LETTER

Robust Authentication Scheme between User and Remote Autonomous Object in Telecommunications System

Eun-Jun YOON[†a)], **Il-Soo JEON**[††b)], ***and*** **Kee-Young YOO**[†c)], ***Members***

SUMMARY Autonomous objects represent active database objects which can be distributed over the Internet. This paper proposes a robust authentication scheme for the remote autonomous object based on AES (Advanced Encryption Standard) symmetric cryptosystem. Compared with related schemes, the proposed scheme not only resists various security attacks but also provides computation and communication efficiency.

key words: *network security, autonomous system, cryptography, authentication, AES*

1. Introduction

In the telecommunications system environment, a remote autonomous object acts with its own thread of control. In general, the conduct of an autonomous object is defined by methods, rules and dynamic constraints [1], [2]. Therefore, it needs to communicate securely and authenticate between a user and the remote autonomous object [3]. The authentication scheme is commonly used to verify the identities of users. Remote access control is one of the important applications to ascertain whether the user is legal and whether he/she can access the remote resources.

In 2003, Novikov-Kiselev [4] proposed an authentication scheme of the user from the remote autonomous object with public key cryptosystem [5] which is applicable to perform secure authentication between the user and the remote autonomous object in the telecommunications system. However, Yang et al. [6] pointed out that the scheme is not secure against man-in-the-middle attack. That is, a certain attacker can displace a user's identity by performing the attack. Awasthi [7] also pointed out that the scheme is not secure against man-in-the-middle attack and reflection attack.

This paper proposes a new authentication scheme based on the AES symmetric cryptosystem to overcome such security problems of the Novikov-Kiselev scheme. We adopt time-stamp techniques to prevent the man-in-the-middle attack and the reflection attack. We also adopt the AES symmetric cryptosystem to provide computation efficiency. Moreover, the proposed scheme needs only three communication rounds. Therefore, it can reduce two communication rounds compared with Novikov-Kiselev's scheme. As a result, the proposed scheme resists various security attacks, while also providing computation and communication efficiency because it can be executed faster than Novikov-Kiselev's.

Manuscript received September 1, 2010.

Manuscript revised December 7, 2010.

[†]The authors are with the School of Electrical Engineering and Computer Science, Kyungpook National University, 1370 Sankyuk-Dong, Buk-Gu, Daegu 702–701, South Korea.

[††]The author is with the School of Electrical Engineering, Kumoh Institute of Technology, Sanho-ro 77 (Yangho-dong), Gumi, Gyeongbuk 730–701, South Korea.

a) E-mail: ejyoon@knu.ac.kr

b) E-mail: isjeon@kumoh.ac.kr

c) E-mail: yook@knu.ac.kr (Corresponding Author)

DOI: 10.1587/transinf.E94.D.1113

2. Telecommunications System Environment

The telecommunications system "User - remote object" is presented in Fig. 1. In the autonomous mode, the remote autonomous object operates with *j* data acquisition. After a while the user sends some certain message to the object, e.g., *c* command - "Go to the communication mode and transmit the *j* data collected". In such systems, it is necessary to authenticate the user from the remote autonomous object so as not to allow the malicious user to control the remote object using message *c*. Autonomous robotic devices such as a drilling machine [8], a pick and place robot [9] and an automated guided vehicle [10] are widely employed in manufacturing systems including this telecommunications system environment.

Security in the telecommunications system environment [11] is fundamentally about the provision of core security services, some of the most important of which are as follows. (1) The service confidentiality is about keeping data secret. (2) An integrity service prevents data from being altered in an unauthorized or unintended way. (3) Entity authentication (sometimes called identification) is the process whereby one entity is assured of the identity of another entity. (4) Data origin authentication is the assurance that data came from its reputed source. (5) Availability is the property of being accessible and useable upon demand by an authorized entity. At the heart of most security technologies is the deployment of specific cryptographic primitives, which are mathematical tools that can be applied to data to provide the core security services.

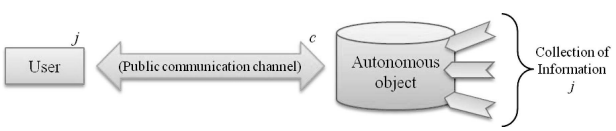

Fig. 1 The telecommunications system environment.

3. The Proposed Scheme

This section describes the proposed authentication scheme for remote autonomous objects. Throughout the paper, notations are employed in Table 1. The proposed scheme consists of two stages; registration stage and authentication stage.

