An Efficient Key Distribution Method Applying to OMA DRM 2.0 with Device Identifier

Zonghua Liu, Guangqing Liu, Byungwook Lee
College of Software, Kyungwon University
lzh5333@hotmail.com, haibuo1981@hotmail.com, leebw@kyungwon.ac.kr

Abstract

As digital contents are increasingly used on mobile devices, Digital Rights Management (DRM) application will become a core component of mobile terminals. OMA DRM, invented by the Open Mobile Alliance (OMA), is the most widely available mobile DRM standard. Following a general description about OMA DRM 2.0, this paper gives a detailed analysis about cryptographic operations and Rights Objects acquisition. To reduce processing time and energy consumption in mobile terminal, previous papers mentioned to substitute asymmetric algorithm with symmetric algorithm on the protection of Rights Encryption Key (KREK). However, security analysis did not resolve. In this paper, we firstly make a comparison of asymmetric and symmetric algorithm on processing time, and then proposed using Device Identifier as symmetric encryption key to substitute asymmetric algorithm. Protection and distribution of symmetric encryption key are presented in the end.

1. Introduction

The Open Mobile Alliance (OMA), a standards body which develops open standards for the mobile phone industry, approved version 2, OMA DRM 2.0, in March 2006[1]. It is an extension to the first version. Each participating device in OMA DRM 2.0 has an individual DRM PKI certificate with a public key, and the corresponding private key. Each Rights Object (RO) is individually protected for one receiving device by encrypting it with the device public key. The RO in turn contains the key that is used to decrypt the media object. Delivery of RO requires a registration with the Rights Issuer (RI) to establish trust.

OMA DRM 2 provides a significantly higher level of security to protect high-value digital content like polyphonic ringtones, mp3 audio files or video clips on mobile terminals. However, from an end user's perspective, service's processing time and energy consumption (ie, battery lifetime) are said as the most importance performance-dimensions in paper[2]. Paper[3] referred that most of medias used on mobile devices are some light media content types with a lower value of around $1.00-$2.00 per item. With network and mobile device's capabilities increasing, access of high-value contents will becomes possible. Therefore, we can conclude that efficiency is also an important component in mobile environment.

Paper[2] chosen to substitute asymmetric algorithm with a symmetric algorithm using a device-generated key(KDev) when installing the Rights Objects(RO). It can achieve the same purpose that binding the RO to DRM Agent. However, how the symmetric key is distributed to Rights Issuer and how it is managed in Device securely did not describe. This paper starts out by making a general description about OMA DRM 2.0. And then a detailed analysis about cryptographic operations is presented. In section 3, we make a simple analysis about the cryptographic operations in paper[2]. And then a comparison of asymmetric and symmetric algorithm on processing time with different file sizes is made. Section 4 presents key distribution method that we proposed. In section 5, we describe the performance and conclude our paper.

2. OMA DRM 2.0

OMA DRM 2.0 defines four entities, Content Issuer, Rights Issuer(RI), DRM Agent, and User that interact with each other in order to provide access to protected digital content to the end-user. Content Issuer does packaging and delivering of DRM. RI makes the responsibility to assign permissions and constraints to DRM contents, and generate Rights Objects(RO). DRM Agent is responsible for enforcing permissions
and constraints and controlling access to DRM contents. User is the human user of DRM contents and can only access DRM contents through a DRM Agent. Trust in OMA DRM 2.0 is based on PKI-certificates issued by a Certificate Authority (CA).

### 2.1 Cryptographic Chain

Figure 1 shows the cryptographic chain that protects contents in OMA DRM 2.0. Contents are protected by symmetric key encryption and packaged to DRM Content Format (DCF). DCF has its own MIME content type and contains encrypted contents and addition meta-data, such as content description (original content type, vendor, version, etc.), rights issuer URL (a location where a RO may be obtained), and so on [4]. To ensure content confidentiality, Rights Issuer encapsulates the Content Encryption Key (K_CEK) in a RO as well as the permissions and constraints granted to the DRM Agent when accessing a DCF, the Message Authentication Code (K_MAC) which is used to ensure RO’s integrity, and the Rights Encryption Key (K_REK) with which K_CEK is encrypted. K_REK itself is encrypted using the DRM Agent’s public key (K_Pub). Thus only the holder of the DRM Agent’s private key (K_Priv) can dissolve this cryptographic chain.

