A License Audit Model for Secure DRM Systems in IP-based Environments

Ui Jin Jang*, Hyung-Min Lim* and Yong-Tae Shin*

Abstract—Communication devices aim to provide a multimedia service without spatial or temporal limitations in an IP-based environment. However, it is incapable of allowing for fair use by consumers who legally buy content, and damages provider contents through the indiscriminate distribution and use of illegal contents.

The DRM system that emerged to solve this problem cannot protect licenses stored on communication devices, and manage licenses by redistribution. This paper proposes a license audit model, which checks for illegal access, modification and redistribution, and reports alert logs to the server.

Keywords—Digital Forensic, DRM, IP-Based Network

1. INTRODUCTION

In an IP-based environment, all the communication devices should provide multimedia services without temporal or spatial limitations. However, it does not allow for fair use by users and a great deal of damage results from the indiscriminate distribution and use of unlicensed contents.

The DRM system introduced to solve such problems still has a problem in that the protection of licenses stored in the devices and the redistribution of these licenses are not managed. Usage in the license life cycle is not managed, because this system depends on protection by device authentication or an encryption algorithm.

To solve this problem, the license audit model in this paper proposes to collect evidence and provide post-management for access interception of unlawful users by auditing misuse behavior such as unlawful access, modification and redistribution of licenses by users, and reporting alert logs generated by unlawful attempts.

This paper is organized as follows. In Chapter II, the platform technology and research trends for secure content protection is described; in Chapter III, the design of the license audit model is described; in Chapter IV, the protocol analysis and implementation is described; Finally, in Chapter V, the conclusion is drawn and future directions are described.

Manuscript received May 6, 2010; accepted May 28, 2010.

Corresponding Author: Hyung-Min Lim, Yong-Tae Shin

* Dept. of Computer Engineering, Soongsil University, Seoul, Korea (neon7624@gmail.com, atskyo@gmail.com, shin@ssu.ac.kr)

2. RELATED WORK

2.1 Digital Forensics

Digital forensics may be defined as “the method to scientifically deduce and validate digital evidence, which is needed to settle or validate the matter of fact of various actions by digital sources including information processing devices, for preservation, gathering, validation, identification, analysis, interpretation, documentation, and presentation”, and may also be defined as “a series of actions to submit legal evidence through the process to collect, analyze, and preserve information from digital sources such as computer systems and networks to obtain legally evidential materials in relation to actions performed through media such as digital devices including computers[1, 2].” Recent advances in computer forensics include procedures to prevent crimes targeting computers and networks. It also includes a means to submit digital evidence for making judgments. This involves collecting digital evidence through an appropriate process at the time a crime occurs and processing the evidence to form legally effective evidence for civil/criminal responsibility.

2.2 DRM

DRM is the technology for continuous protection of contents rights over the contents life cycle, such as creation, storing, distribution, use and disuse of contents.

The existing DRM technology protects contents stored in a device using encryption, authentication, content packaging, rights expression language, and tamper resistance technology.

However, besides the existing DRM technology, protection of streaming contents, domain rights management, and inter-compatibility between DRM technologies is supported for contents protection based on IP-based environment[3].

The DRM technology for the protection of streaming contents is classified into two types; multicast contents providing simultaneous services for many users and VOD contents servicing one-to-one users. At present, standardization is being advanced with ISMA, OMA, DVB, etc[4].

The inter-compatibility between DRM technologies guarantees inter-compatibility between different technologies. DMP and MPEG-21 are advancing standardization and ETRI is advancing EXIM technology, which is compatible with different DRMs[5]. The management technology of domain rights permits the free use and distribution of contents between domains(devices) for users, supporting convenient contents use by guaranteeing private copying, and its standardization is advancing with OMA, MPEG-21, DVB, DMP, etc[6].

3. CONFIGURATION OF PROPOSED MODEL

This section describes the license audit model proposed in this paper. The model is configured with a server and client. The server is configured with a Forensic Manager as a countermeasure against unlawful use of license, a License Server, a License Issuing Server, and a Forensic Database, and the client is configured with a DRM Client module to manage the use of contents and a Forensic Agent to monitor the status of the license and audit security[7]. The configuration and compatibility between the configuration objects of the license audit model are shown in Fig 1.

