Secure Domain Architecture for Interoperable Content Distribution

Lei Lei Win[1], *Tony Thomas*[1], *Sabu Emmanuel*[1]
[1] School of Computer Engineering
Nanyang Technological University, Singapore

Mohan S. Kankanhalli [2]
[2] School of Computing
National University of Singapore, Singapore

Abstract. Authorized domains are used to share digital content among multiple devices without violating the copyright issues. However, if a domain is composed of multiple devices supporting different DRM technology, sharing and accessing of contents among the multiple devices in a domain may not be possible. To address this issue, in this paper we propose a new secure domain architecture which uses a Local Domain Manager (LDM) and T-licenses for achieving interoperability. The LDM serves as a middle entity that handles the distribution of interoperable domain content to all the registered domains according to the T-Licenses provided by the respective content providers. Thus, the proposed domain architecture enables secure sharing and accessing of digital content in an authorized domain.

Key Words: DRM, Authorized Domain, Interoperability, Content distribution.

1. Introduction

With the advances in DRM technologies, the distribution of digital content over electronic network has become a convenient and attractive means for commercial content publishers. In a traditional DRM architecture, creation, distribution and consumption of digital content are carried out by Contents Provider (CP), Contents Distributor (CD), and Contents Consumer (CC) respectively [1], [2], [3]. Most of the current DRM systems are now realizing the need for a mechanism which ensures seamless content flow among multiple devices of a user. This requirement has lead to the advent of authorized domain (AD) concept. The content which bounds to an AD can flow across the devices in the AD. However, all the devices in the domain need to stick to a common DRM technology. This is because the current DRM regimes are not interoperable. The naive approach for interoperability of DRM content in a domain is to install multiple DRM agents or multiple content subscription systems on the devices in the domain. However, this approach is not viable, if the domain contains devices with less storage capability and processing power.

In this paper, we propose secure domain architecture for interoperable content sharing using a middle entity called Local Domain Manager (LDM) and special licenses called T-licenses. There are many existing papers that use middle entity locally or online to achieve interoperability [5], [6], [7], [8], [9]. In [5], each device needs to request the translation to the middle entity, requiring a continuous online connectivity for each device. In [6], [7], [8], [9], they use the middle entity locally within the home network, thus difficult to control the content translation of middle entity by respective CPs. Further, since the content translation is carried out offline within the home network, malicious home devices can request translated content unlimitedly. In the following section we describe our new interoperable domain architecture. Due to space limitations, we do not discuss any mechanisms for license translation in this paper. For those readers interested in license management issue can refer to [11], [13].

2. Proposed Architecture

Our architecture makes use of Trusted Platform Modules (TPM). Readers may refer to TCG [7], [12] for detailed specification of a TPM. In this section, the internal structure of proposed multi-domain architecture as illustrated in figure 1 and the detail work flows will be explained.

2.1 Functional Entities

The various entities involved in the architecture are *Registration Server (RS), Content Providers (CPs), Home Domain Manager (HDM), Local Domain Manager (LDM) and Log Collection Center (LCC)*. RS is a TTP (third trusted party) responsible for registration and managing of all the devices in the architecture. Each end device registers either as a domain member device, a Home domain manager or a standalone device. An HDM is one of the domain devices in a domain and is a TCG-compliant machine with good computational power and storage capacity that is dedicated for managing home domain devices and the content flow within the domain. Each domain is allowed to have only a single home domain manager specified by a domain owner and RS using a certificate from a CA. An LDM is meant for providing content distribution and negotiation services to authorized-domains or end devices. It has its own content server (CS) and a third trusted party License Server (LS) which is trusted by all CPs. LCC is a trusted third party of CPs that performs violation detection of LDM and consumers. License Servers (LS) of CP and LDM, and domain devices generates audit logs files of their usage patterns. Those files are appended when LDM requests T-licenses from the respective CP or when a domain devices requests usage license from the HDM. Those files will be collected by the LCC and validated in order to detect violation of LDM and domain devices.

