

\[ S_8 : U_i \xleftarrow{\text{E}_j} \langle \text{E}_j, V_2 : < \text{ID}_p, E_i, R_i, R_j >_{MK}, R_j \rangle \]

According to \( S_8 \), \( A_3 \) we apply message meaning rule to obtain

\[ S_9 : U_i \equiv S |\sim ( \text{ID}_i, C_i, R_i, R_j ) \]

According to assumption \( A_1 \) we apply the freshness conjunction rule to obtain

\[ S_{10} : U_i \equiv \#( \text{ID}_i, C_i, R_i, R_j ) \]

According to \( S_9 \) and \( S_{10} \) we apply the nonce verification rule to obtain

\[ S_{11} : U_i \equiv S \equiv ( \text{ID}_i, C_i, R_i, R_j ) \]

According to \( S_{11} \), \( A_6 \) and jurisdiction rule, we obtain

\[ S_{12} : U_i \equiv ( \text{ID}_i, C_i, R_i, R_j ) \]

According to \( S_{11}, A_1 \) and session key rule, we obtain

\[ S_{13} : U_i \equiv ( U_i \xleftarrow{\text{SK}} S ) \quad \text{Goal 1} \]

According to \( S_{13}, A_1 \) and nonce verification rule, we obtain

\[ S_{14} : U_i \equiv S \equiv U_i \xleftarrow{\text{SK}} S \quad \text{Goal 2} \]

3.2 Further Security Analysis and Discussion

Proposition 1: An attacker A from outside of the system gets the user’s smart card and reveals the information \( \{ Y, L, r \} \) stored in it, then he will not be able to guess the user’s password and private key \( d \).

Proof: If by any means the attacker A gets the user’s smart card and extracts the information \( \{ Y, L, r \} \) stored in it. We show that the adversary A cannot get user’s identity, password and secret key \( d \) as follows:

1. A has \( L = MK \oplus \text{RPW} = h(ID_i || d) \oplus h(PW_i || r) \), for a given \( r \). But it is computationally hard to
extract identity $ID_i$, password $PW_i$ and secret key $d$, from $L$ due to inversion of cryptographic one-way hash function. Thus, attacker cannot solve one equation for three unknown values.

2. A has $Y = J \oplus B = ID_i^d \mod n \oplus h(MK||RPW) = ID_i^d \mod n \oplus (h(ID_i||d)||h(PW_i||r))$ for given $r$. But it is computationally hard to extract identity $ID_i$, password $PW_i$ and secret key $d$, from $Y$ due to inversion of cryptographic one-way hash function.

**Proposition 2:** An attacker $A$ from inside of the system uses his own smart card parameters $\{Y, L, r\}$, then he cannot extract private key $d$ of the server.

**Proof:** In this attack model, a legal but malicious user tries to extract the private key $d$ by using his own $\{ID_i, PW_i\}$ and smart card parameters $\{Y, L, r\}$. In the following, we show that the malicious user cannot get the secret key $d$.

1. A has $L = MK \oplus RPW = h(ID_i||d) \oplus h(PW_i||r)$. But it is computationally hard to extract the secret key $d$ from $L$ due to inversion of cryptographic one-way hash function.

2. A has $Y = J \oplus B = ID_i^d \mod n \oplus h(MK||RPW) = ID_i^d \mod n \oplus (h(ID_i||d)||h(PW_i||r))$. Due to factorization problems and inversion of cryptographic function, it is hard to find $d$ from $Y$.

**Proposition 3:** An attacker $A$ from the outside of the system cannot know the user’s identity $ID_i$, server’s private key $d$, random nonce $R_i$ and $R_j$, from the login request message $\{AID, C_i, V_i, R_i\}$ and reply message $\{E_i, R'_j, V'_j\}$.

**Proof:** In this attack model, the attacker traps the login request message $\{AID, C_i, V_i, R'_j\}$ and reply message $\{E_i, R'_j, V'_j\}$. We show that the attacker cannot extract user’s identity $ID_i$, private key $d$, random nonce $R_i$ and $R_j$.

1. We have $AID = ID_i \oplus h(R_i||MK) = ID_i \oplus h(R_i\oplus h(ID_i||d)||h(PW_i||r))$. An attacker has to guess two unknown parameters $R_i$ and $d$ at the same time to get the user’s identity from the above equation, which is infeasible.

2. Similarly, the attacker cannot verify an identity $ID_i$ from $\{C_i, R'_j\}$ parameters due to the same reason.

3. From $V_i = h(ID_i||C_i||R_i||MK)^e \mod n = h(ID_i||C_i||R_i||h(ID_i||d)) \mod n$, due to factorization problem, it is hard to find $d$ from $e$. An attacker cannot decode $h(ID_i||C_i||R_i||MK)^e \mod n$ from $V_i$ without knowing $d$. Hence the attacker cannot extract user’s identity $ID_i$, private key $d$ of the server and random nonce $R_i$.

