An Authentication Protocol for Multicast Communications*

Min-Shiang Hwang† Wei-Pang Yang‡

Graduate Institute of Networking and Communication Engineering†
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: mshwang@cyut.edu.tw
Fax: 886-4-23305539

Department of Computer and Information Science‡
National Chiao-Tung University
1001 Ta Hsueh Road,
Hsinchu, Taiwan, R.O.C.

November 5, 2002

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC91-2213-E-324-003.

An Authentication Protocol for Multicast Communications

Abstract

Providing security for electronic documents is an important issue. Particularly when a message must be delivered to more than one destination and authentication is required. In this study, this problem is solved using a group authentication detection method. Each recipient is not required to authenticate the documents. In contrast, the sender authenticates these documents whenever all recipients have received them.

Keywords: Authentication, Cryptography, Electronic Document, Security.

1 Introduction

Computer networks allow rapid and convenient communication. Therefore, computer networks have become the principal media for the distribution of information.

Value added networks provide a set of services via computer networks. The services include electronic mail, file transfer, electronic newspapers, and electronic data interchange. However, these services via computer networks are vulnerable to relatively easy access by third parties [3]. Without appropriate protection, these services are susceptible to unauthorized access [6]. Therefore, cryptosystems are deemed necessary for authorizing users as well as protecting the privacy of the service.

In modern computer systems, how to authenticate electronic document delivery over an insecure communication channel is a relevant concern in the field of computer security.

Three conventional approaches to securing electronic document delivery are 1988 CCITT X.411 Recommendation, a number of "Request For Comments (RFC)" documents, and Message Security Protocol [4]. The 1988 CCITT X.411 Recommendation provides security for message contents. RFC series provides security enhancements for SMTP-based messaging systems. In the X.400 model, the RFC approach provides security for body parts. The Message Security Protocol is a hybrid of the two above approaches.

The case next considered involves a message is designed to be sent from Taiwan to m recipients ($m \geq 2$) in USA. The message, when being sent, can only be replicated so that a single message is made into m copies after it has crossed the Pacific. In that process, the transmission time is reduced to $1/m$ times [9, 10, 11].

Providing security for electronic documents delivered to more than one destination is an important issue, particularly when authentication is required. In this study, this problem is solved using the group authentication detection method. Each recipient is not required to authenticate the documents. In contrast, the sender authenticates those documents whenever all recipients have received them.

The rest of this paper is organized as follows. The secret key distribution is discussed in the next section. Our new authentication method is presented in Section 3. Next, a discussion of performance and security analysis is performed in Section 4. Concluding remarks are made in the last section.

2 Secret Key Distributions

In 1976, Diffie and Hellman proposed a simple but effective key distribution scheme for distributing a secret common key [2]. Two users thus use the common secret key (also termed session key) to communicate with each other in a secure manner over insecure channels. In 1982, Ingemarsson et al. generalized the key distribution scheme [5] which is referred to as the conference key distribution scheme (CKDS). In CKDS, a group (two or more) of participants can generate a common secret key over the public channel to hold a secure conference.

Since 1987, a number of studies have been carried out concerning conference key distribution systems [1, 7, 8]. Koyama and Ohta proposed identity-based conference key distribution schemes with authentication in three configurations, i.e., ring network, complete graph network, and star network [7]. Two investigations have proposed schemes for broadcasting secret messages in both complete graph and star network. One is in which Chiou and Chen proposed a method based on the Chinese remainder theorem [1]. The other is Laih et al.'s scheme which is based on cross production [8].

The above key distribution schemes can be used in our authenticating multicast electronic documents scheme.

3 A New Authentication Protocol

In this section, we present an authenticating multicast electronic documents scheme. The scheme is that the original sender enciphers the signature of the message under the session keys with recipients in sequence. A detailed discussion of the session key scheme is provided in Section 2. All recipients, when receiving the ciphertext, decipher it under their session key. The last recipient checks the integrity using his session key.

When a message is sent from user U_1 to user $U_j, j = 2, \cdots, m$ in a secure manner, the following procedure is followed. A conventional cryptosystem, e.g., DES, is assumed to be available. Let E be an enciphering procedure, D be a deciphering procedure for the available cryptosystem, and let M be a message which is sent to all recipients. This new authentication schemes can be divided into two phases, i.e., the initialization phase and the authentication phase.

Authentication Protocol:

Before transmitting messages in the system, the sender encrypts the signature of the messages in sequence under the session keys between the sender and the recipients in the initialization phase.

Initialization phase:

Step 1:

Compute message authentication code (M') by $f(M)$, where f is a one-way function [12].

Step 2:

Compute $C'_2 = E_{K_{12}}(M')$, where K_{12} is a session key between the sender U_1 and the recipient U_2.

Step j $(j = 3, 4, \cdots, m)$**:**

Compute $C'_j = E_{K_{1j}}(C'_{j-1} \oplus M')$, where K_{1j} is a session key between the sender U_1 and the recipients U_j; the operator "$\oplus$" denotes an exclusion OR operation. The original sender sends (C'_m, M) to the recipient U_m.

Authentication phase:

When the target's recipient U_m receives the message (C'_m, M), the following procedure is followed.

