Originator Control in Usage Control*

Jaehong Park

Laboratory for Information Security Technology
ISE Department, MS4A4
George Mason University, Fairfax, VA 22030
jaehpark@ise.gmu.edu, www.list.gmu.edu/park

Ravi Sandhu

SingleSignOn.Net, Inc. Reston, VA.
and
George Mason University, Fairfax, VA
sandhu@gmu.edu, www.list.gmu.edu

Abstract

Originator Control is an access control policy that requires recipients to gain originator's approval for re-dissemination of disseminated digital object. Originator control policies are one of the generic and key concerns of usage control. Usage control is an emerging concept which encompasses traditional access control and digital rights management solutions. However, current commercial Digital Rights Management (DRM) solutions lack enforcement of access control policies such as role-based access control (RBAC), mandatory access control (MAC), discretionary access control (DAC) and originator control because their control of access to digital object is mainly based on payment.

In this paper, we attempt to combine originator control policies and usage control. Then we show how this can extend traditional originator control solutions to enforce access control policies even outside of a local control environment where a central control authority is not available. License and ticket concepts are proposed and used for originator control in usage control. Also, we define seven different solution approaches to deal with various dissemination situations. In addition, we discuss some published DRM solutions and relate these to our solution approaches.

1. Introduction

Recently we have seen that peer-to-peer (P2P) distribution of digital information without any rights holder's control over the use of the digital information has caused many copyright related problems. New solutions based on superdistribution paradigm have been proposed to provide mechanisms for controlling access to digital information after dissemination. These technologies are known as digital rights management (DRM). Current DRM solutions have been employed mainly for controlling payment-based access to distributed digital information. Because current DRM solutions mainly pertain to payment-based dissemination, they lack access control features that should be considered for payment-free digital object dissemination. Note that, payment-free is different from zero payment case of payment-based dissemination. In zero payment, authorization is not required and everyone can access the digital object free of charge. Whereas, in payment-free dissemination, payment does not matter, but some other requirements such as clearance, role, ownership or originator's approval are required for authorization.

The notion of usage control (UCON) is emerging as a promising means of controlling and managing usage of digital objects [12]. It is a broader concept than DRM or access control because it covers both payment-based and payment-free type of digital information dissemination, as well as the traditional area of access control. One of the key concerns of UCON is how to control re-dissemination of disseminated digital objects. Originator Control (ORCON) is an access control policy that requires recipients to gain originator's approval for re-dissemination of an originally disseminated digital object or a new digital object that includes originally distributed digital objects.

UCON is a relatively new approach for next generation information security solutions, while ORCON has been discussed for more than a decade. Nevertheless, ORCON and UCON are alike in many aspects. In ORCON's perspective, by using UCON technologies, ORCON policies can be enforced in more versatile and flexible ways compared to the traditional ORCON solutions because blending ORCON with UCON enables control of dissemination and re-dissemination outside of a closed system environment where central control authority such as a reference monitor is not available. In UCON's perspective, ORCON is a "must have" policy because ORCON policy is one of the generic access control policies that are applicable to UCON solutions. Unlike other access

* This Research has been partially supported by National Science Foundation (NSF).

control policies like RBAC, MAC and DAC, ORCON is naturally applicable for both payment-free and payment-based dissemination control.

Regardless of this tight relationship, ORCON has not been examined carefully in current DRM solutions because of the lack of immediate commercial interest. We believe investigating UCON with ORCON policy in mind can provide a promising way to control and manage digital information dissemination not only for non-commercial, payment-free environment such as the intelligence community or the commercial B2B environment, but also for commercial, payment-based dissemination.

In section 2 and 3, we explain UCON and ORCON technologies briefly. In section 4, we first define license and ticket concepts which are key elements in the UCON solution to implement ORCON policies. Then, we demonstrate how ORCON in UCON solutions can extend traditional ORCON to control even outside of the local control domain area and identify variations of ORCON policy enforcement in UCON solutions by using license and ticket. Finally, in section 5, we relate some recent DRM works by other authors to our ORCON in UCON solutions.

