A Cloud based SIM DRM Scheme for the Mobile Internet *

Peng Zou† Chaokun Wang† Zhang Liu‡ Jianmin Wang† Jia-Guang Sun†
†School of Software, Tsinghua University
Key Laboratory for Information System Security, Ministry of Education
Tsinghua National Laboratory for Information Science and Technology, Beijing 100084, China
‡Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China
{†zoup04, ‡liuzhang08}@mails.thu.edu.cn, †{chaokun, jimwang, sunjg}@tsinghua.edu.cn

ABSTRACT

With the rapid growth of the mobile industry, a considerable amount of mobile applications and services are available. Meanwhile, pirates and illegal distributions of digital contents have become serious issues. Digital Rights Management (DRM) aims at protecting digital contents from being abused through regulating the usage of digital contents. In this paper, a cloud based SIM DRM scheme, called CS-DRM, is proposed for the mobile Internet. Also, a prototype of our DRM scheme is implemented to demonstrate the correctness, effectiveness and efficiency of CS-DRM.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Authentication*

General Terms

Design, Security

Keywords

Cloud computing, DRM, SIM card, Mobile Internet

1. INTRODUCTION

With the rapid growth of the mobile industry, a considerable amount of mobile applications and services are available. As a result, users are capable of sharing and distributing digital media contents easily through the mobile Internet. However, a large number of digital contents have been pirated and illegally distributed.

Digital Rights Management (*DRM*) is a mechanism which protects digital media contents from being abused through regulating the usage of digital contents. In the context of a DRM system, only an authorized user, who has obtained a license, can access the digital content according to the rights information defined in the license.

*This work was partially supported by the National Natural Science Foundation of China (No. 60803016, No. 90718010), the National Basic Research Program of China (No. 2007CB310802), the National High Technology Research and Development Program of China (No. 2008AA042301) and Tsinghua National Laboratory for Information Science and Technology (TNList) Cross-discipline Foundation.

CCS'10, October 4–8, 2010, Chicago, Illinois, USA.
ACM 978-1-4503-0244-9/10/10.

Current DRM schemes can be classified into two categories — Device based DRM and Smart Card based DRM. In a device based DRM scheme, such as OMA (Open Mobile Alliance) DRM [1], the security comes from enforcing usage of compliant players and unique global device identifiers. However, this kind of DRM schemes is constrained by its inflexibility, especially in the mobile Internet. The smart card based DRM scheme is proposed to overcome the inflexibility of the device based DRM scheme. The security of smart card based DRM schemes comes from key generation related algorithms and protocols protected by the smart card. However, there are security issues, such as imposter attacks [4, 5], in some existing smart card based DRM schemes. Meanwhile, existing smart card based DRM schemes are uneconomic and inconvenient in the mobile Internet. For example, besides a smart card, each mobile device needs a smart card reader [5].

Taking note of shortcomings of smart card based DRM schemes, for the mobile Internet, we propose a SIM DRM (SIM card based DRM) scheme which use a SIM card instead of a smart card. In our SIM DRM scheme, the SIM card is not just for authentication. Based on the SIM card, we design a set of algorithms and protocols for the safety of licenses and contents. It overcomes the deficiency of existing smart card based DRM schemes. Meanwhile, we introduce cloud computing into DRM schemes. It can satisfy performance requirements of the entire DRM system with low cost by providing powerful services when the number of user visits scales up. Also, the virtualization technology in a cloud computing environment guarantees data security, sharing and isolation among a large number of content providers.

In summary, our main contributions are as follows.

1) We propose a novel DRM scheme, called CS-DRM, which is a cloud based SIM DRM scheme for media protection in the mobile Internet. The usage of the SIM card instead of the smart card not only reduces the unnecessary cost, but also provides higher security. In addition, the cloud computing is introduced into the scheme to provide more efficient and higher quality services.

2) We have implemented a prototype, called *Phosphor*, of our proposed scheme. Meanwhile, extensive experiments on the performance of our proposed CS-DRM scheme and Phosphor are conduced, which demonstrates that CS-DRM is efficient, secure and practicable.

2. CS-DRM SCHEME

A CS-DRM scheme is defined as a 4-tuple $(\mathbb{E}, \mathbb{S}, \mathbb{P}, \mathbb{A})$ where $\mathbb{E}$ is the set of entities in cloud clients, $\mathbb{S}$ the set of

Table 1: A Comparison of Some DRM Schemes

DRM Scheme	OMA DRM [1]	Conrado et al.'s DRM [4]	TMP-based DRM [6]	CS-DRM
Characteristic	Device based	Smart card based	Trust mobile platform Based	SIM card and cloud based
Encrypted Content	Yes	No	Yes	Yes
Privacy Protection	No	Yes	No	Yes
PKI used in the license delivery	Yes	No	Yes	No
Information Stored	Public/Private key	PK/SK, SK_p and $SK_p^{'}$	Public/Private key and sensitive information for proving the identity	K_i, LSW and sensitive information for proving the identity

application services based on cloud computing, $\mathbb{P}$ the set of protocols among all elements in both $\mathbb{E}$ and $\mathbb{S}$, and $\mathbb{A}$ the set of auxiliary algorithms used in $\mathbb{P}$.

