Multilevel Encryption for Classified Multimedia Applications in MPEG-7

Zheng Xiaojian
Faculty of Software
Fujian Normal University
Minhou Section, 350108, China
zxiaojian@126.com

***Abstract*—In order to address the security issues of the classified multimedia contents, a multilevel encryption scheme is presented which support multilevel encryption by introducing the time seed which used for generating time master key and then further generating encryption key. This scheme takes advantage of the properties of MPEG-7 standard to generate the multimedia hierarchy organized into tree structure involving many elements each of which belongs to a security clearance level, the sensitive element or security content can be encrypted with proper key in term of security level and then the entire multimedia encrypted with another appropriate key and the multilevel encryption achieved.**

Keywords-Classified Multimedia, Multilevel Encryption Scheme, Security Clearance, MPEG-7

I. INTRODUCTION

Multimedia applications have become increasingly popular and prevalent in recent years. The classified multimedia applications are multimedia applications involving some sensitive information or security information about Government or Enterprise which cover more and more application domains, including Digital libraries, E-Commerce, Home entertainment, News programs, and Multimedia editing [1], especially E-health contains privacy information of patients. The tremendous growth of the amount of classified multimedia content requires appropriate methods and strategies to describe and manage the classified multi- media content efficiently and securely. The multimedia standard MPEG-7[2,3,4] is to satisfy the requirements of effectively describing multimedia contents.

However, the security requirements of multimedia contents, especially multilevel encryption according to different security clearance [6], are left open in present MPEG-7 standard. The description tools provided in MPEG-7 do not include the mechanism of multilevel encryption, therefore, there is a need to develop security mechanisms that perform multilevel encryption and exploit and extend MPEG-7 Description Tools in order to provide protection for multimedia contents.

Several characters of the classified multimedia contents could cause some specific security requirements. Multimedia contents usually contain a huge number of elements, some of which may have different security levels. Therefore, the performance of multilevel encryption to those elements should be according to the security level of each element, the multilevel encryption mechanism should take into account and make full use of the properties of MPEG-7.

In order to handle these requirements, we propose a multilevel encryption scheme that enhanced the existing encryption methods. After this introduction, Section 2 introduces MPEG-7 briefly. The proposed multilevel encryption scheme is discussed in detail in Section 3. Section 4 provides simple security analysis. The conclusions are given in Section 5.

II. INTRODUCTION OF MPEG-7 STANDARD

The MPEG-7 standard provides tools for effectively and efficiently describing the multimedia contents [1,5]. The classified multimedia is a multimedia that involving some sensitive contents or security information, therefore, the classified multimedia contents could also be described by MPEG-7 standard tools: Descriptors (Ds), Description Schemes (DSs), and Description Definition Language (DDL) are three main components of the standard.

Two MPEG-7 properties lay the foundation of our multilevel encryption scheme. First, our scheme benefits from the segment description in MPEG-7 can be decomposed and organized into a tree structure. The decomposition function allow us decompose the classified multimedia contents into multi elements and organized into a tree structure and each of which has their own security level.

Another character facilitates our multilevel encryption scheme is the extensibility of the Description Schema in MPEG-7. The allowed extension allows us to create a new Description Schema or modify the existing ones which more kinds of classified multimedia objects of different security levels could be described and thus our multilevel encryption scheme can be achieved.

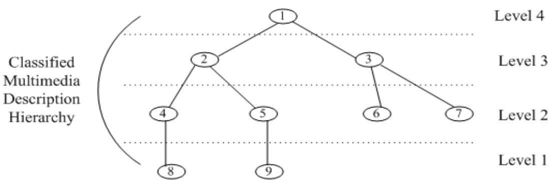

Figure 1. Classified multimedia description hierarchy

In MPEG-7, each of the classified multimedia can be described into tree structure and the description hierarchy showed as Figure 1. Node 1 represents the classified multimedia and decomposed into node 2 and node 3, and so on. If node 9 contains sensitive information, we use appropriate key in terms of the security clearance level to encrypt and then use another key with the corresponding

Published by Atlantis Press, Paris, France.

security clearance level to encrypt the entire classified multimedia.

III. Multilevel Encryption Scheme

A. Background

Normally, the multimedia information and the corresponding users can be classified into four multi security level in terms of security clearance which is a status granted to individuals allowing them access to classified information from lower to top as Follows [6]:

Top Secret: This is a more stringent clearance which affords one access to data that affects national security, enterprise security. Secret: This level of clearance acquire the valid users must be department managers who need to know the secret multimedia information. Confidential: This level of clearance will grant the right to access designated and classified information on a need-to-know basis. The valid users with the corresponding duty can access this level of multimedia information. Reliability: This level of information can be authorized to valid users who passed the reliability checks which are done by verifying personal data, educational, professional qualifications, a fingerprint check, and a credit check.

Multilevel encryption scheme is acquired in order to protect the security of the multilevel multimedia information according with multi security clearance. In conventional practice, forward secrecy ensures that the past multimedia information are protected even if the current secret key is exposed [7], and backward secrecy means that the exposed secret key is no longer useful in the future [8].