2. Usage Control

The UCON concept is originally based on the superdistribution paradigm. In superdistribution, electronic information is available freely, but access to the information is controlled [3]. In UCON, digital information is encapsulated into a cryptographically protected electronic container called a *Digital Container*. This encapsulated digital information is only accessible by using special application software or hardware called a *Virtual Machine*, with approved access rights that are stored in a *Control Set* [11]. A Control Set can be thought of as our license.

2.1 Virtual Machine

The *virtual machine* is a trusted, tamper-resistant, recipient-side application software or hardware component that runs either standalone or on top of a vulnerable computing environment such as a PC and employs control functions to provide the means to control and manage access and usage of digital information. The existence of a virtual machine on the recipient side is one of the most influential factors of the architecture, and it provides the foundation of usage control technologies. A virtual machine works as a reference monitor of a trusted computing base. However, implementing mobile agent like virtual machine that can be trustable even in malicious host is still not easy. To make UCON technologies more reliable, robust technologies resistant against attacks are required. In UCON systems, digital information can only be accessible within the virtual machine. By using a virtual machine, we can specify the access privileges. For instance, we can enable or disable the print function, save function, and save-as function within the virtual machine.

2.2 Control Set

The *control set* is a list of usage rights that is followed by the virtual machine to control a recipient's access and usage of digital information. Previously, Park et al [11] proposed three styles of control sets as follows. A *fixed control set* is hardwired into the virtual machine and applies uniformly to all digital information documents and all users. An *embedded control set* is inextricably bound to each digital document and is carried along with it. An *external control set* is separate and independent from the digital document and can be transported separately or together with the document. Embedded and external control sets can apply different controls to each document and each user.

2.3 Digital Container

The *digital container* [9, 14] is another key element of UCON technologies. A digital container is a tamper-resistant electronic envelope that is designed to protect digital information and control usage by wrapping it with cryptographic mechanisms. Digital containers can be implemented using either a control set or watermarks for controlling usage rights. Control set technology is a typical configuration for digital containers while watermarking approaches are optional.

2.4 Control Center

A *control center* exists for controlling and managing the access rights, usage rules, and even usage history. A control center holds security policies (control sets) that govern usage of digital information and holds a database of senders and recipients. Generally, the purpose of the control center is to provide designated users access rights, so users can access the digital information. To achieve this, client-side application software (the virtual machine) will check the control set, and if necessary, it will communicate with the control center for additional information such as granting access rights to certain digital information. In the commercial sector, the control center can also be responsible for payment functions, where access to the digital information can be granted or revoked based on payment.

3. Originator Control

In the spectrum of access control policies, Mandatory Access control (MAC) and Discretionary Access Control (DAC) reside at each end. Between MAC and DAC ends

of the spectrum, there are areas where neither MAC nor DAC are applicable. ORCON is one of the access control policies that belong to this middle ground. ORCON is similar to MAC in that access restrictions on original objects are propagated to derived objects. However, ORCON is different from MAC in that policies are modifiable on a subject/object basis, while in MAC policies are uniform across all subjects and objects. Also, ORCON is similar to DAC in that policies are changeable by the original owner or originator of the object. However, ORCON is different from DAC in that control privileges on an object can be modifiable only by the originator of the object, while in DAC the owner (recipient) of a derived object can often also change control privileges on the object or on copies of the object. In some sense, DAC can be viewed a special case of ORCON where the originator delegates all the rights to recipients. The term owner and originator are used in this paper as defined by [5].†

In the paper world, ORCON is one of the control markings for restriction of document distribution defined by the Director of Central Intelligence Directive (DCID) 1/7 [4]. A distributed document marked ORCON can only be distributed with the approval of the originator of the document. Traditional ORCON solutions [1, 5, 10, 13] try to automate the paper world's originator controlled dissemination policies. In the proposed solutions, ORCON policies typically utilize some form of non-discretionary access control list [2]. The implementation of this non-discretionary access control list, however, limits the ability to enforce ORCON policies to a closed control environment.

Traditional ORCON solutions are focused on the enforcement of ORCON access control policies within a control domain. A control domain implies a system environment that facilitates a central means to control access of any subject within the domain to digital information objects. These solutions have tried to enforce access control policies in a centrally controlled manner. They normally set centrally controlled policies for a whole domain and all of the users have to behave within the boundaries of the policies. These solutions may run on either mainframe systems or client-server systems.

