Securing Mobile Access of Confidential Documents by Integrating Trusted Computing Platforms with Digital Rights Managements

Sue-Chen Hsueh

Chien-Chih Kuo

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

Sue-Chen Hsueh[1], Chien-Chih Kuo[2]
Department of Information ManagementChaoyang University of Technology, Taiwan
[1]schsueh@cyut.edu.tw; [2]s97114633@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. We use the public key in TPM to encrypt the rights object so that only the dedicated mobile device, i.e. the mobile user, may decrypt the rights object using the private key of the device. 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 to 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.

Relate 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. Next, we wrapped the message and MAC so that both parties in the communication may verify the integrity of the receipt of this message. Aspects of the one-way hashing, using the hash function to compute the three parameter then use the output value as the key to encrypt message and MAC, the malicious users cannot know the parameter so it is not possible to obtain key to decrypt the message. Aspects of the timestamp, it is used to verify whether the both sides time of the send the message within the specified time and it is used to detect whether the messages is being tampered.

According to the Chin-Ling Chen scholar proposed E-DRM system [4], it use the PKI to design security mechanism, the author create the contents of the package into a DRM format. When a user access to content, it must through the certificate server to register, the user must send the IMEI and certificate of mobile devices to the certificate server register, after successful registration will return a random number to the user and then the user send the message and certificate to the certification center, the certification center re-transmission of a message to the certificate server for authentication. The certificate server received and confirmation message, it will a key of decrypt the message to passed to the user, after the user received can use the key to decrypt the message. It is can prevent though malicious user to get the message is also unable to obtain key through use hash function to compute the random numbers and personal certificate information, therefore, it can prevent forgery and alternation of message.

According to Yin-Ling Liong and Sudhir Dixit proposed digital rights management for the mobile internet [5], introduction of DRM and DRM components and OMA (Open Mobile Alliance) organization [7] and REL (Rights Expression Language). OMA will be DRM delivery models divided into three kinds, forward-lock, combined delivery and separate delivery. In the forward-lock mode, the digital content is packaged into a DRM format, does not include right object, users are free to use the digital content, is suitable for low-value content. In the combined delivery mode, the digital content is divided into content and right packaged into a message, through the right object to regulate the condition of use digital content, such as: frequency of use and use of time. In the previous two methods, when the mobile phone users to download content, you cannot send the content to other users. In the separate delivery mode, the message is divided into content and right is separated from each other with no packaging, when a user downloads digital content and to use it, you must to obtain the right to use, in this mode, digital content can be passed to other users, right will have to get through the issuer.

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 (C_{ID}) and a random number (*RN*), to prevent the intercept of the confidential documents. We use a pair of keys by the TPM mechanism (PK_{TP}, SK_{TP}) 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_{UR} to encrypt the $_{\mathrm{PKTP}}$ and $_{\mathrm{UID}}$ delivered the two ciphertext to content provider, expression: $K_{UC}(C_{ID}, IMEI)$, $K_{UR}(PK_{TP}, U_{ID})$. The content provider receive the ciphertext from user and then it decrypts $K_{UC}(C_{ID}, IMEI)$ using K_{UC} to

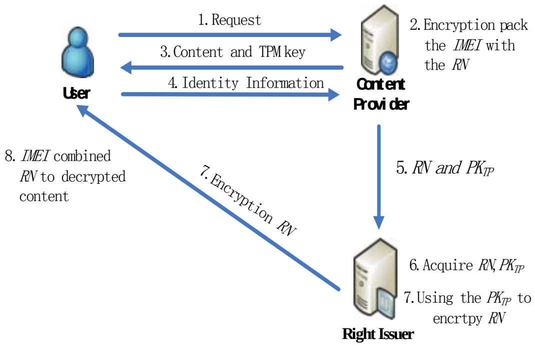
1. Request
2. Encryption pack the *IMEI* with the *RN*
3. Content and TPM key
4. Identity Information
User
Content Provider
5. *RN and* PK_{TP}
8. *IMEI* combined *RN* to decrypted content
7. Encryption *RN*
6. Acquire *RN*, PK_{TP}
7. Using the PK_{TP} to encrtpy *RN*
Right Issuer