![Figure 1: Cryptographic Chain in OMA DRM 2.0](image)

### 2.2 Rights Object Acquisition Protocol (ROAP)

The Rights Object Acquisition Protocol (ROAP) is a suite of DRM security protocols between a Rights Issuer (RI) and a DRM Agent in a Device. The Protocol suite contains a 4-pass protocol for registration of a Device with an RI and protocols: 2-pass and 1-pass, by which the Device requests and acquires RO [5].

Figure 2 is the 4-pass registration protocol which is a complete security information exchange and handshake between the RI and the Device.

1. Device Hello Message: is sent to Rights Issuer to initiate the 4-pass Registration protocol. This message expresses Device information and preferences.
2. RI Hello Message: is sent from the Rights Issuer to the Device in response to the Device Hello Message. This message expresses RI preferences and decisions based on the values supplied by the Device.
3. Registration Request Message: is sent as the third message to an RI to request registration with the RI.
4. Registration Response Message: is sent to Device in response to Registration Request message and completes the Registration protocol.

Successful completion of the Registration Protocol results in the establishment of an RI Context which is necessary for execution of the other protocols in the ROAP suite.

Figure 3 is the 2-pass acquisition protocol by which the Device acquires RO. This protocol includes mutual authentication of Device and RI, integrity-protected request and delivery of RO, and the secure transfer of cryptographic keying material necessary to process the RO.

![Figure 2: The 4-pass Registration Protocol](image)

![Figure 3: The 2-pass RO Acquisition Protocol](image)
3 Substitute Asymmetric with a Symmetric Algorithm

Through the description above, we know that how contents are protected and how the Content Encryption Key is protected and distributed in OMA DRM 2.0. High level security is ensured through two-layer encryption mechanism, however, processing time and energy consumption of mobile terminal (ie, battery lifetime) did not be considered sufficiently which is said as the most importance performance-dimensions in paper[2].

To improve the efficiency, paper[2] chosen to substitute asymmetric algorithm with a symmetric algorithm using a device-generated key $K_{Dev}$ when installing the RO. It can achieve the same purpose that binding the RO to DRM Agent. However, how the symmetric key is distributed to Rights Issuer and how it is managed in Device did not describe.

3.1 Comparison of Cryptographic Algorithms

In this section, we make a comparative test of symmetric and asymmetric algorithm on processing time. Test environment is Intel(R) Core(TM)2 Duo CPU E6750 @ 2.66GHz 2.66GHz, 2.00GB RAM. Standard symmetric algorithm AES is employed with 128bits key. We implement the AES encryption algorithm using the class library System.Security.Cryptography.Rijndael which is provided by .Net. Asymmetric algorithm RSA is employed and implemented using the library System.Security.Cryptography.RSACryptoServiceProvider which is also provided by .Net. We varied the file size as the Table 1 for encryption to see the possible influences on the performance. Because the encryption algorithm is used to encrypt keys(REK+MAC) in OMA DRM 2.0, we choose file size from 256 bits. Encryption time in Table 1 is a sum of 1000 times. Figure 4 shows the dates in table with a graph. We can see that encryption time of AES and RSA shows a significant difference. Furthermore, with the increasing of file size, the difference on processing time becomes larger.

<table>
<thead>
<tr>
<th>File size (bit)</th>
<th>AES(ms)</th>
<th>RSA(ms)</th>
<th>Difference(ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>256</td>
<td>15.625</td>
<td>109.375</td>
<td>93.750</td>
</tr>
<tr>
<td>512</td>
<td>15.625</td>
<td>125.000</td>
<td>109.375</td>
</tr>
<tr>
<td>1024</td>
<td>15.625</td>
<td>218.750</td>
<td>203.125</td>
</tr>
<tr>
<td>2048</td>
<td>31.250</td>
<td>312.500</td>
<td>281.25</td>
</tr>
</tbody>
</table>

4. An Efficient Key Distribution Method

Through the analysis above, we find that it is possible to provide a more efficient service if we substitute the asymmetric algorithm with a symmetric algorithm. But the security must be ensured at the same time. This section presents our proposals. Instead of using asymmetric algorithm, we use symmetric algorithm like paper[2]. But we use Device Identifier as symmetric encryption key. In section 4.2, key distribution method will be presented.