2.2 Domain Management

Domain management issues may be divided into two groups: domain device management and domain content management. Domain device management involves the issues of domain creation, joining or leaving of devices from a domain, and domain upgrading. Domain content management deals with managing the content and license acquisition for each domain. RS is responsible for Domain device management. To join a domain, a device can choose a domain group from a list of authorized domain provided by the RS. If a domain owner wants to create a new domain of his devices, he needs to register a device as a HDM and some set of his devices as domain members to RS. RS stores domain generation counter, current number of domain devices N_C and the maximum number of devices N_{max} allowed for that domain and domain information *I* such as domain key(s), domain ID, domain device list and supported DRM information of domain devices. One or more domain keys are a result of domain upgrades performed by the RS. Domain generation counter indicates the number of upgrades performed on the domain. Domain is upgraded when any one of the domain members is found to be revoked or compromised. After domain creation, RS provides domain information *I* to HDM. The domain key should not be revealed even to the domain owner and should be securely stored by the HDM DRM agent inside the TPM. When a device leaves the domain, the HDM sends an updated domain key to the existing domain members. In addition to that, HDM also do domain content management. It securely stores and provides purchased domain licenses to authorized domain members. It can also track the domain content usage of its domain members by collecting their usage logs and sending to the LCC.

2.3 Initial Setup, Trust and Security Assumptions

All the parties involved in the architecture have to register to the RS by sending their public key certificates to RS. For end devices, RS forwards the certificates to its supported registered CPs. The trusted DRM agent of one CP will be installed in the device. For HDM devices, a trusted agent called HDM DRM agent will be installed after successful authentication. That agent is responsible for secure content distribution to authenticated home domain devices. For LDM, RS checks whether LDM is with trusted platform module and trusted LDM DRM agent. LDM DRM agent is a server side program that has two main functional modules called *Media Management Module and Content Provider Support Module* as shown in Figure 1. Media Management Module of the LDM is responsible for media and license translation functions. Content Provider Support Module is used to get the required information about a registered CP such as Content format and encryption mechanism and signature scheme used. RS checks LDM DRM agent's trust level using TPM module's remote attestation feature. After testing its software integrity level, the RS can certify the LDM DRM agent as a trusted agent. A certificate that contains its general description about its service and its security properties signed by RS is also generated after successful authentication.

2.4 Content Packaging and License Generation

In different DRM régimes, an encrypted content is packaged using their own content packaging format and stored securely in the content owners' CSs. Different CPs generate usage licenses for each content by using their supported REL formats for end users. In our architecture, each CP that is contractually bound to LDM produces T-licenses as well as usage licenses. T-License is similar to the redistribution license of [14] but it contains permission and constraints for translation along with redistribution. The T-license includes ID of License Issuing Entity, Content ID, ID of license receiver, Permission and constraints to distribute and issue usage licenses to end users with or without translation of content, Valid Period of license, Translation parameter field and a concatenated Usage license. An authentic LDM can produce usage licenses, with usage rights *R* to use content, Content ID, *CEK1* to decrypt the content, according to permission and constraint in the T-license.

Among the constraints based on time, count and region, we use count based constraints in T-licenses. For example, for a T-license with a redistribution count = 1000 and translation count= 200, the LDM can distribute translated content for 200 counts and original content for 800 counts. Translation parameter field includes IDs of destination DRMs and other parameters such as Key Seeds S used to regenerate new CEKs with appropriate KDF function for encryption of translated content. The number of seeds provided in the T-license is equal to the number of allowed destination DRMs in the T-License. Upon LDM's T-license request, CP authenticates and attests the LDM's DRM state using remote attestation. After that, they establish a symmetric session key J by which CP encrypts T-license and sends to LDM. LDM checks the license and if the translation along with redistribution is allowed, *Content Translation and Packaging module* of LDM DRM agent does content translation and license generation according to T-license constraints and parameters. It truncates the usage license part from the T-license. Let original usage license be Lic: A. It extracts CEK1from Lic: A. The content is then decrypted and transcoded into the destination formats allowed in the T-license. Each of the new translated contents are encrypted with new CEKs generated using the seeds provided in the T-license for each DRM formats. For example, for original content X in DRM A format, it gets CEK1 from usage license and generates new CEK2s for B and C formatted content as CEK2$_B$ = KDF (CEK1, S$_B$), CEK2$_C$ = KDF (CEK1, S$_C$) where KDF = a key derivation algorithm supported by importing DRM regime, CEK1 = content encryption key for original content format, CEK2$_I$ and S$_I$ = newly generated CEK and Seed for DRM regime I. Then translated contents are encrypted with the respective CEK2s.