B. Notation

The proposed model is an extension of the MLE scheme [8]. The components of the items in [8] are enhanced in order to handle the multilevel encryption for classified multimedia as follows.

MK : Master key, which hold by security server. MC_i : Plaintext of leveled classified Multimedia Content i . C_i : Cipher text of corresponding MC_i . CC_i : The Composite Characteristics of node i , the result of Boolean expression $OS_i \oplus AS_i \oplus MAC_i \oplus IP_i \oplus PN_i$ which the items is composed of the terminal node's platform of software, operation system OS and application software AS , and platform of hardware, the MAC address MAC, IP address IP , and port number of the network access switch PN .

$SUID_i$: It is composed of the identity of secure user ID_i and his or her fingerprint information FP_i and corresponding environment characteristics CC_i by $ID_i \oplus FP_i \oplus CC_i$. UK_i : User key for secure user i . K_{D_i} : Department Key (ex. K_{D_1} for Department D_1 , that is Department 1). $Enc(K, MC)$: Encrypt Multi- media Content MC using key K . $\{MC\}_K$: Encrypted Multimedia Content MC by key K . $H^n(MC)$: Hash n times of Multimedia Content MC . $H(MC_i, MC_j)$: Hash of MC_i concatenates MC_j . KB_{CC_i, L_n} : Base key for level n of terminal node CC_i . KE_{CC_i, L_n, T_j} : Encryption Key for level n of terminal node CC_i , during time period T_j . T_i : The i th Time period. TMK_{CC_i} : Time Master Key for terminal node CC_i . TK_{CC_i, T_j} : Time Key for terminal node CC_i , during time period T_j .

In order to understand our multilevel encryption scheme more precisely, there are some important terms should be described as follows:

Secure server: It is responsible for generating and holding the master key MK , and periodically broadcasts Time seed Key to terminal nodes of every department and manage time master key. In addition to this, server is also responsible for authenticating the secure user's identity.

Secure user: Individuals can be identified as valid users who must be a regular employee of the Government or Enterprise and registry his or her identity information into the secure server which contains their computer's platform of software and hardware. In addition to this, it must be contain their registered ID and fingerprint information. Valid users can be identified as secure users who must be passed the authentication by the secure server.

Secure permission: Secure users can be classified into four categories in terms of the security clearance: the first categories is Administrators who have the secure permission of Top Secret level, and Managers have the Secret level, and Officeholders have the Confidential level, and general Employees have Reliability level respectively.

Department: Each of the level of the users belong to a department, therefore, a Government or Enterprise can be divided into department 1, 2, 3 and 4 according to the level of security clearance.

Secure object: It is the classified multimedia content composed of some secure sub object each of which belongs to a specific security level.

C. Multilevel Encryption Scheme

The multilevel encryption scheme requires the secure server to hold one master key MK . The secure server randomly generates K_{D_1} for the Department 1 and computes K_{D_2} , K_{D_2} by performing one-way Hash function, and then gives these keys to D_1 , D_2 , and D_3 secure users respectively[8].

The classified multimedia data is time sensitive which in different time period may be has different security clearance, therefore, we can use the term time as our consideration of encryption key.

The secure server periodically broadcasts $seedT_i$ to terminal nodes of department, the value of $seedT_i$ could be a computational result of time period T_i using the expression $seedT_i = Enc(MK, T_i)$ where encrypt algorithm could be symmetric encryption or asymmetric encryption. $seedT_i$ are used to update encryption keys. Since these $seedT_i$ values were broadcasted to terminal nodes of department, they could be captured and recorded by adversary thus endanger the system. In order to solve this problem, the secure server gives each terminal mode of department an unique time master key TMK_{CC_i} through expression $TMK_{CC_i} = Enc(MK, CC_i)$ where encrypt algorithm could be symmetric encryption or asymmetric encryption too. TMK_{CC_i} are used to generate time keys $TK_{CC_i,T_j} = Enc(TMK_{CC_i}, seedT_j)$ where encrypt algorithm could be symmetric encryption or asymmetric encryption too, and the time keys are aimed to update encryption keys for each secret level through Hash function $KE_{CC_i,L_n,T_j} = H(KB_{CC_i,L_n}, H^{L_{n-1}}(TK_{CC_i,T_j}))$. Because of performing this one-way Hash algorithm in each security level of the classified multimedia, the colluding attack could be prevented in our scheme.

The secure server gives each terminal node of department a different key set which is recognized as base key KB_{CC_i,L_n} where the subscript CC_i represents that this key belongs to this terminal node of department and L_n represents the security clearance level of the key. Composing base keys KB_{CC_i,L_n} and time keys TK_{CC_i,T_j} values we will obtain encryption keys of the secure object by the expression $KE_{CC_i,L_n,T_j} = Enc(KB_{CC_i,L_n}, TK_{CC_i,T_j})$ where encrypt algorithm could be symmetric encryption or asymmetric encryption too.