Figure 1 illustrates the structure of a traditional ORCON solution. In this schematic, the originator creates a digital object marked with "ORCON" and makes it available to subject A by setting appropriate access control policies that are tied to a subject and object relationship. If subject A wants to allow subject B to access the received digital object, the control authority (which is effectively a reference monitor) must check if subject B's access to the object is allowed or not by the non-discretionary access control lists. In this way, the originator can always control recipient access to the distributed digital object.

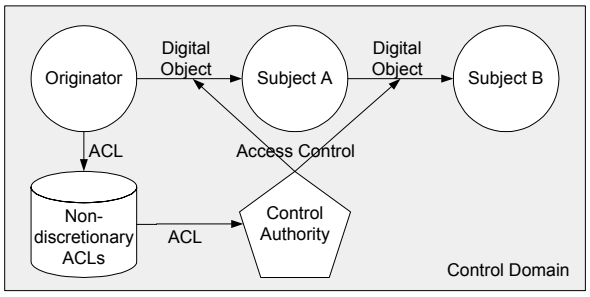


Figure 1. Traditional ORCON solutions

4. ORCON in UCON

UCON is different from access control policies. The usage rights of UCON are more versatile and finer-grained than privileges of traditional access control policies. UCON can be viewed as a broader concept than access control. UCON solution may include various kinds of access control policies. ORCON is one of the most tightly related access control policies to UCON solutions. ORCON and UCON are similar in their goals. Both focus on original distributor's controls on the usage of distributed digital objects. While UCON deals with delegation of control privilege and controlling re-dissemination of digital objects, ORCON considers only re-dissemination of distributed digital information objects. In UCON, we can implement other access control policies such as MAC, DAC and RBAC. In practice, the re-dissemination control of ORCON policies can be enforced by allowing access to the digital object with the originator's direct or indirect approval. In UCON, ORCON policies can be achieved in different ways by using licenses and tickets. In the next sub-sections, we define license and ticket concepts and demonstrate how ORCON in UCON can support control of digital information re-disseminations. Then we define different variations of ORCON in UCON solutions.

4.1 License and Ticket

License and ticket are used for propagation of usage rights such as read, print, dissemination/re-dissemination rights, etc. They are key concepts needed to implement ORCON policies in the UCON solution. Commercial DRM solutions also use some form of license or even tickets. However, most of these solutions have used them for payment-based dissemination and usage. There are few, if any, solutions for payment-free dissemination where payment does not matter and access control policies are resolved. In payment-free dissemination, authorization requires certain access control policies such as MAC, DAC, RBAC or ORCON. By using license and ticket, we can enforce ORCON policies for digital information

† Please note the distinction between owner and originator. "Owner refers to the subject that is responsible for the creation of an object and is authorized to change DAC permission on the object. Originator is responsible for the data contained in an object and for determining to whom the data can be released." [5]

dissemination. The following sections briefly describe the concepts of license, license-granting ticket, and license-requesting ticket.

4.1.1 License

A license is a digitally signed certificate that includes all the usage rights information of qualified recipients on specified digital objects and allows the user access to the digital objects through a Virtual Machine. Only users with a qualified license are allowed to access digital objects. With ORCON in UCON, a license has to be issued by either the originator of a digital object or third parties approved by the originator. A license may or may not include a *license-issuing privilege (LIP)*. If LIP is included in a license issued by the originator, the recipient of this primary license can issue a secondary license to a license requester without consulting the originator about the request.

4.1.2 Ticket

A ticket is a specialized license that is used either to delegate LIP or to provide the information from where the requester can obtain a license. A ticket may be used only for a limited number of times or for a limited time period and marked to be void after use. In this paper we define two different kinds of tickets: *License-Granting Ticket (LGT)* and *License-Requesting Ticket (LRT)*. The issuer of the LGT is the originator of the requested digital object (or recipients who are qualified as issuers of the LGT by the originator), while the issuer of the LRT is the original requestee (that is, the subject to whom the license requestor makes its original request). Both the LGT and the LRT may include ticket issuer, ticket recipient, license issuer and license recipient information.