4.1 Device Identifier

Almost all devices such as mobile or desk-top have identifiers to make them be able to identify uniquely. IMEI(Internation Mobile Equipment Identification) or IMSI(International Mobile Subscriber Identity) numbers can be used as the mobile device identifier[6]. SN(Serial Number) can be used as IMEI number because it is different with other device’s and can not be changed. MN(Model Number) is a number that can uniquely identify the hardware and software version of a mobile device.

Device identifier is often used when content must be played only in a certain device, or used to indicate device’s capability when DRM entity such as content provider packages contents[7].

4.2 Key Distribution Method

We employ device’s SN(Serial Number) as symmetric encryption key($SN_{Dev}$). Review Figure 1, $SN_{Dev}$ takes the role of device’s public key($K_{pub}$) or private key($K_{pri}$), protecting Rights Encryption Key($K_{REK}$) and binding RO to Device. As discussed in section 4.1, $SN_{Dev}$ is unique to mobile device and unchangeable. Therefore, it certainly ensures RO only be used in device with the matching SN. Furthermore,
there is no need to manage it in device terminal. Just need to extract it when using. Hence, How the $SN_{Dev}$ can be distributed to RI securely remains to solve.

![Figure 5: Process of Distributing Device Identifier]

Figure 5 is the 4-pass Registration Protocol. Basic principle and functions are discussed in section 2.2. As seen in Figure 5, Device Identifier($SN_{Dev}$) is sent to RI with the Registration Request message. To ensure the key($SN_{Dev}$)'s confidentiality, we use RI’s public key to encrypt it($E_{Pub}[SN_{Dev}]$). Thus, only the RI can decrypt it out and use it to encrypt $K_{REK}$. After 4-pass Registration Protocol successfully completed, RO Acquisition Protocol begins. In other words, Distribution of symmetric encryption key does not happen with the RO acquisition. Hence, efficiency of the distribution of RO cannot be influenced.

5. Performance analysis and conclusions

5.1 Performance Analysis

Performance analysis of our proposal refers to next aspects:

- Efficiency
  Test results shown in section 3.1 illustrate that processing time can be significantly reduced by substituting asymmetric algorithm with symmetric algorithm. Processing time should be considered in OMA DRM, is the encryption time in Rights Issuer and decryption time in device terminal. Therefore, total time of license acquisition would be reduced more significantly. Certainly, energy consumption would be reduced to some degree.

- Security
  RO authenticity: The authenticity of the received Rights Object has been verified when $K_{REK}$ was decrypted successfully, since it is assumed that only trusted DRM agents can successfully do this operation. $K_{CEK}$, $K_{REK}$ and $K_{MAC}$ confidentiality: $K_{CEK}$ gets protected by $K_{REK}$, $K_{REK}$ and $K_{MAC}$ get protected by $SN_{Dev}$. $SN_{Dev}$ is protected by public key of Rights Issuer with asymmetric algorithm when distributing to Rights Issuer.

5.2 Conclusions

As digital contents are increasingly used on mobile devices, DRM application will become a core component of mobile terminals. Given the broad use of digital contents in mobile terminal, service efficiency must be considered. In this paper, we propose an efficient key distribution method for OMA DRM 2.0 by substituting asymmetric algorithm with symmetric algorithm. Device Identifier is used as symmetric encryption key and protected by asymmetric algorithm when distributing to Rights Issuer.

Efficiency of asymmetric algorithm and symmetric algorithm was test in PC client, and had a significant difference between them. However, a precision analysis in security and efficiency is also needed in further works.

6. Acknowledgement

This work is supported by the Ministry of Education, Seoul, Korea, under the BK 21.

Reference