3.1 Registration Stage

In the registration stage, a user negotiates the identity with remote autonomous object before functioning as an object. The following steps are executed just one time via a secure communication channel.

1. User → Autonomous Object: id

   The user sends its identity id to the remote autonomous object. Then, the id is securely stored in the operative memory of the remote autonomous object by the user.

2. Autonomous Object → User: k

   The remote autonomous object generates a secret key k by the AES algorithm, and then sends it to the user. Note that k is kept securely by both the remote object and the user.

3.2 Authentication Stage

When the user communicates with the remote autonomous object, the user's identity id must be verified in this stage. The procedures of the proposed authentication stage are shown in Fig. 2.

1. User → Autonomous Object: $\mathcal{E}_k(id||ok||t_1)$

   The user generates a one-time secret key ok and makes an encrypted message $\mathcal{E}_k(id||ok||t_1)$ with the shared secret key k. Note that t_1 is the current date and time of the user. Finally, the user sends the encrypted message $\mathcal{E}_k(id||ok||t_1)$ to the autonomous object as a start communication request through the public communication channel.

Table 1 Notation used in scheme.

id	The identity of the user.
k	The secret key of autonomous object.
ok	The one-time secret key of the user.
x	The message which includes the command C.
c	The user selected control command.
$\mathcal{E}(\cdot)$	The encryption function of AES algorithm.
$\mathcal{D}(\cdot)$	The decryption function of AES algorithm.
t_i	The current date and time parameter.
$\oplus$	A bit-wise exclusive-or operation.
$\|\|$	A message concatenation operation.
$A \rightarrow B : M$	A sends the message M to B.

2. Autonomous Object → User: $ok \oplus (id||x)$

   The autonomous object decrypts the received message $\mathcal{E}_k(id||ok||t_1)$ with the shared secret key k using the decryption function of the AES algorithm as follows:

   $$(id||ok||t_1) \leftarrow \mathcal{D}_k(\mathcal{E}_k(id||ok||t_1)) \quad (1)$$

   The autonomous object checks the time interval between t_1 and t_2, where t_2 is the timestamp of message receiving. If $(t_2 - t_1) \geq \Delta t$, where Δt is the expected legal time interval for transmission delay, then the autonomous object terminates the current session. Otherwise, the autonomous object checks the validity of the user's id by using the user's id saved in memory of the object. If they differ, then the autonomous object terminates the current session. Otherwise, the autonomous object concatenates id and the message x which includes the command C, and then encrypts the message $id||x$ with the user's one-time secret key ok as $ok \oplus (id||x)$. Here, if the size of ok is different from that of $(id||x)$, a message padding algorithm can be applied to make it equal in size. Finally, the autonomous object sends it to the user.

3. User → Autonomous Object: $\mathcal{E}_{ok}(id \oplus c||id'||c||t_3)$

   When the user receives the message $ok \oplus (id||x)$ from the autonomous object, the user decrypts it with its one-time secret key ok as follows:

   $$(id||x) \leftarrow (ok \oplus (id||x)) \oplus ok \quad (2)$$

   The user verifies the legality of the received identity id.

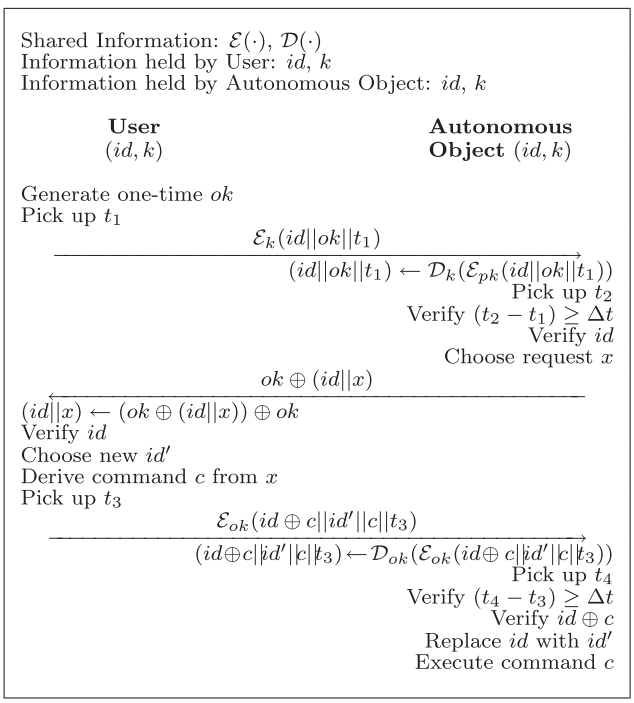

Fig. 2 The proposed authentication stage.