A LGT always include LIP. A LGT may also include usage rights information, so it can be used when a license is issued to original requesters. By issuing a LGT, the issuer (including the originator) can allow third parties to issue licenses to further availability of the digital object on behalf of the originator or the previous issuer. LIP can optionally exist in a license. If a license includes LIP, re-dissemination is possible only to pre-defined qualifiers. However, with a LGT, approval can be reviewed case-by-case upon each license request and the distribution can be monitored. A license with LIP and a LGT can coexist, but cannot be used for the same request instance together.

LRT is a ticket that is issued by an original requestee other than originator and is used by the requester to request a license from the originator to access a digital object. The original requestee is the primary recipient from whom the requester gets the digital object information and is the subject who is asked for the license. Suppose the original requestee does not have an appropriate LGT to fulfill the request. In this case the original requestee can return a LRT to the requestor, and this LRT can be used to request a license from the originator. The originator will then decide to issue the license by checking whether the license requester is a qualified user and has a valid LRT.

4.2 Binding ORCON and UCON

While traditional ORCON solutions try to control access to disseminated digital objects centrally, our solutions of ORCON in UCON try to enforce access control policies for both centralized and de-centralized cases. As mentioned in chapter 3, traditional ORCON solutions can enforce access control policies within the closed control domain environment. However, by using the concept of license and ticket, ORCON in UCON can go further and enforce access control policies outside the control domain area.

Figure 2 shows an example of ORCON in UCON and demonstrates how ORCON in UCON solutions can enforce access control policies outside of the local control domain. Here, each recipient belongs to different control domains. The gray areas (originator's control domain and recipients' virtual machine) indicate the control areas of an originator on disseminated digital objects. Control mechanisms for dissemination and re-dissemination of the originator's digital object within the originator's control domain are exactly the same as those for the open control environment. In our solution (for both the closed and open control environments), access to the disseminated digital objects can be done only through the virtual machine. In Figure 2, the digital object is available to Subject A either directly or indirectly. The key is that Subject A needs a license to access the received digital information object. In this particular example, Subject A gets a LGT from the originator so she can issue a license to Subject B.

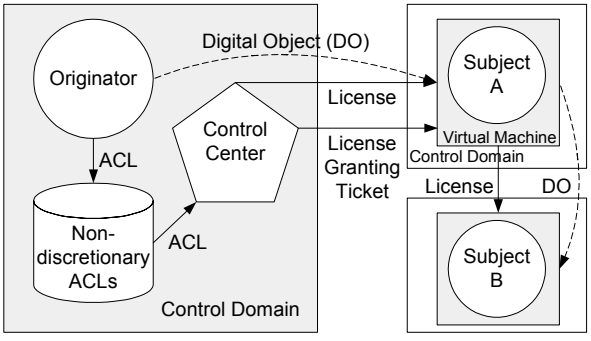


Figure 2. An example of ORCON w/ UCON

4.3 Variations of ORCON in UCON

In UCON, ORCON can be accomplished in various ways. In the following sub-sections, we identify different kinds of architectural approaches by incorporating the concepts of license and ticket in different ways. However, we are not trying to analyze every aspect of each variation. Rather, we are trying to demonstrate different approaches

by introducing different uses of licenses and tickets. The purpose or benefit of this distinction is not to show which one is better than others but to demonstrate possible approaches based on message (e.g., usage rights requests, rights approval and rights delegation information) flows, so that the approaches can be considered and included in UCON solutions to deal with various situations. In some cases, for example, an originator may want to delegate license-issuing privilege to other recipients so further requests can be handled by authorized recipients without the originator's involvement. In other cases, if requester does not have originator's contact information, she may first have to contact the provider of digital information object. Unlike traditional ORCON solutions, possession of both the digital information object and the relevant license with qualified usage rights is required to access the object.

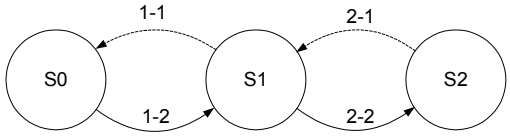
In the following figures, note that though the virtual machine is omitted for the sake of convenience, it is required for every recipient and should be used to handle all license/ticket requests of and license/ticket issuance to subjects other than the originator. In addition, the digital object is assumed available to requesters (the digital object may or may not be received directly from the requestee) and is not explicitly shown. Also, detailed configurations of the originator site are omitted since there can be many possibilities. Although LRT can be used for license/LGT requests, we consider this as a request. The following legends pertain to the figures in this section.