Figure 1: System architecture

Notation

Table 1: Notation

Notation	Description	Notation	Description
CP	The Content provider	*SEK*	Session key
RI	The Right provider	*Content*	Company document
U_{ID}	A User ID	*RN*	Random number
C_{ID}	A Company document ID	||	The concatenation operator
K_{UC}	Users and content providers share a key	*IMEI*	International Mobile Equipment Identity number
K_{UR}	Users and rights providers share a key	PK_{TP}, SK_{TP}	The public and private Key pair of principal TPM
K_{CR}	Content providers and rights providers share a key	$PK_{TP}(M)$	The encryption of a M, using the PK_{TP}
H()	A One-way hash function		

obtain C_{ID} and *IMEI*. Using the hash function to hashing the *CID*||*IMEI*||*RN*, expression: *SEK*=H(C_{ID}||*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}(Content). Content provider cannot be solved the ciphertext by K_{UR} 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)

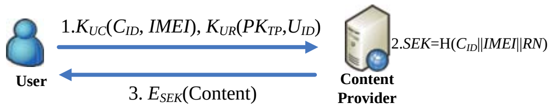
1.$K_{UC}(C_{ID}, IMEI)$, $K_{UR}(PK_{TP},U_{ID})$
2.*SEK*=H(C_{ID}||*IMEI*||*RN*)
User
3. E_{SEK}(Content)
Content Provider

Figure 2: Acquire content phase

Acquire Right Phase

When the employee wants to use the document of the company, then encrypt the C_{ID} using K_{UC} 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 receipt 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 receipt the message and unlock to obtain the *RN*、PK_{TP}、$U_{ID.}$ It uses the PK_{TP} to encrypt the *RN* and U_{ID} to 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).

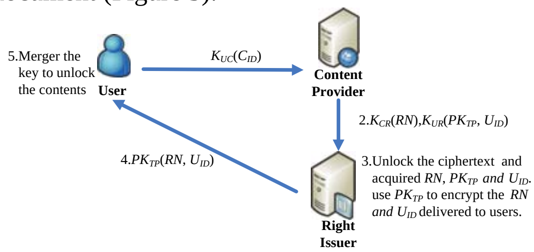
5.Merger the key to unlock the contents
User
$K_{UC}(C_{ID})$
Content Provider
2.$K_{CR}(RN)$,$K_{UR}(PK_{TP}, U_{ID})$
4.$PK_{TP}(RN, U_{ID})$
3.Unlock the ciphertext and acquired *RN*, PK_{TP} *and* U_{ID}. use PK_{TP} to encrypt the *RN* *and* U_{ID} delivered to users.
Right Issuer

Figure 3: Acquire right phase

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_{UC} and K_{UR} to encrypt to content provider, expression: $K_{UC}(C_{ID}, IMEI)$，$K_{UR}(PK_{TP}, U_{ID})$. 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 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_{TP} 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}、K_{UR}、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_{TP} 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_{TP} 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

[1] Adrian Leung, “A Mobile Device Management Framework for Secure Service Delivery,” *Journal of Information Security Technical Report*, 2008, vol. 13, no. 3, pp. 118-126.

[2] Imad Abbadi and Chris Mitchell, “Digital Rights Management Using a Mobile Phone,” *Proceedings of the ninth International Conference on Electronic Commerce*, 2007, pp. 185-194.

[3] Kwon Il Lee, Kouichi Sakurai, Jun Seok Lee, and Jae Cheol Ryou, “A DRM Framework for Secure Distribution of Mobile Contents,” *Proceedings of the International Conference ICOIN on Information Networking*, 2004, pp. 905-914.

[4] Chin-Ling Chen, “A Secure and Traceable E-DRM system Based on Mobile Device,” *An International Journal of Expert Systems with Applications*, 2008, vol. 35, no. 3, pp. 878-886.

[5] Yin-Ling Liong and Sudhir Dixit, “Digital Rights Management for the Mobile Internet,“ *An International Journal of Wireless Personal Communications*, 2004, vol. 29, no. 1-2, pp. 109-119.

[6] Xiaoping Wu, Zhidong Shen, Huanguo Zhang, “Secure Key Management of Mobile Agent System Using TPM-Based Technology on Trusted Computing Platform ,” *Proceedings of International Conference on Computer Science and Software Engineering*, 2008, vol. 3, pp.1020-1023,

[7] Open Mobile Alliance (OMA) http://www .openmobilealliance.org/

[8] Trusted Computing Group (TCG)http:// www.trustedcomputinggroup.org