If it holds, the user derives the command c based on the message x, and encrypts the authentication token $id \oplus ok$, new identity id', the command c and the timestamp t_3 with the one-time secret key ok of autonomous object using the AES algorithm. Finally, the encrypted message $\mathcal{E}_{ok}(id \oplus c||id'||c||t_3)$ is sent to the autonomous object.

4. The autonomous object decrypts the received message $\mathcal{E}_{ok}(id \oplus c||id'||c||t_3)$ with the one-time secret key ok using the decryption function of the AES algorithm as follows:

$$(id \oplus c||id'||c||t_3) \leftarrow \mathcal{D}_{ok}(\mathcal{E}_{ok}(id \oplus c||id'||c||t_3)) \quad (3)$$

The autonomous object checks the time interval between t_3 and t_4, where t_4 is the timestamp of message receiving, and verifies the legality of the received authentication token $id \oplus c$. If they hold, the autonomous object records in its memory the value of the new id' and executes the command c. Otherwise, the autonomous object terminates the current session.

4. Security and Efficiency Analysis

This section provides the security analysis of the proposed authentication scheme.

4.1 Security Analysis

A useful method of proofing the security of the proposed scheme is in terms of passive attacks and active attacks [12].

Definition 1 (Strong secret key): A strong secret (k and ok) is a value of high entropy, which cannot be guessed in a reasonable polynomial time.

Definition 2 (Passive attacks): Passive attacks attempt to learn or make use of information from the user or object but does not affect their resources.

Definition 3 (Active attacks): Active attacks attempt to alter communication resources or affect their operation.

Under the above definitions, the following theorems are used to analyze nine security properties in the proposed scheme.

Theorem 1 (Passive attacks): The proposed scheme can resist passive attacks.

Proof 1: If an adversary who eavesdrops on a successful proposed scheme run can make a guess at the one-time secret key ok by using only information obtainable over a network and a guessed value of the user's identity id, the adversary could break the AES symmetric key cryptosystem. The reason will be clear. Such the AES symmetric key cryptosystem problem can be reduced to get id and ok from the messages $\mathcal{E}_k(id||ok||t_1)$, $ok \oplus (id||x)$, and $\mathcal{E}_{ok}(id \oplus c||id'||c||t_3)$ in the proposed scheme. Without the ability to decrypt the keying material k, the messages $\mathcal{E}_k(id||ok||t_1)$, $ok \oplus (id||x)$, and $\mathcal{E}_{ok}(id \oplus c||id'||c||t_3)$ do not leak any information to the passive adversary. Since the user and the object do not leak any information either, the proposed scheme can resist passive attacks.

Theorem 2 (Active attacks): The proposed scheme can resist active attacks.

Proof 2: Active attacks can take many different forms, depending on what information is available to the adversary. For the replay attacks, neither the replay of user's messages $\mathcal{E}_k(id||ok||t_1)$ and $\mathcal{E}_{ok}(id \oplus c||id'||c||t_3)$ in steps 1 and 3 of the authentication stage nor the replay of the autonomous object's response message $ok \oplus (id||x)$ in step 2 of the authentication stage will work, as it will fail in steps 2 and 4 of the authentication stage due to the time interval $(t_2 - t_1) \geq \Delta t$ and $(t_4 - t_3) \geq \Delta t$, respectively. Therefore, the proposed scheme can resist replay attack. A man-in-the middle attack, which requires an adversary to fool both sides of a legitimate conversation, cannot be carried out by an adversary who does not know the shared long-term secret key k between the user and the autonomous object. In the proposed authentication scheme, an adversary can attempt to modify a message $\mathcal{E}_k(id||ok||t_1)$ into $\mathcal{E}_k(id_{\mathcal{A}}||ok_{\mathcal{A}}||t_{\mathcal{A}})$, where $id_{\mathcal{A}}$ is the adversary's identity, $ok_{\mathcal{A}}$ is the adversary's one-time secret key, and $t_{\mathcal{A}}$ is the adversary's current date and time, so as to succeed in step 2 of the authentication stage. However, such a modification will fail in step 2 of the authentication stage, because an adversary has no way of obtaining the identity id of the user to compute the valid message $\mathcal{E}_k(id||ok_{\mathcal{A}}||t_1)$. In the proposed scheme, we can see that id of the user is acting like another secret key of the user. In addition, the object always verifies the legality of the received identity id. Since the user also always verifies the legality of the identity id from the received $ok \oplus (id||x)$. Without knowing the one-time secret key ok of the user, an adversary also cannot impersonate the legal object. If the adversary wants to get the one-time secret key ok, he/she has to decrypt $\mathcal{E}_k(id||ok||t_1)$. However, it is impossible because he/she does not have the secret key k. Therefore, the proposed scheme can resist impersonation attacks including Yang et al.'s [6] and Awasthi's [7] man-in-the-middle attacks and reflection attack. As a result, the proposed scheme can resist active attacks.