S0 : Originator
S1/S2 : Recipients
: LC/Ticket Request
: LGT/LRT issuing
: License issuing
1-x : Original dissemination steps
2-x : Re-dissemination steps

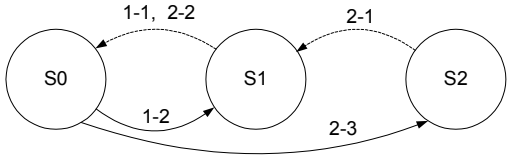
4.3.1 Re-dissemination without Ticket

The originator can approve recipient re-dissemination of the distributed digital object without implementing a ticket either by issuing a license directly to the original requester or by issuing a license that includes LIP. The originator receives requests either directly or indirectly. In figure 3.a, S0 issues a license with LIP to S1 (1-2). If S2 requests a license from S1 (2-1), S1 issues a license with tacit permission from S0 (2-2) because S1 has LIP. This is the only approach in which a license should include LIP among our ORCON in UCON solutions. This means that the originator delegates license-issuing privilege to primary recipients so the recipients can issue licenses to third parties without asking originator's authorizations. This may be useful when the originator wants to distribute its license issuing tasks to increase performance or availability.

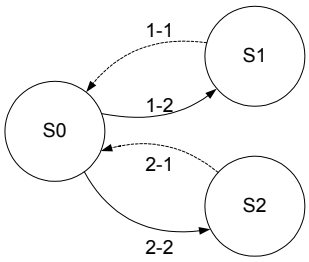
In figure 3.b, S1 requests a license from the originator S0 (1-1) to access the digital object that is originally released by S0 and S0 issues a license for the digital object (1-2). If S2 gets the digital object from S1 and wants to access it, S2 requests a license from S1 (2-1) and S1 requests a license for S2 from S0 (2-2). If qualified, S0 issues a license directly to S2. This approach can be used in case the requestee cannot or doesn't want to issue a license or a ticket to the requester. Figure 3.c is the same as 3.b except that the license request is submitted directly to the originator, rather than through S1. The originator responds to every request directly without any involvement of requesters. In 3.b and 3.c, there is no authorization activity of recipients. Rather the originator authorizes usage rights by issuing the license directly to the original requester. However, these latter two cases provide the same functional effect as in re-dissemination under the originator's control.



(a) Indirect Request w/ Indirect Approval



(b) Indirect Request w/ Direct Approval



(c) Direct Request

Figure 3. Re-dissemination w/o Ticket

4.3.2 Re-dissemination with LGT

A license-granting ticket (LGT) can be used to delegate the license-issuing privilege to recipients. In an indirect request configuration (figure 4.a), S2 requests a license from S1 and S1 requests a LGT from S0. If qualified, S0 issues a LGT to S1 so S1 can issue a license to S2. The direct request approach (figure 4.b) is same as the indirect request approach except that S2 requests a license (LGT) directly from S0. As mentioned previously, LGT is different from a license with LIP in that a LGT is issued upon requests and can be customized to each request while a license is pre-issued for future requests.

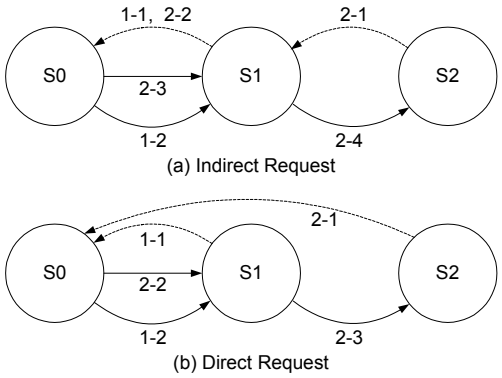


Figure 4. Re-dissemination w/ LGT

4.3.3 Re-dissemination with LRT

Re-dissemination with LRT, illustrated in figure 5, is similar to re-dissemination without a ticket with direct request (figure 3.c) except that it requires a LRT from the previous recipient (2-1, 2-2) so the LRT can be submitted to S0 with a direct request for a license from S0 (2-3). For simplicity, we assume the original recipient does not have to present a LRT to the originator to receive a license for his or her own usage on the digital object released by originator. Approaches using the LRT (figure 5, 6) require two requests from the requester S2. In this case, S2's requests for a license include LRT so S0 may verify S1's agreement on the re-dissemination.