Because of the encryption key is the encrypted combination of the base key and the time key, the forward secrecy and backward secrecy can be obtained through this key-insulated method.

As described in literature [4], in our multilevel encryption scheme we also give each secure user a user key UK_i by the expression function $UK_i = Enc(MK, SUID_i)$, these user keys can be used to perform user identity authentication and encrypt time key TK_{CC_i,T_j} before sending to users.

D. Secure User Identity Authentication

Secure user identity authentication is very important in our multilevel encryption scheme, only the valid user of department can have the chance to get in touch with the terminal node of department such as computer or workstation. Valid users summit the authentication information to secure server to perform the process of identity authentication, which must be contain their registered ID, fingerprint information and environment information such as their computer's platform of software, operation system and application software, and platform of hardware, the MAC address, IP address, and port number of the network access switch. Valid users can be identified as secure users who must be passed the identity authentication by the secure server. Only the secure users can obtain the user key used to encrypt and decrypt the secure object.

IV. Security Analysis

There are many known attack methods in multimedia application, including Denial-of-Service, traffic analysis, eavesdropping and so on [8]. We concentrate on the security of our multilevel encryption scheme for classified multimedia, there may be some possible attack methods such as eavesdropping and colluding attack to our proposed scheme and we analyze and evaluate the security here.

Eavesdropping: In our multilevel encryption scheme for classified multimedia, adversaries can only obtain the available information is time seed $seedT_i$ value, but without the time master key TMK_{CC_i}, the $seedT_i$ value is useless because only this value can not generate TK_{CC_i,T_j} by the expression function $TK_{CC_i,T_j} = Enc(TMK_{CC_i}, seedT_j)$. Therefore, our scheme has the ability to resist the eavesdropping attack.

Impersonation Attack: From the process of secure user identity authentication we know that only the valid user can have the chance to get in touch with the terminal computer or workstation. Valid users can be identified as secure users who must be passed the identity authentication by the secure server. Only the secure users can obtain the user key used to decrypt the secure object. If a adversary has the chance to get in touch with the terminal computer in some circumstance and obtain the valid user's ID information, he or she can not pass the identity authentication because the fingerprint information of valid user can not be got by adversary. Therefore, our scheme has the ability to resist the impersonation attack.

Colluding Attack: If a secure user in lower privileged level collude with a secure user in higher privileged level, although she can get the department key of higher level, after passed the identity authentication, the secure server will only give the time key of corresponding privileged level to her. Without time keys of higher level, the user cannot derive specific encryption keys to obtain the secure object.

V. Conclusion

This paper presents a multilevel encryption scheme which is enhanced the method in literature [8] and support multilevel encryption by introducing the secure user who must be the valid user and passed the identity authentication, secure server which is responsible for key management and identity authentication, secure object involving sensitive or privacy information of classified multimedia, and the comprehensive user identity authentication which considering the environment factors and the fingerprint of secure user, and the time seed which used for generating time master key and then further generating encryption key. This scheme takes advantage of the properties of MPEG-7 standard to generate the multimedia hierarchy organized into tree structure involving many elements each of which belongs to a security clearance level, the sensitive element or security content can be encrypted with proper key in term of security level and then the entire multimedia encrypted with another appropriate key and the multilevel encryption achieved. Finally, the security analysis of our scheme was describe and demonstrated that our scheme can resist the eavesdropping, impersonation attack, and colluding attack.

References

[1] Pan, L. and Zhang, C. N. A criterion-based multilayer access control approach for multimedia applications and the implementation considerations. ACM Trans. Multimedia Comput. Commun. Appl. 5, 2, Article 17 (November 2008), 29 pages.

[2] Kosch , H. Distributed Multimedia Database Technologies Supported by MPEG-7 and MPEG-21, CEC Press. 2004.

[3] Manjunath, B. S., S Alemabier, P., Sikora, T. Introduction to MPEG-7 Multimedia Content Description Interface, John Wiley & Sons, Ltd. 2002.

[4] S Alemabier, P., Smith, J. R. MPEG-7 multimedia description schemes. IEEE Trans. Circ. Syst. Video Techn. 2001. 11(6):748-759.

[5] Pan, L. and Zhang, C. N. A Criterion-Based Role-Based Multilayer Access Control Model for Multimedia Applications. Proceedings of the Eighth IEEE International Symposium on Multimedia (ISM'06). 145-152.

[6] http://en.wikipedia.org/wiki/Security_clearance

[7] Itkis G. Forward Security: Adaptive Cryptography-Time Evolution. Invited chapter for the Handbook of Information Security, John Wiley and Sons, Inc. 2006.

[8] Teng, P.Y., Huang, S.I. and Perrig, A.. Multi-Layer Encryption for Multi-Level Access Control in Wireless Sensor Networks. in IFIP International Federation for Information Processing, Volume 278. Proceedings of the IFIP TC11 23rd International Information Security Conference, Boston. Springer, 2008, 705-709.