# Man-in-the-Middle Attack on the Authentication of the User from the Remote Autonomous Object

Cheng-Ying Yang[1], Cheng-Chi Lee[2,3] and Shu-Yin Hsiao[4]

*(Corresponding author: Cheng-Ying Yang)*

Department of Computer Science and Information Engineering, National Formosa University[1],
64 Wen-Hwa Road, Hu-Wei, Yun-Lin , Taiwan 63208, R.O.C. (Email: cyang@cyut.edu.tw)
Department of Computer Science, National Chung Hsing University[2],
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.
Department of Computer & Communication Engineering, Taichung Healthcare and Management University[3],
500 Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan 413, R.O.C.
Graduate Institute of Networking and Communication Engineering, Chaoyang University of Technology[4],
168 Gifeng E. Rd., Wufeng Taichung County, Taiwan, R.O.C.

*(Received Feb. 20, 2005; revised and accepted March 17, 2005)*

## Abstract

In 2003, Novikov and Kiselev proposed an authentication of the user from the remote autonomous object. In this article, we shall show that the Novikov-Kiselev scheme cannot against a man-in-the-middle attack.

*Keywords: Authentication, cryptography, RSA, security*

## 1 Introduction

The authentication scheme is commonly used for verifying a user's identity. 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]. In Novikov-Kiselev scheme [6], they proposed the authentication of the user from the remote autonomous object with public key cryptosystem which is applicable in the telecommunications system.

In this article, we shall point out that the Novikov-Kiselev scheme cannot resist the man-in-the-middle attack; that is, the displacement of a user's identity by certain attacker.

## 2 Review of the Novikov and Kiselev Scheme

In this section, we will briefly review Novikov-Kiselev Scheme [6]. The scheme consists of two stages. The first stage is the one in which a user negotiates the identity with remote autonomous object before functioning as an object. When the user communicates with the object, the user's identify must be verified in the second stage.

***The first stage:***

The user negotiates the identity $ID$ and the time parameter $T_0$ with the remote object beforehand. And this step is executed just one time. The $ID$ and $T_0$ are stored in the operative memory of the object by the user.

***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 $PK_O$ and $SK_O$ by the RSA algorithm [7] and sends the public key $PK_O$ to the user. Note that $SK_O$ 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 $E_{PK_O}(ID,\ PK_U)$ to the object, where $E_A(M)$ is that message $M$ is encrypted by the public key $A$ using the encryption function $E(\cdot)$ of the RSA algorithm. The identity $ID$ and public key $PK_U$ are encrypted with $PK_O$ using the encryption function of the RSA algorithm. Note that the user also has a pair of keys $PK_U$ and $SK_U$ are generated by the RSA algorithm and $SK_U$ is kept securely by the user.

**Step 4:** The object decrypts the message $D_{SK_O}(E_{PK_O}(ID,\ PK_U)) = (ID,\ PK_U)$ with secure key $SK_O$ 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 $D(\cdot)$ of the RSA algorithm. $T_2$ is recorded simultaneously. If the difference in time $\Delta T$ between $T_1$ and $T_2$ is smaller than $T_0$ compared with the user's $ID$. Supposing $ID$ discord with user's $ID$ 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 $PK_U$ 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 $SK_U$ using the RSA algorithm. The user can derive the command $K$ from the message $X$ and encrypt the command $K$ and new identity $ID'$ with pubic key $PK_O$ 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 $SK_O$ after receiving the message from the user. The object executes the command $K$, if the difference in time $\Delta T$ 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.

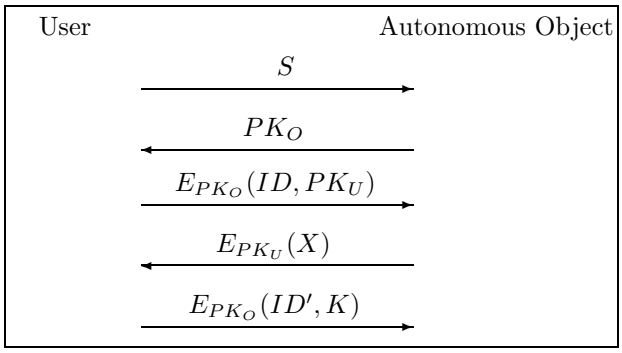


Figure 1: The procedures of the second stage

# 3 The Weakness of Novikov-Kiselev Scheme

In this section, we point out that the Novikov-Kiselev scheme cannot resist the man-in-the-middle attack. The adversary can replace the legal identity of that user. In the Novikov-Kiselev scheme, we assume there exists an adversary who attempts to become a legal user superseding the original user. WE show the man-in-the-middle attack on Novikov-Kiselev scheme in Figure 2. The procedures of that are stated as follows.

***In the second stage:***

**Step 1:** The user sends a start communication request $S$ to the object through the public communication channel. The attacker intercepts the message.

**Step 2:** When the object sends the public key $PK_O$ to the user, the attacker also intercepts the public key $PK_O$ from the public communication channel. Simultaneously, the object turns on the timer and records the start transmission time $T_1$.