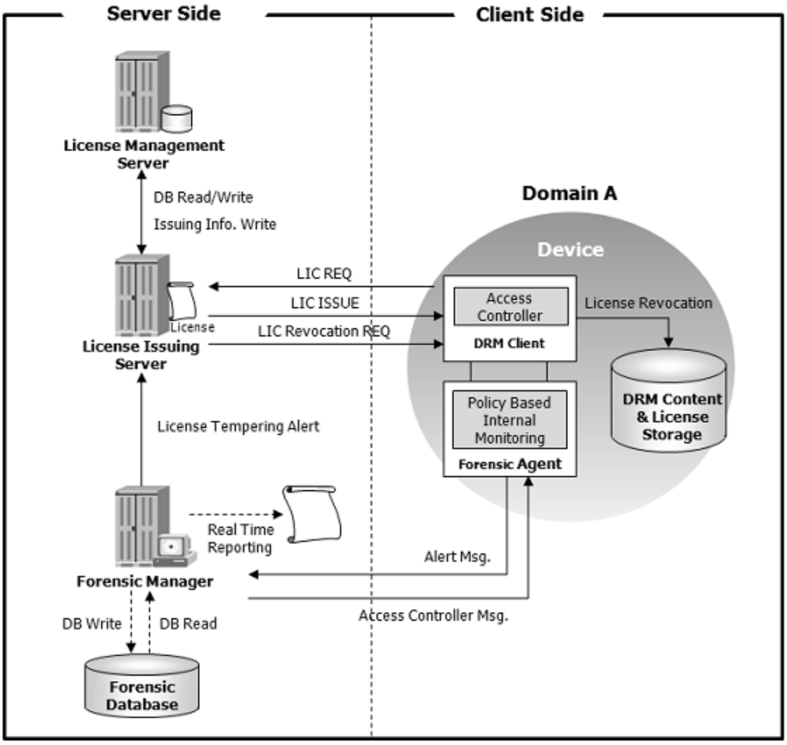


Fig. 1. Configuration of license audit model

Forensic Manager decentralizes the agent's access and is responsible for storing security audit logs in the database and processing real-time statistics transactions.

In addition, Forensic Manger performs real-time monitoring and analyses of the alert logs, which are collected in Forensic Database by security level, in order to obtain evidence of infringement of digital contents and licenses possessed by users. Forensic Manager generates and manages the related and readable reports based on the obtained evidence.

Forensic Manager analyzes the collected logs in consideration of the accumulated security threat and, if an event is generated at the level requiring a countermeasure, sends a control signal to limit the use of licenses or digital contents to the Forensic Agent. Forensic Agent transmits the corresponding information to the Access Controller of the DRM Client in order to limit the use of the corresponding licenses or digital contents.

4. DESIGN OF PROPOSED MODEL

The proposed model performs copyright protection and license management for media contents stored on user devices in an IP-based environment. In order to protect personal information, the information about who will be monitored should be sufficient notice to the user of contents and monitored in case of obtaining user consent. A sufficient notice should be given to the content users regarding the information to be monitored in order to protect personal information and it should be monitored only under user consents.

The required log and evidence gathering procedures are described in this section.

4.1 Log Gathering Procedure

DRM Client to play content and Forensic Agent (1) to monitor the status of the license and perform a security audit are operating in the user device.

$$Forensic\_Agent=\{Msg\_Type||Directory||License\_File\_Name||Active\_Type\} \quad (1)$$

Forensic Agent runs from the device boot time to the termination time, and generates License HASH Profiles (2) as countermeasures against unlawful forgery/alteration of the licenses stored in the device. This is the profile that confirms the integrity of the issued licenses.

$$License\_Hash\_Profile=\{ID||Time||Type||Hash\} \quad (2)$$

The license file and License HASH Profile are periodically compared in order to inspect the integrity of the licenses; if the two values are inconsistent, the license is deemed to have been attacked by the account of the user accessing the current device and an alert is generated. Forensic Agent has a rule-set consisting of the system call signature information based on the attack scenario of licenses for the security audit of the license. When there is a system call for access to, modification of, addition to, deletion from, moving to, copying of, or file opening in the folder, other than a reliable DRM system, where licenses are stored, the call is compared in terms of the signature of the rule-set, and the alert log (3) of the corresponding signature is generated[8, 9].

$$Alert\_Log=\{Phy\_Addr||Logi\_Addr||Account||Date||RS\_ID||ID\_type||Alert\_Type||RS\_Class\_Type||RS\_FSID\} \quad (3)$$

To use media contents, DRM Client should obtain usage rules (count, period) and rights (Contents Encrypt Key) after accessing the corresponding license file. To access the license file and use a license, an Access Controller message (4) is transmitted to Forensic Agent. After use of the license, the same type of message is transmitted to Forensic Agent which prevents an alert being generated as an exception during the security audit.

