On the Authentication of the User from the Remote Autonomous Object

Amit K Awasthi

Pranveer Singh Institute of Technology
Kalpi Road, Bhauti, Kanpur, (UP) India (Email: awasthi_hcst@yahoo.com)

(Received May 28, 2005; revised and accepted June 1, 2005)

Abstract

In 2003, Novikov and Kislev proposed a scheme for an authentication of the user from the remote autonomous object. Recently Yang et al. pointed out an evidence of man-in-middle attack. In this paper we show another evidence of man-in-middle-attack. We also pointed out that reflection attack can also be framed successfully on the scheme.

Keywords: Authentication, cryptography, RSA, man-in-middle attack, reflection attack

1 Introduction

Novikov and Kislev [1] proposed a protocol (we call it NK protocol) for a user authentication from the remote autonomous object. They used public key infrastructure for this protocol. The design of the protocol is very week. Various attacks may be framed against this scheme. Recently one attack was proposed by Yang et al [2]. Here we also propose a different evidence of a man-in-middle-attack. Except this attack we also show that the reflection attack also works on the scheme.

2 Review of NK Protocol

This protocol runs in two stages as follows.

2.1 The First Stage

The user negotiates the identity ID and the time parameter T_0 with the remote object beforehand. The autonomous object stores these information in its operative memory. This is one time executable protocol.

2.2 The Second Stage

The steps of the second stage are shown in Figure 1.

1) The user sends start request S to the object. He uses public channel for this purpose.

2) The object uses RSA key generation algorithm. He computes (x_O, y_O) as private key and public key respectively. The object sends y_O to user and starts timer to note the time T_1

3) The user computes the encrypted message using public key y_O of object
$$E_{y_O}(ID, y_U),$$
where y_U is RSA public key of user and corresponding private key of user is x_U. User sends this encrypted message to the object.

4) The object stops timer, notes the time T_2 and decrypts the message
$$D_{x_O}(E_{y_O}(ID, y_U)) = (ID, y_U)$$

5) If $|T_2 - T_1| \leq T_0$ The object accepts the request otherwise rejects. If session is accepted, the object sends a message X after encrypt it with user's public key. i.e. it sends $E_{y_U}(X)$ to user.

6) When user receives the message from the object he decrypts it with his secret x_U. The user derives the command K from X. User sends the following information: $E_{y_O}(ID', K)$.

3 The Man-in-middle Attack

3.1 The First Stage

In the first stage user sends (ID, T_0) to the object. During this communication the intruder intercepts the information. Now he sends the tuple (ID, T_*) instead of the original (ID, T_0).

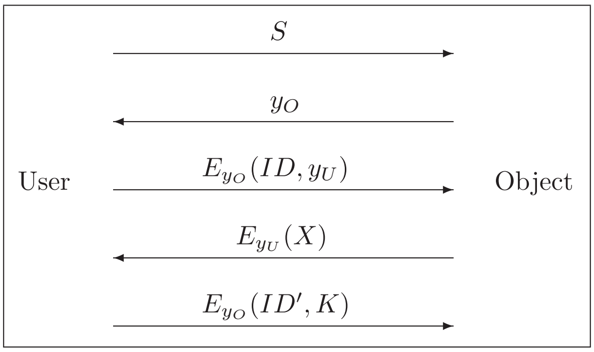

Figure 1: NK II Stage Protocol

3.2 The Second Stage

1) The user sends start request S to the object. He uses public channel for this purpose. Here intruder intercepts S. He send S to the object. If required he can modify S.

2) The object uses RSA key generation algorithm. He computes (x_O, y_O) as private key and public key respectively. The object sends y_O to user and starts timer to note the time T_1

3) The intruder intercepts the y_O. He sends self generated y'_O to the user.

4) The user computes the encrypted message using public key y'_O of object
$$E_{y'_O}(ID, y_U),$$
where y_U is RSA public key of user and corresponding private key of user is x_U. User sends this encrypted message to the object.

5) The intruder intercepts this encrypted message and decrypts it using x'_O. He modifies the the encrypted message as
$$E_{y_O}(ID, y'_O).$$

6) The object stops timer, notes the time T_2 and decrypts the message
$$D_{x_O}(E_{y_O}(ID, y'_O)) = (ID, y'_O).$$

7) If $|T_2 - T_1| \leq T_*$, the object accepts the request otherwise rejects. If session is accepted, the object sends a message X after encrypting it with user's public key. i.e. it sends $E_{y'_O}(X)$ to user.

8) The intruder intercepts this message and decrypts $E_{y'_O}(X)$ again. He encrypts X with y_U and sends to the user.

9) When user receives the message from the object he decrypts it with his secret x_U. The user derives the command K from X. User sends the following information
$$E_{y'_O}(ID', K).$$

10) Now intruder is again in between. He decrypts this incepted message and sends
$$E_{y_O}(ID', K).$$

Here we observer that whole communication is open in front of intruder. He can make the modification whatever he wants.

4 Reflection Attack

In previous section it is obvious that user is communicating all the messages with intruder not with object. Here it is again a chance that intruder can work as reflector. He can create illusion of object. To show this attack we can modify previous section protocol. Remove the role of object. Then protocol works as reflection attack.

5 Conclusion

In this paper we show that the Novikov and Kislev's scheme is insecure against man-in-middle attack and reflection attack.

References

[1] S. N. Novikov and A. A. Kislev, "The authentication of the user from the remote autonomous object," 4th Siberian Russian Workshop and Tutorial on Electron Device and Materials EDM, NSTU, Altai, Erlagol, 2003, Section II.

[2] C. Y. Yang, C. C. Lee and S. Y. Hsiao, "Man-in-middle-attack on the authentication of the user from the remote autonomous object," International Journal of Network Security, Vol 1, No 2, 81-83, 2005.

Amit K Awasthi received his M. Sc. Degree in 1999 from Bareilly College, (M. J. P. Rohilkhand University,) Bareilly. He is member of Indian Mathematical Society, Group for Cryptographic Research, Cryptography Research Society of India and Computer Society of India. His current research interests include data security and cryptography. His interests include Cryptology, Network Security, Smart cards.