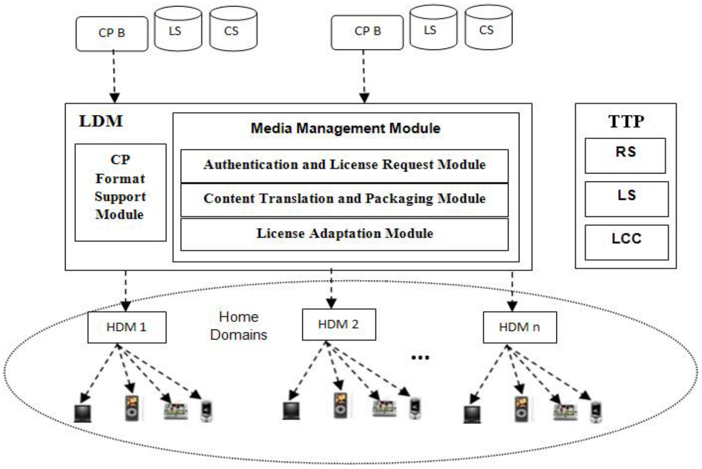
CP B
LS
CS
CP B
LS
CS
LDM
CP Format Support Module
Media Management Module
Authentication and License Request Module
Content Translation and Packaging Module
License Adaptation Module
TTP
RS
LS
LCC
HDM 1
Home Domains
HDM 2
...
HDM n

Fig 1: Secure Domain Architecture for Interoperable Content Distribution

Finally, *License Adaptation Module* translates the original license to usage licenses with allowed different DRM formats and adds respective CEK2 and translated usage rules. The generated new and original usage licenses are encrypted with the device specific key K which is stored by encrypting with the non-migratable asymmetric key pair P of TPM. Those licenses are stored in TTP License Server under its associated content provider's ID. Since Key P is bound to an environment configuration state as mentioned in section 2.2, only trusted LDM DRM agent can access that key.

2.5 Content and License Acquisition

HDM sends license request with supported DRM format since it has all information of its domain devices. HDM and LDM will mutually authenticated using PKI authentication and establish a Symmetric session key S. To access the Licenses from LS, the LDM agent needs access to Key *K*. TPM checks PCR value of that agent and its environment. Only when the PCR value is as expected, the agent can access Key *K*. After getting access to K, it decrypts the license with K and encrypts those licenses with the domain key *DK* and concatenate those licenses as shown in (1).Those licenses are sent to the HDM of the requested domain by encrypting with Key *S* via secure channel.

$$\begin{gathered}(Enc\ \{Usage\ LicenseB\}_{DK} \| Enc\ \{Usage\ License\ C\}_{DK}, \\ Enc\{Content\ XB\}_{CEK2_B}, Enc\{Content\ XC\}_{CEK_{2C}})_S \qquad (\mathbf{1})\end{gathered}$$

Upon receipt of those encrypted set, HDM will store it in its Content Server. For each requested domain device, HDM DRM agent sends the encrypted content and license of the device's supported DRM type by wrapping with public key *(PK)* of authorized device. For example, for domain device D_B with supported DRM format B, HDM will send $Enc\big(Enc\ \{\ Usage\ License_B\}_{DK}, Enc\{Content\ X_B\}_{CEK_{2B}}\big)_{PK_{DB}}$.