$$Access\_Controller\_Msg=\{Time||User\_Account||License\_ID||Msg\_Type||Rev\} \quad (4)$$

When the events “HASH Profile Miss-Match” and “Rule-Set Signature Identity” are generated, Forensic Agent generates an alert log in the form of an Alert Event Message (5).

$$Alert\_Event\_Msg=\{Date||License\_ID||User\_Account||Alert\_Class\_Type||Alert\_Signature\_ID\} \quad (5)$$

The alert log is generated when the status of the user is offline, and it is encrypted and stored with the public key of Forensic Management Server and transmitted to Forensic Management Server when the device is in online status for VOD or streaming services. Forensic Manager stores the received alert log in the alert table of the Forensic Database and accumulates and manages the log by the level of security threat set for each alert log in the Abnormal User Table

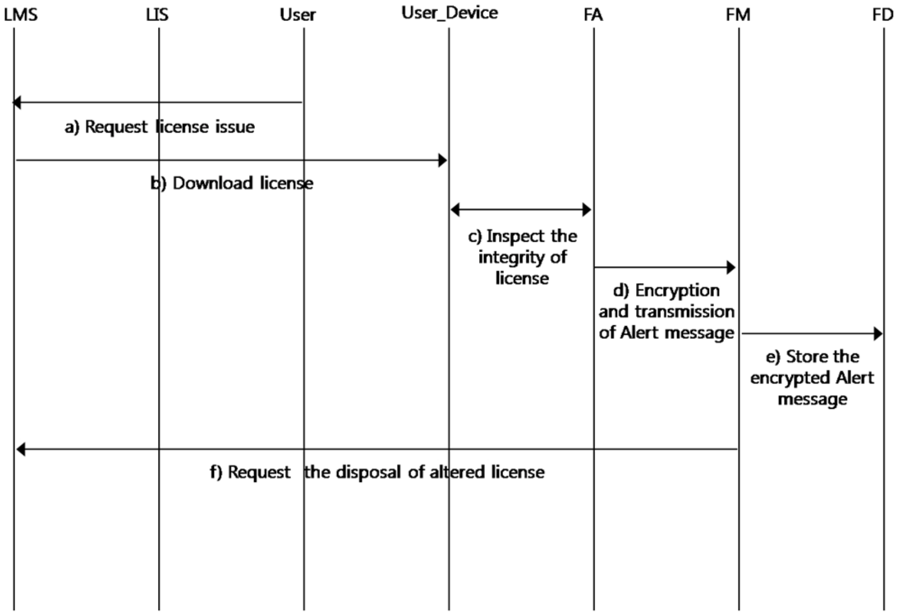

LMS
LIS
User
User_Device
FA
FM
FD
a) Request license issue
b) Download license
c) Inspect the integrity of license
d) Encryption and transmission of Alert message
e) Store the encrypted Alert message
f) Request the disposal of altered license

Fig. 2. PIP Model

in the account of each reported user. To evaluate the proposed model, the security level is set to the top-grade when the security status is at the license counterfeiting and tampering, and is set to a random grade when the status is otherwise. When the security threat level has accumulated to the point where it exceeds the threshold set by the manager of Forensic Manager, the account and license of the corresponding user is disposed for re-issuance of the license through inter-compatibility between License Issuer Server and License Management Server.

Proper use of the contents by the user involves re-issuance and re-registration of the license. The Forensic Agent requests from License Management Server the license of the contents desired by a user, and the integrity of the downloaded license is periodically inspected by making a comparison with License HASH Profile. If Forensic Agent suspects that the license has been altered, it generates an alert and performs encryption for safe reporting and management to Forensic Manager. The license, which got confirmed alteration, performs the disposal scenario and the license may properly be used through the re-issuance process.

The log gathering procedure of an altered license is shown in Fig. 2[10].

4.2 Evidence Gathering Procedure

The proposed model gathers evidence for unlawful user access to the digital contents and license through inter-compatibility between Forensic Agent and Forensic Manager. The inter-compatibility between Forensic Agent and Forensic Manger enables safe management and the sending and receiving of messages by using an agreed security protocol. The operating procedure between Forensic Agent and Forensic Manger is shown in Fig. 3.