4.2 Efficiency Analysis

The computation costs of the proposed scheme and Novikov-Kiselev scheme [4] are summarized in Table 2. Novikov-Kiselev scheme requires a total of three RSA encryptions, three RSA decryptions, and five communication rounds. However, the proposed scheme requires a total of two AES encryptions, two AES decryptions, and two bit-wise exclusive-or operations, and three communication rounds. Since the AES symmetric encryption/decryption computations are much faster than the RSA asymmetric encryption/decryption computations, the proposed scheme can

Table 2 Comparison of computational costs.

	Novikov-Kiselev scheme	Proposed scheme
# of RSA encryptions	3	0
# of RSA decryptions	3	0
# of AES encryptions	0	2
# of AES decryptions	0	2
# of exclusive-ors	0	2
# of communication rounds	5	3

be performed more computational and communicational efficiently than the Novikov-Kiselev's scheme.

5. Conclusions

This paper proposed a new authentication scheme of the user from the remote autonomous object that overcomes the weaknesses of the Novikov-Kiselev scheme. The proposed scheme is based on the AES symmetric cryptosystem to provide better computational efficiency than that of the Novikov-Kiselev scheme. Moreover, the proposed scheme requires three communication rounds. As a result, the proposed authentication scheme resists various security attacks, while also providing more efficiency because it can be executed faster than Novikov-Kiselev scheme.

Acknowledgment

We would like to thank the anonymous reviewers for their helpful comments. This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2011-(C1090-1121-0002)).

References

[1] A. Kemper, P.C. Lockeman, G. Moerkotte, and H.D. Walter, "Autonomous objects: A natural model for complex applications," J. Intelligent Information Systems, vol.3, no.2, pp.133–150, 1994.

[2] N. Krivokapic, S. Grieser, M. Islinger, M. Keidl, S. Prols, S. Seeltzam, and A. Kemper, "AutO: A distributed system of autonomous objects," Technical Report, University Passau, Germany, 1996.

[3] E. Gudes and A. Tubman, "AutoWF-A secure Web workflow system using autonomous objects," Data & Knowledge Engineering, vol.43, no.1, pp.1–27, 2002.

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

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

[6] 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, pp.81–83, 2005.

[7] A.K. Awasthi, "On the authentication of the user from the remote autonomous object," International Journal of Network Security, vol.1, no.3, pp.166–167, 2005.

[8] G.C. Onwubolu, S. Aborhey, R. Singh, M. Prasad, H. Reddy, S. Kumar, and S. Singh, "Development of a pc-based computer numerical control drilling machine," Proc. Institution of Mechanical Engineers, Part B: J. Engineering Manufacture, vol.216, no.B11, pp.1509–1515, 2002.

[9] R.V. Sharan and G.C. Onwubolu, "Development of a vision-based pick-and-place robot," Proc. International Conference on Autonomous Robots and Agents, pp.473–478, 2006.

[10] R. Singh and G.C. Onwubolu, "An integrated design towards the implementation of an automatic guided vehicle," Proc. International Conference on Computational Intelligence, Robotics and Autonomous Systems, 2005.

[11] F. Higgins, A. Tomlinson, and K. Martin, "Survey on security challenges for swarm robotics," ICAS 2009, pp.307–312, 2009.

[12] E. Gelbstein and A. Kamal, "Information insecurity: A survival guide to the uncharted territories of cyber-threats and cybersecurity," ICT Task Force Series, 2nd edition, United Nations, 2005.