4. From $E_i = h(R_i\oplus MK||Y) = h(R_i \oplus h(ID_i||d)||Y)$. An attacker has to guess two unknown parameters $R_i$ and $d$ at the same time to get the user’s identity from the above equation, which is infeasible.

5. Similarly, the attacker cannot obtain the identity $ID_i$ from $\{R'_j, V'_j\}$ parameters due to the same reason.

**Proposition 4:** An attacker $A$ from the inside of the system cannot know server’s private key $d$ of the server from the login request message $\{AID, C_i, V_i, R'_j\}$ and reply message $\{E_i, R'_j, V'_j\}$ between the user and server.

**Proof:** In this attack model, a legal but malicious user tries to extract the private key $d$ of the server by intercepting the login request message $\{AID, C_i, V_i, R'_j\}$ and reply message $\{E_i, R'_j, V'_j\}$ between the user and server. Due to inversion of cryptographic hash function the attacker cannot compute the server’s private key $d$ from the message $MK = h(ID_i||d)$. Hence the proof of proposition 4.

3.2.1 Resistance to Insider attack

In real environment, it is common practice that many users use same password to access different servers for their convenience. However, if the privileged insider of $S$ has learnt the password of $U_i$, he may try to impersonate $U_i$ by access the other server. In our scheme, $U_i$ registers with $S$ by presenting $RPW = h(PW_i||r)$ instead of $h(PW_i)$. The insider of $S$ cannot directly obtain $PW_i$. Therefore, our scheme is secure against the insider attack.

3.2.2 Resistance to password guessing attack

Proposition 1 and proposition 3 show that an attacker cannot extract or guess the user’s password and secret key $d$ using the secret values extracted from the smart card and communication message between user and server. Thus our scheme is secure against the password guessing attack.

3.2.3 Resistance to Replay attack

An adversary may intercept the previous login request and reply message. Then the attacker can impersonate $U_i$ to access the server by sending the intercepted message. However, in each session of our scheme, the user $U_i$ and the server $S_i$ generate a different random nonce $R_i$ and $R_j$, respectively. The random nonce ensures that the authentication messages are distinct in different sessions and valid for that session only. Therefore our scheme is...
secure against replay attack.

3.2.4 Resistance to Forward secrecy attack

Forward secrecy means that if the master key of the system is compromised, then the secrecy of previously established session key should not be affected. In our scheme, if the master key MK and Y are compromised due to some reason, the attacker cannot compute the session key without knowing the values of $R_i$ and $R_j$. Therefore our scheme is secure against the forward secrecy attack.

3.2.5 Resistance to user impersonation and server spoofing attack

Propositions 1, 2, 3, and 4 show that an adversary cannot extract the secret information between the user and server. Thus the attacker cannot create valid login request and reply message without knowing the secret information between the user and server. Thus our scheme is secure against the user impersonation and server spoofing attack.

3.2.6 Preserving User anonymity

In our scheme, the user’s anonymity is preserved in each login request. We compute an anonymous identity $AID = ID \oplus h(R_i || MK)$ for the user and this identity is different in each login attempt because it is calculated with the random nonce $R_i$. Only the authentication server knows the secret value MK and $R_i$. So only the authenticated server can retrieve user $ID_i$. Hence, in our scheme, an attacker cannot identify the person trying to log into the server.

4. Performance evaluation

In this section we compare security and performance of the proposed scheme with other relevant schemes [13, 14, 15]. In Table 1, we summarized the communication cost and computation cost of the proposed scheme and other relevant scheme. The total computation overhead of our scheme is $16T_h+3T_E$, where $T_h$ is time taken in the secure one-way hash function and $T_E$ is time taken in modular exponentiation operation. To analyze the communication overhead, we use the following facts and assumptions, identity, password, random nonce and output of secure one-way function are 160 bit long. One block in AES is 128 bit long and modular exponentiation operation takes 1024 bits. The communication overhead of our scheme is $160\times 6 + 1024 = 1984$ bits. In Table 2, we have presented several security functionalities comparison of the proposed scheme with other relevant schemes [13, 14, 15] and it is noticeable that the proposed scheme is secure against relevant security attacks than other schemes.