In a system implementing a CS-DRM scheme, only customers who have purchased the corresponding licenses can use or access the digital contents by a frontend, i.e., a cloud client. The backend of the system contains kinds of application services based on cloud computing, which are charge of generating, storing and transmitting encrypted digital contents and corresponding licenses. Communication protocols support the licenses acquisition and verification between cloud clients and servers. Besides, algorithms for encrypting/decrypting secret keys and digital contents are also necessary parts in CS-DRM schemes.

In CS-DRM, a digital content is encrypted by a content key K_c. In order to decrypt and render the digital content, a DRM client must obtain the corresponding license ℓ which contains K_c from the license server. Note that K_c is encrypted in ℓ, and therefore a malicious user cannot acquire the content of K_c even though (s)he gets ℓ. In order to protect K_c, a SIM card is introduced as a client entity in the frontend. In detail, the secret key K_i which is used to decrypt K_c in ℓ is stored in the SIM card, and the algorithm used to decrypt K_c is implemented as a hardware module inside the SIM card. To prevent ℓ from being tampered, a data structure called *license state word (LSW)* is stored in the file system of the SIM card. LSW is calculated by hashing the content of ℓ. Each time when the cloud client applies for K_c, the SIM card verifies LSW via comparing the value of LSW stored in the SIM card with the hash value of ℓ. If the verification is successful, the SIM card decrypts K_c in ℓ and K_c can be used to decrypt the digital content. Otherwise, the K_c application is denied.

To support the communication between the cloud client and the SIM card, we designed two new protocols — License State Word Protocol (LSWP) and License Acquisition Protocol (LAP). Both protocols are implemented with APDU instruction set which is defined in GSM11.11 and GSM11.14.

3. CHARACTERISTICS OF CS-DRM

In this section, we discuss characteristics of CS-DRM by analyzing security, privacy issues and the cost of CS-DRM. As shown in Table 1, in order to elaborate on these characteristics more clearly, we compare CS-DRM with several typical DRM schemes.

3.1 Security Analysis

The security of our proposed CS-DRM scheme is distinguished by the utilization of SIM card and LSW.

SIM card is safe enough to store K_i and other important information due to the following points, though it is perhaps running in a hostile environment. Firstly, it is difficult to crack a SIM card thanks to well-defined industrial standards, such as ISO 7816, GSM11.11, and GSM11.14. Secondly, data hiding approaches [2] applied in the file system of the SIM card make LSW secure and invisible to crackers. Finally, the interaction between a SIM card and a DRM agent is protected by LSWP.

Two attack types are listed as follows. We analyze these attacks and present the solutions in CS-DRM.

Attack 1: Tamper the License. CS-DRM guarantees the integrity of a license by the LSW and SIM card. If an illegal modification happens, a hash value ($Hash$) will be calculated according to the license. The DRM agent compares the computed $Hash$ with $License\_Hash$ in the LSW by LSWP, before the DRM agent uses the license. The modification can be noticed if the computed $Hash$ is different from the $License\_Hash$. Once the DRM agent notices that the license has been tampered, it marks the license. It means that the license is not available any more. The attacker could not use the tampered license.

Attack 2: Tamper or Detect the LSW. First, the LSW is stored in the SIM card file system that owns a complete access control mechanism. Only authorized programs can access and modify the file system. Because of that, a malicious user could not tamper the SIM card file system. Second, a malicious user can scan the SIM card file system using special tools, e.g. SIMbrush [2]. However, the data hiding approach applied on the LSW makes LSW invisible. A malicious user will not detect the LSW information even if (s)he can scan the file system. Therefore, the attacker could not access the content by tampering or detecting the LSW.

3.2 Privacy Analysis

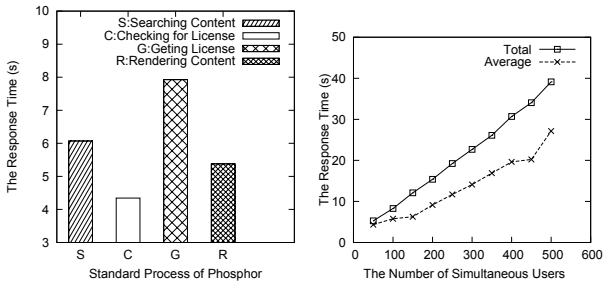
CS-DRM has the privacy protection for users. In our scheme, the International Mobile Subscriber Identity (IMSI) of the SIM card is the only sensitive information which can be used to know the user identity. However, the hash value of IMSI instead of IMSI itself is used during the process of the license acquisition. The license server could not match this hash value with a certain user. Meanwhile, the mobile operator does not divulge user privacy, which makes sure that the license server can only get K_i and is impossible to acquire the user identity information from the mobile operator. Therefore, no one could acquire the privacy information of a user, such as the license list of contents consumed by a user and the user identity.

