User Authentication From the Remote Autonomous Object

K. K. Goyal a and Kuldeep Bhardwaj b

a Faculty of Management & Computer Application, R.B.S.College, Khandari, Agra-282002 (U.P), E-Mail:kkgoyal@gmail.com
b Department of Mathematics, Institute of Basic Science, Dr.B.R.Ambedkar University, Khandari Agra-282002 (U.P), E-Mail:kuldeepibs@yahoo.co.in

ABSTRACT
In 2003, Novikov and Kiselev [6] proposed an authentication of the user from the remote autonomous object. In 2005 Yang et al [10] pointed out that Novikov and Kiselev scheme is insecure against the man-in-middle attack. In this paper, we propose an improvement to secure Novikov-Kiselev scheme against a reflection attack and man-in-middle attack.

KEYWORDS
Authentication, Remote User, RSA, Security

1. INTRODUCTION
The authentication scheme is commonly used for verifying a user’s identity. Only the authenticated users can access the remote systems. The scatter of remote systems in different places allows more efficient and convenient access for geographically dispersed users. Remote access is one of the applications which ascertain whether the user is legal and whether it can access [1, 2, 3, 4, 5, 8, 9]. In Novikov-Kiselev scheme [6], the authentication of the user is done from the remote autonomous object with public key cryptosystem. The scheme has applications in the telecommunications systems. In this paper, we propose an improvement to secure Novikov-Kiselev scheme against a reflection attack and man-in-middle attack.

2. NOTATIONS
- U i , O, and I denote the User, the remote autonomous Object, and the Intruder.
- ID i and K denote the user’s identifier and the control command.
- (P KU,S KU) and (P KO,S KO) denote a pair of session keys of U i and O, generated by RSA algorithm.
- (P KI,S KI) are the keys of Intruder generated by the RSA algorithm.
- T i denotes the time parameter.
- E(.) and D(.) are the encryption and decryption functions.

The Novikov-Kiselev scheme consists of two stages. In the first stage a user negotiates the identity with remote autonomous object before functioning as an object. In the second stage the user’s identity is verified, when the user communicates with the object.

3.1 THE FIRST STAGE
The user negotiates the identity ID i and the time parameter T 0 with the remote object beforehand. This step is executed just once. The ID i and T 0 are stored in the operative memory of the object by the user.

3.2 THE SECOND STAGE
Step 1: The user sends start communication request S to the object through the public communication channel.
Step 2: The object generates a pair of keys P KO and S KO by the RSA algorithm [7] and sends the public key P KO to the user. Note that S KO is kept securely by the object. Simultaneously, the object turns on the timer and records the start transmission time T 1.
Step 3: The user sends the encrypted message E P KO(ID i, P KU) to the object, where E A(M) is that message M is encrypted by the public key A using the encryption function E(.) of the RSA algorithm. The identity ID i and public key P KO is encrypted with P KO using the encryption function of the RSA algorithm. Note that the user also has a pair of keys P KU and S KU are kept securely by the user.
Step 4: The object decrypts the message D S KO(E P KO(ID i, P KU)) = (ID i, P KU) with secure key S KO using the decryption function of the RSA algorithm, where D B(M) is that, message M is decrypted by the secret key B using the decryption function D(.) of the RSA algorithm. T 2 is recorded simultaneously. If the difference in time ∆T between T 1 and T 2 is greater than T 0 compared with the user’s ID i. Supposing ID i discard with user’s ID i saved in memory of the object, then the object terminate the session. Otherwise, the object encrypts the message X with the user’s public key P KU using the RSA algorithm, and then sends it to the user.
Step 5: When the user receive the message from the object, the user decrypts X with secure key S KU using the RSA algorithm. The user can derive the command K from the message X and encrypt the command K and new identity ID i with public key P KO of object using the RSA algorithm. And then, the encrypted message is sent to the object. The object decrypts the message with the secure key S KO after receiving the message from the user. The object executes the command K, if the difference in time ∆T between T 1 and T 2 is smaller than T 0. The object terminate the session, or else. The procedures of this stage are shown in Figure 1.
User                  Autonomous Object

\[ S \]
\[ P_{KO} \]
\[ E_{PKO}(ID, P_{KU}) \]
\[ E_{PKI}(X) \]
\[ E_{PKO}(ID', K) \]

Figure 1: The procedures of the second stage

4. REFLECTION ATTACK
4.1 THE FIRST STAGE
The first stage is the pre-tuning of the parameters \( U_i \) and \( O \). \( U_i \) produces ID and synchronizes T with the remote object. This processing is executed just once. ID and T are produced and stored in the operative memory of O by \( U_i \).

