SECURING MOBILE ACCESS OF CONFIDENTIAL DOCUMENTS BY INTEGRATING TRUSTED COMPUTING PLATFORMS WITH DIGITAL RIGHTS MANAGEMENTS

Sue-Chen Hsueh¹, Chien-Chih Kuo²
Department of Information Management, Chaoyang University of Technology, Taiwan
¹schsueh@cyut.edu.tw; ²s9714633@cyut.edu.tw

Abstract
The mature mobile network today empowers mobile employees to access Intranet documents via mobile devices and increases the productivity of company workers. Internal documents transmitted without encryption through the open mobile networks undoubtedly creates security holes for eavesdroppers. A common way to provide preliminary protections for an important document to be accessed outside the Intranet is to transmit the document after encryption. Such mechanisms, however, cannot assure the security of documents because the documents can be decrypted and then forwarded without protections once the ciphering keys were known. Therefore, we propose an approach to enhance the security of transmitted mobile documents, using the idea from digital rights managements. A confidential document is encrypted so that, except the targeted mobile user, none can read the confidential document without proper rights. The proposed approach utilizes the trusted computing platforms (TPM) technology to protect the rights object of a confidential document. A rights object can be as simple as a ciphering key of the document or as complicated as the usage-rules of the document. A malicious user can never decrypt the rights to access the transmitted document, which is encrypted. Moreover, the usage-rules in the rights object may specify whether the document can be further forwarded or be read more than once, and so on. Therefore, the proposed scheme provides maximum flexibilities for mobile employees to access confidential documents without compromising the security, in addition to the mobility and timeliness of mobile environments.

Keywords: Mobile enterprise, digital rights management, trusted computing platforms, information security

Introduction
To avoid the disclosures of confidential information in a company, the employees only accessed the paper documents in a company. In the mobile Internet era, it will be allowed to access digitalized documents at any time and any place through mobile added-valued services using the mobile phones.

Whenever necessary, an employee uses handheld devices to connect to Internet so that he can instantly access documents for efficiency. Currently, digital content protection method is protected by digital rights management mechanisms [3]. Digital content will be divided into the content part and the rights part to prevent illegal use of a malicious user. Previous methods can only protect the security of digital content during transmission but the security issue of digital content transmission to other devices is ignored. Therefore, this research will combine the security services delivery mechanism of the mobile device, proposed by Adrian Leung [1], with DRM to protect the forgery, modification and transmission problems of the digital content.

Related work
According to the security service delivery mechanism proposed by Adrian Leung [1], three kinds of security technologies including TPM, MAC (Message Authentication Code) and hash function are used in the design of our proposed security mechanism. First, TPM is used to generate a non-migratable key to encrypt a message. Thus, even if a malicious user has the content, he has no key to decrypt the message. The message needs the key owned by the mobile device to decrypt the message. Moreover, the usage-rules in the rights object may specify whether the document can be further forwarded or be read more than once, and so on. Therefore, the proposed scheme provides maximum flexibilities for mobile employees to access confidential documents without compromising the security, in addition to the mobility and timeliness of mobile environments.
In this paper, we will apply symmetric encryption, DRM and TPM as the main security mechanisms.

**A Company document transmission Mechanism**

This study combines TPM technology with DRM technology, using mobile devices as the platform, for manipulating company documents remotely. We ensure that the classified documents will not be tampered and forged by malicious users during transmissions. It will encrypt the documents using a secret key, concatenating International Mobile Equipment Identity number (IMEI), documents ID (CID) and a random number (RN), to prevent the intercept of the confidential documents. We use a pair of keys by the TPM mechanism (PKTP, SKTP) for the document to be delivered to other equipment, so that non-recipients cannot access the encrypted document having no private key. Section 3.1 first introduces the system structure of a company document transmission mechanism. The process of obtaining company documents obtained, comprising the content and the right, is described. The two stages of our design, content acquisition and rights acquisition will be illustrated and the functions and security will be discussed.

**System Architecture**

The proposed architecture, as shown in Figure 1, is composed of user, content provider and rights provider. The main process of obtaining content and rights is also outlined. The architecture bases on the TPM approach, proposed by Adrian Leung, and extends the DRM mechanism to enhance the security of transmissions of the documents in the company.

When users want access to company documents must be send a request to content provider, when the content provider receives a request then the company document and to open the parts of key of the document to transmission to users. When the user wants to use company documents must be sent as identity information to content providers, If the validation is successful, the content providers will transmission the parts of key to rights issuer. Rights issuer receives the part of the key and confirm legal then the key to re-package will be delivered to users. Users receive two sets of keys will be merged with the keys to unlock the encrypted company documents to obtain the content.

**Acquire Content Phase**

At the beginning users, content provider and rights issuer has a mutual key to encrypt the messages. The user uses $K_{UC}$ to encrypt the $C_{ID}$ and IMEI, and we uses $K_{UID}$ to encrypt the $PKTP$ and $UID$ delivered the two ciphertext to content provider, expression: $K_{UC}(C_{ID}, IMEI) \cdot K_{UID}(PKTP, UID)$. The content provider receive the ciphertext from user and then it decrypts $K_{UC}(C_{ID}, IMEI)$ using $K_{UC}$ to
obtain $C_{ID}$ and $IMEI$. Using the hash function to hashing the $CID||IMEI||RN$, expression: $SEK=H(CID||IMEI||RN)$, the generated value by the hash function is defined as $SEK$, the purpose is enable users use RN to unlock the company documents in the obtain right phase, because RN is generated by the content providers and user to get content at the beginning did not know, therefore it is not possible to calculate $SEK$. Content provider using $SEK$ to encrypt the content and sent to the user, expression: $E_{SEK}(\text{Content})$. Content provider cannot be solved the ciphertext by $K_{CR}$ to encrypt the content at this phase, the purpose is the content promoter doesn't know a content, so cannot counterfeit or distort a content (Figure 2).