3.3 Cost Analysis

Comparing with existing DRM schemes, the cost of CS-DRM is much lower. Firstly, the SIM card of CS-DRM replaces the smart card of smart card based DRM schemes.

(a) (b)

Figure 1: Screenshots on Nokia N73: (a) customizing the right content when purchasing a license; (b) rendering a testing video in a DRM player.



(a) (b)

Figure 2: Experimental Results: (a) running time; (b) total response time in the private cloud.

It reduces the cost of issuing a smart card and a smart card reader. Secondly, comparing with some DRM schemes (such as OMA DRM) which protect the sensitive data depending on the mechanisms of Certificate Authority (CA) and PKI , CS-DRM removes CA from the scheme, which reduces the cost of purchasing certifications for each cloud client. Thirdly, CS-DRM is a cloud based DRM scheme whose most important characteristic is its "pay-as-you-go" manner. Meanwhile, the high elasticity of the cloud [3] brings capabilities of matching resources to workload much more closely by adding or removing resources at an acceptable time of minutes rather than weeks, which makes CS-DRM satisfy the requirements of cloud clients automatically according to the current demands with a low cost. Also, the disaster recovery and maintenance cost of the entire system is reduced by the cloud.

4. IMPLEMENTATION & EXPERIMENTS

We have developed a prototype called Phosphor which implements the CS-DRM scheme. The frontend of Phosphor is implemented using Symbian C++ on the Nokia S60 3rd platform and deployed on Nokia N76 mobile phones, as shown in Fig. 1. In the backend, we developed and deployed application services of CS-DRM based on the J2EE framework on a cluster of machines locally as a private cloud.

Specifically, Phosphor is designed for protecting mobile streaming multimedia currently. Obviously, we can easily extend Phosphor to protect other kinds of media. A preliminary description of Phosphor was presented in [7].

We run our DRM player in the N76 to show the effectiveness of Phosphor according to a standard process which can be divided into the following four main steps (a video is available at http://learn.tsinghua.edu.cn:8080/2006990024/demo/Phosphor.wmv). The first step starts when a user browses the content portal web site and ends when (s)he selects her/his favorite. The second starts when the user clicks "play" button to check for a license for watching the media content and ends when the rights customization web page appears on the browser. The third starts when the user customizes the rights and ends when (s)he acquires the license. The fourth starts when the user gets the license and ends when the user can watch the media. As shown in Fig. 2(a), we measure the approximate running time of each step, which includes the time of artificial operations, such as filling out forms. Just because of artificial operations, users would not feel intolerable or boring. Removing the time-cost of these artificial operations, our scheme has excellent effectiveness.

In addition, for the efficiency, we simulate simultaneous users sending requests to license service for acquiring licenses and calculate the response time — T_{tlt} and T_{ave}. T_{tlt} denotes the duration from the moment when the first user sends request to the moment when the last user receives the response, which reveals the longest latency a user endures. T_{ave} represents the average response time for one user. As shown in Fig. 2(b), both T_{tlt} and T_{ave} increase when the number of simultaneous users scales up. Meanwhile, the total running time is a little longer than the response time of the individual user.

5. CONCLUSION

In this paper, a cloud based SIM DRM scheme, called CS-DRM, is proposed for the mobile Internet. SIM card is introduced to not only reduce the cost but also provide higher security. Meanwhile, because of the cloud, CS-DRM can concern benefits for content providers, and well satisfy the performance requirements with low cost when the number of users scales up. A prototype of our DRM scheme, called Phosphor, is also implemented to demonstrate that CS-DRM is efficient, secure and practicable.

6. REFERENCES

[1] OMA DRM Specification V 2.1, 2009. http://www.openmobilealliance.org.

[2] S. Antonio and G. Paolo. Data Hiding in SIM/USIM Cards: A Steganographic Approach. In *SADFE07*, pages 86–100, 2007.

[3] M. Armbrust. Above the Clouds: A Berkeley View of Cloud Computing. Technical Report UCB/EECS-2009-28, Berkeley, 2009.

[4] C. Conrado, F. Kamperman, G. J. Schrijen, and W. Jonker. Privacy in an Identity-based DRM System. In *DEXA03*, pages 389–395, 2003.

[5] H. Sun, C. Hung, and C. Chen. An Improved Digital Rights Management System Based on Smart Cards. In *DEST07*, pages 308–313, 2007.

[6] Y. Zheng, D. He, H. Wang, X. Tang, and L. Fiege. Secure DRM Scheme for Future Mobile Networks based on Trusted Mobile Platform. In *WiCOM05*, pages 1164–1167, 2005.

[7] P. Zou, C. Wang, Z. Liu, and D. Bao. Phosphor: A Cloud based Mobile DRM Scheme with Sim Card. In *APWEB10*, pages 459–463, 2010.