3. Relevance of the Proposed Architecture

Consumers usually prefer to use DRM-free contents so that they can flexibly use the contents in all their devices at anytime and anyplace. However, content providers or owners do not prefer to provide DRM-free content since it can lead to illegal content distribution as well as loss of control on their contents. Our architecture tries to achieve a tradeoff between these two extremes, allowing consumers to use any DRM content in any devices in their domain at anytime and anyplace just by connecting to their home domain manager remotely or locally. Content providers or owners can also extend their market share (without losing control on their content) as their content can be played in any device supporting a different DRM-regime.

The proposed architecture can serve as local content distribution architecture for, but not limited to, organizations or apartment buildings. In an organization or an apartment building, efficient and secure distribution of contents from different content providers can be achieved by using a LDM that handles content distribution and negotiation for its domains inside the organizations or apartment building and a HDM that controls the content flow within each department or home.

4. Conclusion and Future Work

The proposed interoperable DRM architecture allows secure sharing and accessing of digital content in multiple authorized domains and does not need to assume the middle entity as a trusted entity. All the devices can get translated content locally without having to request each time separately for translation of content, thus significantly reduce network resource requirement by end devices. Controlled illegal distribution and translation of content is also achieved with LDM DRM agent and T-licenses from respective CPs. Our architecture also supports violation detection of malicious LDM and home domain devices though we do not provide detail mechanisms in this paper. We introduced the T-License concept and provided some key management solution that prevents possibility of content leakage and illegal content translation and distribution by the middle entity. Our future work will be providing privacy preserving mechanisms and efficient distribution of contents with different format to respective domain devices.

References

1. Joshua Duhl, Susan Kevorkian: Understanding DRM Systems, IDC White Paper (2001).
2. William Rosenblatt, William Trippe, Stephen Mooney: Digital Rights Management: Businessand Technology, Paperback (2001)
3. J. Bormans, K. Hill : MPEG-21 Overview v.5, ISO/IEC JTC1/SC29/WG11/N5231, International Organisation for Standardization, Shanghai (2002)
4. R. H. Koenen, J. Lacy, M. Mackay, and S. Mitchell. The long march to interoperable digital rights management. Proceedings of the IEEE, 92: 883{897, 2004}
5. Coral consortium whitepaper, Tech. rep., February 2006. <http://www.coral-interop.org>
6. Kravitz, D.W., Messerges, T.S.: Achieving Media Portability through Local Content Translation and End-to-End Rights Management, DRM 2005, pp. 27–36 (2005)
7. Taban, G., Cardenas, A.A., Gligor, c.d.: Towards a Secure and Interoperable DRM Architecture. In:ACM Workshop On Digital Rights Management, pp. 69–78 (October 2006)
8. Yeonjeong Jeong, Jihyun Park, Jeonghyun Kim, Kisong Yoon: DRM Content Adaptation Scheme Between Different DRM Systems for Seamless Content Service. ICME 2007: 867-870.
9. Serrão C., Dias M., Delgado J., “Bringing DRM interoperability to digital content rendering applications”, In CISSE05, Univ. Bridgeport, USA, 10-20 December 2005
10. Combining DRM with Trusted Computing for effective information access management.
11. R. Safavi-Niani, N. Sheppard, and T. Uehara, “Import/Export in Digital Rights Management,” DRM, 2004, pp 99-110
12. Trusted Computing Group. Trusted Computing Group, 2004.
13. Brenton Cooper and Paul Montague, “Translation of Rights Expressions,” Third Australasian Information Security Workshop (AISW2005), Conferences in Research and Practice in Information Technology (CRPIT), ACS, vol. 44, Jan. 2005, pp. 137-44.
14. A. Sachan, S. Emmanuel, A. Das, M.S. Kankanhalli, Privacy Preserving Multiparty Mulilevel DRM Architecture, CCNC 2009, January 2009.