![Fig1: Performance Comparison: Communication Cost](attachment:fig1.png)

Table 1: Performance Comparison: Communication cost and Computation cost

| Performance Comparison | He et al.[13] | Pippal et al.[14] | Wen et al.[15] | Proposed Scheme |
|-------------------------|--------------|------------------|----------------|------------------|
| Communication Cost      | 1024*2+160*5=2848 | 1024*2+160*3=2528 | 1024+512*2+160=2208 | 160*6+1024=1984 |
| Computation Cost of Login Phase | $2T_h+2T_E$ | $1T_h+2T_E$ | $2T_h+3T_E$ | $5T_h+2T_E$ |
| Computation Cost of Authentication Phase | $3T_h+4T_E$ | $6T_h+5T_E$ | $3T_h+5T_E$ | $11T_h+1T_E$ |
| Total Computational Cost | $5T_h+6T_E$ | $7T_h+7T_E$ | $5T_h+8T_E$ | $16T_h+3T_E$ |
Table 2: Security Features Comparison

| Security Requirement                        | He et al. [13] | Pippal et al. [14] | Wen et al. [15] | Proposed Scheme |
|--------------------------------------------|---------------|-------------------|----------------|----------------|
| Resist Password Guessing Attack            | Yes           | No                | No             | Yes            |
| Resist Replay Attack                       | Yes           | No                | Yes            | Yes            |
| Resist Impersonation Attack                | No            | No                | No             | Yes            |
| Resist Denial of Service Attack            | Yes           | No                | No             | Yes            |
| Resist Forward Secrecy Attack              | Yes           | Yes               | Yes            | Yes            |
| Resist Insider Attack                      | Yes           | No                | Yes            | Yes            |
| Preserving User Anonymity                  | No            | No                | No             | Yes            |

5. Conclusion

In this paper, we have discussed a secure and effective remote user authentication scheme using smart card which achieves mutual authentication and user anonymity properties. In our scheme, the computational cost and communicational cost are relatively low as compared to the important related schemes. Furthermore, the user can always change his password correctly and locally at any time without contacting the server. In addition, we have demonstrated the validity of our scheme through the BAN logic. Finally, in our scheme after successful authentication, a symmetric session key is established between a user and the server so that we can use this key for future secure communication.

References

1. Lamport, Password authentication with insecure communication. Communications of the ACM, 1981, 24(11), pp. 770-772.
2. Chang, C. C. & Wu, T. C., Remote password authentication with smart cards. Computers and Digital Techniques, IEE Proceedings E, 1991, 138(3), pp. 165-168.
3. Chang, C. C., & Hwang, K. F., Some Forgery Attacks on a Remote User Authentication Scheme Using Smart Cards. Informatics, Lith. Acad. Sci., 2003, 14(3), pp. 289-294.
4. Lee, S. W., Kim, H. S., & Yoo, K. Y., Efficient nonce-based remote user authentication scheme using smart cards. Applied Mathematics and Computation, 2005, 167(1), pp. 355-361.
5. Yang, W. H., & Shiieh, S. P., Password authentication schemes with smart cards. Computers & Security, 1999, 18(8), pp. 727-733.
6. Chan, C. K., & Cheng, L. M., Cryptanalysis of a timestamp-based password authentication scheme. Computers & Security, 2001, 21(1), pp.74-76.
7. Fan, L., Li, J. H., & Zhu, H. W., An enhancement of timestamp-based password authentication scheme. Computers & Security, 2002, 21(7), pp. 665-667.
8. Shen, J. J., Lin, C. W., & Hwang, M. S., Security enhancement for the timestamp-based password authentication scheme using smart cards. Computers & Security, 2003, 22(7), pp. 591-595.
9. Giri, D., Maitra, T., Amin, R., & Srivastava, P. D., An efficient and robust RSA-based remote user authentication for telecare medical information systems. Journal of medical systems, 2015, 39(1), pp.1-9.
10. Amin, R., and Biswas GP, An improved RSA based user authentication and session key agreement protocol usable in TMIS. J. Med. Syst.2015, 39(8):pp. 1-14.
11. Ramasamy, Rajaram, and Amutha Prabakar Muniyandi. "An Efficient Password Authentication Scheme for Smart Card." IJ Network Security 14.3, 2012, pp. 180-186.
12. Das, A. K., & Bruhadeshwar, B., An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system. Journal of medical systems, 2013, 37(5), pp.1-17.
13. He, D., Wang, D., & Wu, S., Cryptanalysis and improvement of a password-based remote user authentication scheme without smart cards. Information Technology And Control, 2013,42(2), pp.105-112
14. Pippal, R. S., Jaidhar, C. D., & Tapaswi, S., Robust smart card authentication scheme for multi-server architecture. Wireless Personal Communications, 2013,72(1), pp. 729-745.
15. Wen, F., & Guo, D., An improved anonymous authentication scheme for telecare medical information systems. Journal of medical systems, 2014, 38(5), pp. 1-11.
16. Burrows, M., Abadi, M., Needham, R., A logic of authentication. ACM Transactions on Computer Systems, 1990, 8(1), 1836.