4.2 THE SECOND STAGE
1) The user sends start request \( S \) to the object. He uses public channel for this purpose but intruder intercepts \( S \) and does not send \( S \) to object.
2) The Intruder uses RSA key generation algorithm. He computes \((S_{KI}, P_{KI})\) as private and public key respectively. Intruder sends \( P_{KI} \) to the user and starts timer to note the time \( T_i \).
3) The user computes the encrypted message using public key \( P_{KI} \) of Intruder \( E_{PKI}(ID, P_{KU}) \) Where \( P_{KU} \) is RSA public key of user and corresponding private key of user is \( S_{KI} \). User sends this encrypted message to the object.
4) The Intruder decrypts the message using \( S_{KI} \).
5) The Intruder encrypts his own message \( M \) with the public key of user \( P_{KU} \) and sends to the user: \( E_{PKU}(M) \)
6) When the user received the message from the Intruder he decrypts it with his secret key \( S_{KI} \). The user derives the command \( K \) from \( M \). User sends the following information: \( E_{PKI}(ID', K) \)
7) Now Intruder decrypts this message with \( S_{KI} \). Intruder can get the ID' and K. After that, Intruder can make whatever modification he wants.

Here we observe that whole communication is open in front of Intruder and Intruder intercept in between the user and object and create illusion of object.

5. OUR IMPROVED SCHEME
5.1 THE FIRST STAGE
We have improvement the Novikov-Kiselev scheme by taking into account the reflection attack. In our protocol we have two stages. In first stage user sends his ID and \( T_0 \) and sends to object \( O \) via secure channel. This processing is executed just once. ID and \( T_0 \) are produced and stored in the operative memory of O by \( U_i \). In second stage object identify the user \( U_i \). We have used the concept of random number in this stage.

5.2 THE SECOND STAGE
1) The user sends start request \( E_{PKO}(S, P_{KI}) \) to the object via public channel.
2) The object decrypts the message by using his private key \( S_{KO} \) and sends the following message to the user \( E_{PKU}(r) \).
3) Simultaneously, the object turns on the timer and record the start transmission time \( T_1 \).
4) In second stage object identify the user \( U_i \). Object computes a pair of session keys \((P_{KO}, S_{KO})\) and sends his public key \( P_{KO} \) via secure channel to \( U_i \).

5) The Intruder intercepts this message and \( S_{KI} \). Intruder can get the ID' and K. After that, Intruder can make whatever modification he wants.
6) Now Intruder decrypts this message with \( S_{KI} \). Intruder can get the ID' and K. After that, Intruder can make whatever modification he wants.

Here we observe that whole communication is open in front of Intruder and Intruder intercept in between the user and object and create illusion of object.
User Authentication From the Remote Autonomous Object

the object terminate the session. Otherwise, the object encrypts the message $M$ with the user’s public key $P_{KU}$ using the RSA algorithm, and then sends it to the user: $E_{P_{KU}}(M)$

5) When the user received the message from the object he decrypts it with his secret key $S_{KU}$. The user derives the command $K$ from $M$. User sends the following information: $E_{P_{KO}}(ID', K)$

![Figure 3: Our Proposed Scheme](image)

Now we see that in our protocol the intruder can’t intercept in any stage. Because the public key of object send to user via private channel and the request message and other conversation is done with encrypted form. User identification is done with the help of random number.

6. CONCLUSION

In this paper we have reviewed the the Novikov and Kislev’s scheme. We showed that the scheme is insecure against reflection attack. We also proposed a modification for authentication of the user from the Remote Autonomous Object.

ACKNOWLEDGEMENT

The authors thank Prof. Sunder Lal, Pro-Vice-Chancellor, Dr.B.R.Ambedkar University, Agra - 282002 (U.P) for his kind supervision of the work.

REFERENCES