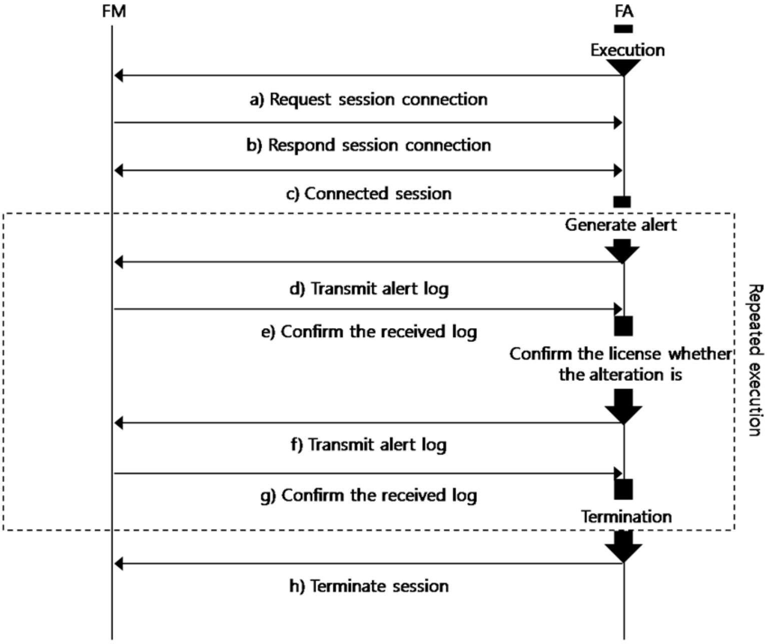
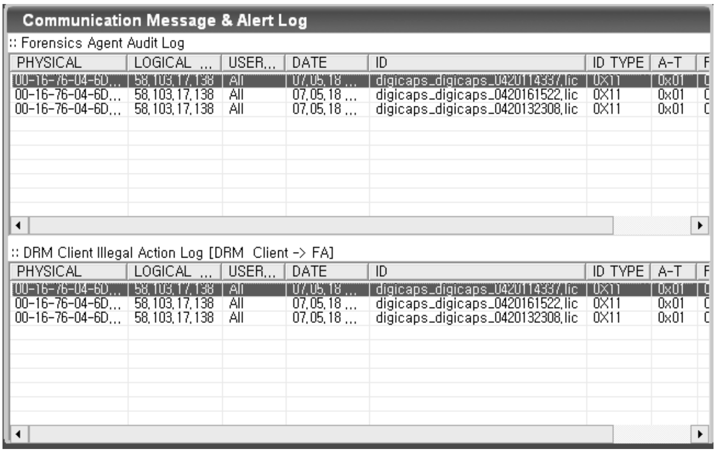

FM
FA
Execution
a) Request session connection
b) Respond session connection
c) Connected session
Generate alert
d) Transmit alert log
e) Confirm the received log
Confirm the license whether the alteration is
f) Transmit alert log
g) Confirm the received log
Termination
h) Terminate session
Repeated execution

Fig. 3. Inter-compatibility between Forensic Agent and Forensic Manager

4.3 Model Verification

In order to test the performance of the model proposed in this paper, there is a compulsory change in the count among the usage rules of DRM License from 50 to 100.

Forensic Agent transmits an alert log to Forensic Manager in case of detecting a license forgery and tampering activity and reports it to the corresponding DRM client. The accumulated alert log reported to the DRM Client is confirmed by Forensic Agent, as shown in Fig. 4.



Communication Message & Alert Log

:: Forensics Agent Audit Log

PHYSICAL	LOGICAL ...	USER...	DATE	ID	ID TYPE	A-T	F
00-16-76-04-6D...	58.103.17.138	All	07.05.18 ...	digicaps_digicaps_0420114337.lic	0X11	0x01	C
00-16-76-04-6D...	58.103.17.138	All	07.05.18 ...	digicaps_digicaps_0420161522.lic	0X11	0x01	C
00-16-76-04-6D...	58.103.17.138	All	07.05.18 ...	digicaps_digicaps_0420132308.lic	0X11	0x01	C

:: DRM Client Illegal Action Log [DRM Client -> FA]

PHYSICAL	LOGICAL ...	USER...	DATE	ID	ID TYPE	A-T	F
00-16-76-04-6D...	58.103.17.138	All	07.05.18 ...	digicaps_digicaps_0420114337.lic	0X11	0x01	C
00-16-76-04-6D...	58.103.17.138	All	07.05.18 ...	digicaps_digicaps_0420161522.lic	0X11	0x01	C
00-16-76-04-6D...	58.103.17.138	All	07.05.18 ...	digicaps_digicaps_0420132308.lic	0X11	0x01	C

Fig. 4. The overall structure and process for PIP

5. RESULTS

In the existing DRM environment, the problem is that when a license is distributed using the encryption algorithm, tracking and managing the distribution of the contents and license is difficult. There is a high chance that security threats may be generated, because users may easily achieve access to the contents and licenses stored in the device.