### Security Analysis

The proposed method satisfies the following security requirement.

1. **Confidentiality**

In content acquiring phase, the user will deliver the information using the $K_{IC}$ and $K_{CR}$ to encrypt to content provider, expression: $K_{IC}(C_{ID}, IMEI) \cdot K_{UR}(PK_{TP}, U_{ID})$. The content provider use the hash function computing the value to encrypt the company document, expression: $E_{SEK}$(Content). In acquire right phase, the content generated using $K_{CR}$ to encrypt $RN$, expression: $K_{CR}(RN)$, it using the public key of the TPM produce to encrypt the $RN$ and $U_{ID}$, expression: $PK_{TP}(RN, U_{ID})$, the ciphertext must using the public key and privacy key of the TPM generated to match.

### Table 1: Notation

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP</td>
<td>The Content provider</td>
<td>SEK</td>
<td>Session key</td>
</tr>
<tr>
<td>RI</td>
<td>The Right provider</td>
<td>Content</td>
<td>Company document</td>
</tr>
<tr>
<td>$U_{ID}$</td>
<td>A User ID</td>
<td>RN</td>
<td>Random number</td>
</tr>
<tr>
<td>$C_{ID}$</td>
<td>A Company document ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$K_{CC}$</td>
<td>Users and content providers share a key</td>
<td>$IMEI$</td>
<td>International Mobile Equipment Identity number</td>
</tr>
<tr>
<td>$K_{CR}$</td>
<td>Users and rights providers share a key</td>
<td>$PK_{TP}$, $SK_{TP}$</td>
<td>The public and private key pair of principal TPM</td>
</tr>
<tr>
<td>$K_{CR}^*$</td>
<td>Content providers and rights providers share a key</td>
<td>$PK_{CR}(M)$</td>
<td>The encryption of a $M$, using the $PK_{TP}$</td>
</tr>
<tr>
<td>$H()$</td>
<td>A One-way hash function</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Acquire Right Phase

When the employee wants to use the document of the company, then encrypt the $C_{ID}$ using $K_{IC}$ to deliver to the content provider. Because the $SEK$ is composed of $C_{ID}$, $IMEI$ and $RN$ in phase of obtained content then it can be through the $C_{ID}$ to find $RN$. The content provider receive the message and unlock, it through the $C_{ID}$ to find the corresponding $RN$ then uses the $K_{CR}$ to encrypt the $RN$. The $K_{CR}(RN)$ together with $K_{UR}(PK_{TP}, U_{ID})$ delivered to the right issuer.

The rights issuer receive the message and unlock to obtain the $RN \cdot PK_{TP} \cdot U_{ID}$. It uses the $PK_{TP}$ to encrypt the $RN$ and $U_{ID}$ delivered to the user, expression: $PK_{TP}(RN, U_{ID})$. Using $PK_{TP}$ is to ensure that only holds $SK_{TP}$ equipment can match with the $PK_{TP}$ to unlock the ciphertext. The user receipts the message and unlock, it using the hash function to compute the RN|$C_{ID}$|$IMEI$ to obtain the $SEK$, then it use the $SEK$ to decrypt company document (Figure 3).

---

Figure 1: System architecture

Figure 2: Acquire content phase

Figure 3: Acquire right phase
then unlock the company document, therefore reach confidentiality of information.

(2) Verifiability
The company document contains the \( C_{ID} \), \( IMEI \) and \( RN \), the equipment must provide the information to enable the composition of \( SEK \), the malicious users cannot provide such information, and therefore it cannot know the content.

(3) Non-repudiation
The user provide the message of include \( IMEI \) to content provider. The user provide the message of include \( PK_{RP} \) to right issuer. These are two information can be proving the message by the user to send.

(4) Integrity
The message through the sharing of the key \( (K_{UC} \cdot K_{UR} \cdot K_{CR}) \) to encrypt, therefore only the both sides of own sharing key can unlock the message. In the acquire right phase, the right issuer delivered the \( RN \) have been tampered by malicious users will not be able to compute the \( SEK \), to cause the company document cannot be unlock, therefore can protect the integrity of the company documents.

(5) Integrity
In the acquire content phase, when the content provider using the \( SEK \) to encrypt the company document, the malicious user cannot acquire the \( RN \), only the content provider known, therefore it can achieve the integrity.

(6) Alternation
In the acquire right phase, the right issuer using the \( PK_{RP} \) to encrypt \( RN \) and \( U_{ID} \), if a malicious user intercept the message and tampering with the message, but only hold the mobile equipment of the \( SK_{RP} \) can be unlock and to acquire the content.

Conclusion
In this research, we integrate TPM and DRM mechanisms to deliver the documents of a company for preventing malicious users to tampering or forgery of the documents. The content is protected by the TPM mechanism so that malicious users cannot decrypt the content in the non-bound mobile device. Therefore, we can prevent invalid delivery of the content. Using the DRM mechanism further binds content with rights so that decrypting the content is impossible unless proper rights are acquired. A malicious user may get the content but he may not be able to decrypt the contents for readable information. In the future, the TPM can be combined with DRM for applications such as e-books so as to resolve current security issues. E-books then can be flexibly used and consumers might be encouraged to use e-books.

References