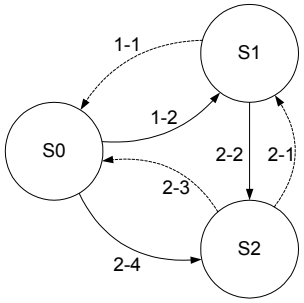


Figure 5. Re-dissemination w/ LRT

4.3.4 Re-dissemination with LGT and LRT

Re-dissemination with LGT and LRT, illustrated in figure 6, is like re-dissemination with LGT with a direct request (figure 4.b) except that it requires LRT from the previous recipient. Thus the LRT can be submitted directly to the originator for a license issuing. Unlike other previous approaches, this approach requires both LGT and LRT to implement ORCON policies. Note that in step 2-2, a LRT is issued to S2 and in step 2-4, a LGT is issued to S1 so that S1 can issue a license to S2 (2-5). In both figure 5 and 6, S0 can verify S1's agreement on re-dissemination to S2. Also S2 has to place two requests to get a license.

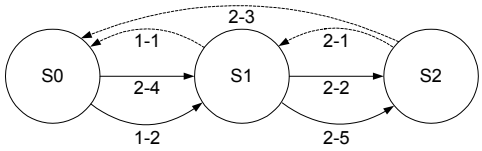


Figure 6. Re-dissemination w/ LGT & LRT

5. Discussion and Related Work

Currently, literature available on models and languages for DRM or UCON is scarce. Most of the work is done in the commercial sector. Some commercial efforts intend to be proprietary and others to be open standards. These models and languages for DRM have mainly focused on payment-enabled usage control systems. None of the solutions has carefully considered access control policies for the environment where payment is irrelevant. In this section, we relate some of the published works available to our ORCON in UCON solutions and to our license and ticket concepts demonstrated above.

5.1 DRM languages by InterTrust

Gunter et al have developed a very simple mathematical model and language to describe licenses for DRM solutions based on InterTrust's DRM solutions [6]. This mathematical model was developed to define license precisely in its semantic meaning. In their models and languages, Gunter et al focused on simplified payment-based control. Their models and languages fail to describe re-dissemination and delegation control functions. Specifically they don't have any kind of ticket concept. The only way to enforce ORCON policies is to include a license-issuing privilege within a license. This means that no instant and temporary delegation of re-dissemination privilege is possible upon request for recipients to re-disseminate the received digital information object but only pre-defined (and delivered) re-dissemination rules can be used. We propose the ticket concept to improve Gunter et al's model.

5.2 XrML

XrML stands for eXtensible rights Markup Language. ContentGuard™ has defined it as "a language in XML for describing specifications of rights, fees and conditions for using digital contents, together with message integrity and entity authentication within these specifications" [15]. Historically, XrML is an extension of the Xerox "Digital Property Rights Language version 2.0 (DPRL)" and has been developed as an open specification licensed on a royalty-free basis by ContentGuard™. ContentGuard™ claims the purpose of XrML, for the commercial sector, is to support commerce in digital contents (i.e. e-book, digital movie, games, software, etc.) and for Intelligence

Community, the purpose is to support specification of access and use controls for secure digital documents. However, XrML still lacks well-defined enforcement of access control policies.

We can build a license in the form of XML by using XrML specification. Our license can be used as a "description part"[‡] of XrML solutions. XrML defines digital license and use "certificate" element under "aPrincipal" entity which is used for identification of principal. This certificate is different from our license because it is used for authentication just like an identity certificate. They also include digital ticket concept using "ticket" element. However, this ticket element is one of two sub-elements of a "fee" element and is used only for the evidence of payment, just like a ticket at a movie theater. By considering our ORCON in UCON approaches, we believe that XrML language specifications and solutions can be improved.