Step 1:

The recipient U_m deciphers C'_m under the session key between U_1 and U_m as follows.

$$\begin{aligned} C_m &= D_{K_{1m}}(C'_m) \\ &= D_{K_{1m}}(E_{K_{1m}}(C'_{m-1} \oplus M')) \\ &= C'_{m-1} \oplus M'. \end{aligned}$$

U_m computes message authentication code (M') by $f(M)$ and obtains C'_{m-1} as follows.

$$\begin{aligned} & C_m \oplus M' \\ = \;& (C'_{m-1} \oplus M') \oplus M' \\ = \;& C'_{m-1}. \end{aligned}$$

U_m sends (C'_{m-1}, M) to U_{m-1}.

Step j $(j = 2, 3, \cdots, m-2)$**:**

The recipient U_{m-j+1} deciphers C'_{m-j+1} under the session key between U_1 and U_{m-j+1} as follows.

$$\begin{aligned} C_{m-j+1} &= D_{K_{1(m-j+1)}}(C'_{m-j+1}) \\ &= D_{K_{1(m-j+1)}}(E_{K_{1(m-j+1)}}(C'_{m-j} \oplus M')) \\ &= C'_{m-j} \oplus M'. \end{aligned}$$

U_{m-j+1} computes message authentication code (M') by $f(M)$ and obtains C'_{m-j} as follows.

$$\begin{aligned} & C_{m-j+1} \oplus M' \\ = \;& (C'_{m-j} \oplus M') \oplus M' \\ = \;& C'_{m-j}. \end{aligned}$$

U_{m-j+1} sends (C'_{m-j}, M) to U_{m-j}.

Step $(m-1)$**:**

In Step $(m-2)$, U_3 sends (C'_2, M) to U_2. U_2 deciphers C'_2 under the session key between U_1 and U_2 as follows.

$$\begin{aligned} C_2 &= D_{K_{12}}(C'_2) \\ &= D_{K_{12}}(E_{K_{12}}(M')) \\ &= M'. \end{aligned}$$

U_2 computes message authentication code (M') by $f(M)$ and checks whether or not $C_2 \oplus M' = 0$. If true, the message M is definitely sent by the sender U_1. Otherwise, the message is a fake. U_2 must to send a notification to all target' recipients to discard the message.

4 Discussions

The security of our scheme is based on the symmetric cryptosystems and the one-way functions. Asymmetric cryptosystems [2] could also be used in our scheme. The security in our proposed scheme is assumed to be assured, since any symmetrical cryptosystem can be applied to it.

A well-known one-way function f for encoding the message is used here as the message authentication code in our scheme. The practical importance of such a function has been known for some time, and researchers have used them in a number of schemes [12]. It is difficult for an intruder to obtain M, M'', and M' such that $f(M) = f(M'') = M'$.

We now examine the complexity of my proposed protocol and a straightforward protocol. We assume that a sender wants to send a message from Taiwan to m recipients ($m \geq 2$) in USA. In a straightforward method, the message must be replicated to m copies. The sender need to compute message authentication code (MAC) and encryption in m times for these m copies before it has crossed the Pacific. In the straightforward protocol, the transmission data between Taiwan and USA is m copies messages and MACs. In my protocol, the sender needs to compute m MACs, encryption, and exclusion OR operations. The time complexity of my protocol is more m exclusion OR operations than that of the straightforward protocol. In general, we can ignore the exclusion OR operation since it spends less than 1 micro second. In my protocol, the transmission data between Taiwan and USA is one copy message and MAC. The transmission time of my protocol is reduced to $1/m$ times than that of the straightforward protocol.

5 Conclusions

A scheme for authenticating multicast electronic documents over a public insecure channel has been proposed in this study. Based on the group authentication detection method, only a single authenticated message can be sent to all recipients. Each recipient is not required to authenticate the documents. In contrast, the sender authenticates those documents whenever all recipients have received them.

References

[1] G. H. Chiou and W. T. Chen. Secure broadcasting using the secret lock. *IEEE Transactions on Software Engineering*, 15(8):929–934, August 1989.

[2] W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22:644–654, 1976.

[3] S. Robin Hall and David P. Maher. Closing in on wireless privacy. *AT& T Technology*, 8(3):22–25, 1993.

[4] Russell Housley. Electronic messaging security: A comparison of three approaches. In *Proceedings of the Fifth Annual Computer Security Applications Conference*, page 29, 1990.

[5] I. Ingemarsson, D. T. Tang, and C. K. Wong. A conference key distribution system. *IEEE Transactions on Information Theory*, IT-28(5):714–720, September 1982.

[6] Borka Jerman-Blazic. Security in value added networks - security requirements for EDI. *Computer Standard & Interfaces*, 12:23–33, 1991.

[7] K. Koyama. Secure conference key distribution systems for conspiracy attack. In *Advances in Cryptology, EUROCRYPT'92*, pages 449–453, Lecture Notes in Computer Science, 1992.

[8] C. S. Laih, L. Harn, and J. Y. Lee. A new threshold scheme and its applications on designing the conference key distribution cryptosystem. *Information Processing Letters*, 32(3):95–99, 1989.

[9] Chris J. Mitchell. Multi-destination secure electronic mail. *The Computer Journal*, 32(1):13–15, 1989.

[10] Chris J. Mitchell. Authenticating multicast internet electronic mail messages using a bidirectional MAC is insecure. *IEEE Transactions on Computers*, 41(4):505–507, April 1992.

[11] Chris J. Mitchell and Michael Walker. Solutions to the multidestination secure electronic mail problem. *Computer & Security*, 7(5):483–488, 1988.

[12] J. Rompel. One-Way Functions are Necessary and Sufficient for Secure Signatures. In *Proc. of the 22nd STOC*, pages 387–394, 1990.