The model proposed in this paper can efficiently control how security elements are used for dealing with user attacks exploiting security holes of licenses and contents and the unlawful distribution of contents and licenses. Also, unlawful use of licenses and contents may be prevented in advance, protecting users' licenses and allowing fair use of contents. For secure management of re-issuing licenses in an IP-based environment, a forensic algorithm should be applied and other DRM systems cannot satisfy this.

Therefore, to address threats such as counterfeiting or tampering of DRM licenses, this paper proposes a license audit model which could be applied to DRM. Table 1 shows the comparison of the recommended model with the other DRM systems.

Tabel 1. Comparison of the recommended model with the other DRM systems

Requirements	OMA DRM	WMRM	Proposed model
License information gathering through a consistent forensic procedure	x	x	○
Automated evidence collection	x	x	○
Support of the inter-compatibility for information gathering by license policy	x	x	○
Support of control of access to licenses	x	x	○
Support of authentication of devices	○	○	○
Countermeasure against unlawful use of license	x	○	○
Reporting the status of use of license	x	x	○

6. CONCLUSION

In this paper, a model is proposed as a countermeasure against license attack by managing the distribution life-cycle of licenses from issuance to disposal through inter-compatibility between Forensic Agent or Forensic Manager and the DRM System, and by managing unlawful security threats to licenses.

The proposed model provides flexible security for licenses in future ubiquitous environments. Also, unlawful distribution of digital contents is prevented. Using more advanced technology than the existing DRM, the creation rights of copyright holders may be guaranteed with the use of license audit logs and contents as legal evidence, based on the function of non-repudiation about unlawful distribution after generation of an event. Also, a mechanism is provided to guarantee fair use in various digital devices in the future.

We need to develop a real implementation model capable of effective execution, to realize message configuration between the configured objects of the license audit model and research an encryption algorithm.

REFERENCES

[1] Kevin Mandia, Chris Prosise, Matt Pepe, "Incident response and computer forensic, Second Edition," McGraw-Hill, 2003.

[2] Warren G, Kruse II, Jay G.Heiser, "COMPUTER forensic: Incident Response Essentials," Addison Wesley, 2001.

[3] Qiong Liu, Reihaneh Safavi-Naini and Nicholas Paul Sheppard, "Digital rights management for content distribution," AISW2003, 2003.

[4] OMA, "OMA DRM Requirements Version 2.0," 2004.

[5] MPEG-21 Overview v.5, ISO/IEC JTC1/SC29/WG11 N5231, Shanghai, 2002.

[6] DMP, "TIRAMISU(IST-2003-506983) DRM Requirements," 2004.

[7] RFC 3227, "Guidelines for Evidence Collecting and Archiving," http://www.faqs.org/rfcs/rfc3227-.html. 2002.

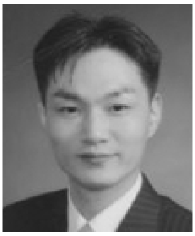
[8] Mariusz Burdach, "Forensic Analysis of a Live Linux System I," http://www.securityfocus.com/infocus/1769. 2004.

[9] Mariusz Burdach, "Forensic Analysis of a Live Linux System II," http://www.securityfocus.com/infocus/1773 , 2004.

[10] Seok-Hee Lee, "A Study of Memory Information Collection and Analysis in a view of Digital forensic in Window System," Center for Information Technologies, Korea University, 2006. 2.

Ui-Jin Jang

She received her BS and MS degrees in Computer Engineering from Soongsil Univ. in 1999 and 2002, respectively. During 2002-2006, she worked in DigiCAP Inc. to develop the DRM, CAS solutions. And now she is undertaking a doctorate course as a member of the computer communication lab at Soongsil Univ. Her research interests include Access Control, CAS and network security.



Hyung-Min Lim

He received his BS and MS degrees in Computer Engineering from Soongsil Univ. in 2001 and 2003, respectively. He is undertaking a doctorate course as a member of the computer communication lab at Soongsil Univ. His research interests are in the area of u-City and network security.

Yong-Tae Shin

He received a Ph.D. degree in Computer Science from Iowa Univ. in 1994. He has been a professor at Soongsil Univ. since 1995. His research interests are in the area of Computer Network, Group Communication, Distributed Computing, Internet Protocol, and E-Commerce technologies.