5.3 ODRM

ODRM stands for Open Digital Rights Management. It is developed by IPR Systems Pty Ltd. and has been submitted as a position paper for the W3C DRM workshop [7, 8]. ODRM is based mainly on a DRM model and DRM language (ODRL). Like XrML, ODRL uses XML for model expression. Since ODRM is still preliminary and focused on the semantics of expressing rights languages, it has not yet evolved any mechanisms or expressions for delegation of dissemination or re-dissemination privileges.

6. Conclusion

In this paper, we reviewed UCON and ORCON in general and introduced two most important elements: license and ticket. Then, we discussed the differences between traditional ORCON solutions and ORCON in UCON solutions to demonstrate extended control on the usage of disseminated digital information and proposed seven approaches that implements license and ticket concepts in various ways. Then we compared some characteristics of each approach. Finally, we briefly discussed currently available DRM solutions in terms of our solutions and provided some suggestions.

The study performed in this paper is the first systematic study of this topic. In particular, the solutions we have proposed have not been previously defined in this manner in the literature. Also we are first to suggest license and ticket concepts to enforce ORCON policies in UCON solutions. Nevertheless, this paper does not provide comprehensive solutions. It provides the basis for future research and development for usage control solutions that enforce access control policies for dissemination and re-dissemination of digital information objects. Many aspects should be considered for better understanding of this subject. One crucial aspect is how to revoke the authorized usage rights. Although revocation is not discussed in this paper, since ORCON in UCON deals with delegations of usage rights, careful studies on revocation of these rights should be performed in further research. In addition, a solid understanding of the models and languages is essential for the development of practical usage control solutions. Further research on these aspects will lead to comprehensive and more practical solutions for digital information dissemination controls.

[‡] According to Xerox, digital works consist of a description part and a content part. Description part contains control information for content part.

References

[1] Abrams, Marshall., et al., "Generalized Framework for Access Control: Towards Prototyping the ORGCON Policy", Proceedings of the 14th National Computing Security Conference, pp. 257-266, 1991.

[2] Abrams, Marshall., "Renewed Understanding of Access Control Policies", Proceedings of the 16th National Computing Security Conference, pp. 87-96, 1993.

[3] Cox, Brad. Superdistribution, MA: Addison Wesley, 1996.

[4] Director of Central Intelligence, Control of Dissemination of Intelligence Information, Directive No. 1/7., May 4, 1981.

[5] Graubart, Richard., "On the Need for a Third Form of Access Control", Proceedings of the 12th National Computing Security Conference, pp. 296-303., 1989.

[6] Gunter, Carl., Stephen Weeks., and Andrew Wright., "Models and Languages for Digital Rights", Proc. of the Hawaii International Conference On System Sciences, 2001.

[7] Iannella, Renato., "Open Digital Rights Management", Position paper for the W3C DRM Workshop, 2000, Online, Available: http://www.iprsystems.com.

[8] Iannella, Renato., "Open Digital Rights Language", 2000, Online, Available: http://odrl.net/odrl-08.pdf.

[9] Kaplan, Marc. "IBM Cryptolopes, Superdistribution and Digital Right Management", 1996, Online, Available: http://www.research.ibm.com.

[10] McCollum, Catherine J., Judith R. Messing., and LouAnna Notargiacomo., "Beyond the Pale of MAC and DAC – Defining New Form of Access Control", Proc. of the IEEE Symposium on Research in Security and Privacy, 1990.

[11] Park, Jaehong., Ravi Sandhu., and James Schifalacqua., "Security Architectures for Controlled Digital Information Dissemination", Proceedings of the 16th Annual Computer Security Applications Conference, 2000.

[12] Park, Jaehong., and Ravi Sandhu., "Towards Usage Control Models: Beyond Traditional Access Control", Proc. of the 7th ACM Symposium on Access Control Models and Technologies, 2002.

[13] Sandhu, Ravi., "The Typed Access Matrix Model", Proceedings of the Symposium on Research in Security and Privacy, IEEE Computer Society Press, pp 122-136, 1992.

[14] Sibert, Olin. et al. "The DigiBox: A self-Protecting Container for Information Commerce", Proceedings of USENIX Workshop on Electronic Commerce, New York, July, 1995.

[15] ContentsGuard Inc., "XrML: Extensible rights Markup Language" 2000, Online, Available: http://www.xrml.org.