**Step 3:** The user sends the encrypted message $E_{PK_O}(ID, PK_U)$ to the object.

**Step 4:** The object decrypts the message $(ID, PK_U)$ with the secure key $SK_O$. $T_2$ is recorded simultaneously. If the difference in time $\Delta T$ between $T_1$ and $T_2$ is smaller than $T_0$ compared with the user's $ID$. Supposing the $ID$ discords with user's $ID$ saved in memory of the object, then the object terminates the session. Otherwise, the object encrypt the message $X$ with the user's public key $PK_U$, and then sends it to the user.

**Step 5:** The attacker intercepts the message $E_{PK_O}(ID', K)$ from the user and then replaces it with $E_{PK_O}(ID", K')$ and sends it to the object. In general, command is formalize and the object is not a recheck command $K'$, which cause the attacker easily supersede the original user.

The object decrypt the message with the secure key $SK_O$ while receiving the message from the attacker. The identity $ID"$ is set in memory of the object which is not selected by the original user but by the adversary.

# 4 Conclusions

In this article, we have showed the weakness of Novikov-Kiselev scheme; that is, they cannot resist the man-in-the-middle attack.

# References

[1] M. S. Hwang, "A remote password authentication scheme based on the digital signature method," *International Journal of Computer Mathematics*, vol. 70, pp. 657–666, 1999.

[2] M. S. Hwang, C. C. Lee, and Y. L. Tang, "An improvement of SPLICE/AS in WIDE against guessing attack," *International Journal of Informatica*, vol. 12, no. 2, pp. 297–302, 2001.

[3] 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.

[4] C. C. Lee, M. S. Hwang, and W. P. Yang, "A flexible remote user authentication scheme using smart

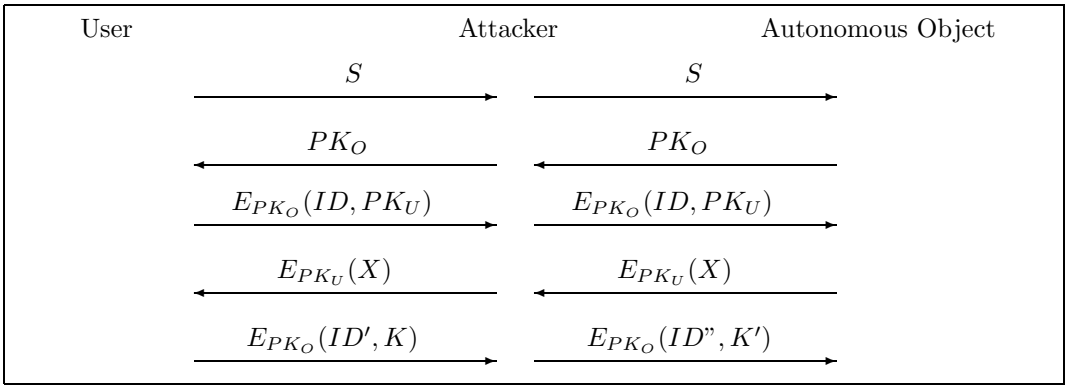


Figure 2: Man-in-the-middle attack on Novikov-Kiselev scheme

cards," *ACM Operating Systems Review*, vol. 36, no. 3, pp. 46–52, 2002.

[5] C. C. Lee, L. H. Li, and M. S. Hwang, "A remote user authentication scheme using hash functions," *ACM Operating Systems Review*, vol. 36, no. 4, pp. 23–29, 2002.

[6] Sergei N. Novikov and Anton A. Kiselev. "The authentication of the user from the remote autonomous object,". in *4th Siberian Russian Workshop and Tutorial on Electron Devices and Materials EDM*, Section II, NSTU, Altai, Erlagol, July 2003.

[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[8] Y. L. Tang, M. S. Hwang, and C. C. Lee, "A simple remote user authentication scheme," *Mathematical and Computer Modelling*, vol. 36, pp. 103–107, 2002.

**Cheng-Ying Yang** was born in Taipei on October 13, 1964. He received the M.S. degree in Electronic Engineering from Monmouth University, New Jersey, in 1991, and Ph.D. degree from the University of Toledo, Ohio, in 1999. He is a member of IEEE Satellite & Space Communication Society. Currently, he is employed as an Assistant Professor at National Formosa University, Taiwan. His research interests are performance analysis of digital communication systems, error control coding, signal processing and computer security.

**Cheng-Chi Lee** received the B.S. and M.S. in Information Management from the Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 1999 and in 2001. He researched in Computer and Information Science from the National Chiao Tung University (NCTU), Taiwan, Republic of China, from 2001 to 2003. He is currently pursuing his Ph.D. in Computer Science from National Chung Hsing University (NCHU), Taiwan, Republic of China. He is a Lecturer of Computer and Communication, Taichung Healthcare and Management University (THMU), from 2004. His current research interests include information security, cryptography, and mobile communications. Dr. Lee had published over 25 articles on the above research fields in international journals.

**Shu-Yin Hsiao** received the B.S. degree in Information Management and M.S. in Graduate Institute of Networking and Communication Engineering from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2002 and in 2004. Her current research interests include cryptography, information security, and network security.