Towards an Engineering Framework for Usage Control and Digital Rights Management

Jaehong Park *Ravi Sandhu*

The Laboratory for Information Security Technology (LIST)
ISE Department, MS4A4
George Mason University, Fairfax, VA 22030
jaehpark@ise.gmu.edu, sandhu@gmu.edu, www.list.gmu.edu

Abstract

The recent popularity of digital information sharing through networking requires new technologies to protect intellectual property rights or digital copyrights. The concept of digital rights management (DRM) has been introduced in this arena. DRM is largely focused on payment-based controls for digital information dissemination and its use. The principal motivation is generation and protection of revenue derived from digital content. Usage control (UCON) is a more general concept also encompassing payment-free dissemination controls motivated by confidentiality and privacy concerns. UCON unifies traditional access control policies with payment-based policies.

In this paper we outline an engineering framework for UCON based on the four layered OM-AM approach, comprising objective, model, architecture and mechanism layers. Each layer has its distinct scope and aim. We identify some of major factors that comprise UCON objectives. We also identify components that should be included and elaborated within UCON models. We go on to define key elements used in UCON architectures. We give an example of a UCON architectural taxonomy and describe sample architectures. Finally, we briefly discuss a few UCON mechanisms. The goal of this paper is to present issues that we require further study and discussion so as to lay a foundation for better understanding and development of UCON systems.

1. Introduction

In today's digitalized and network-connected information society, most sought after digital information is available within just a few mouse clicks. This accessibility of digital information raises a challenge in controlling its usage and distribution. The recent issues raised by peer-to-peer file sharing are an example of the challenge we face. In response to this situation, the digital rights management (DRM) communities have been significantly active. The main concept of

DRM is originally based on the superdistribution paradigm. In superdistribution, electronic information is available freely, but access to the information is controlled [COX96]. Copy and distribution are not prohibited. Rather they are even encouraged for marketing purposes. What is controlled is the access to and usage of digital information. Because of the commercial advantage that the DRM solutions can provide, the major effort in studying and developing DRM solutions have been driven by the commercial sector. Many of these DRM solutions are proprietary and applicable to specific problems and goals. In another words, though good enough for their intended purposes, each solution is narrow in scope. Moreover, certain DRM challenges would not likely be addressed even by a combination of such solutions.

The notion of usage control or use control (UCON) has been used previously to identify these areas of study. In the perspective of information security, we believe UCON is as vital as the three well-known objectives of confidentiality, integrity, and availability, and thus should be considered as an additional fourth objective. UCON has been known as digital rights management (DRM) in the commercial sector. However, UCON is broader in concept than DRM in that UCON attempts to address problems that are not carefully considered in typical DRM solutions. A discussion of these additional problems follows.

Where payment is not a concern, DRM solutions fail to satisfactorily address the problems. In payment-based control the most important matter typically is increasing the frequency of dissemination and thus increasing revenue, while payment-free control may focus on limiting distribution itself. Many commercial DRM solutions are focused on payment-based dissemination controls. However there are other cases where payment-free control is the major concern. Digital information dissemination in the Intelligence community is one good example. In the Intelligence community digital information is often disseminated to organizations in other countries while restricting both deliberate and accidental re-dissemination of the disseminated digital information to countries other than the original. In this case, payment is not a concern. Rather, we may need some kind of access control policies and mechanisms.

Another problem area is where privacy matters. Most current DRM solutions don't resolve privacy problems appropriately. For certain UCON solutions, privacy functions have to be included. For example, UK's healthcare law mandates healthcare systems allow patients to decide who can and who cannot access their history and even to audit who has accessed the information. In another instance, consumers may have the right not to reveal their usage or purchase patterns, while in many cases the provider or distributor may still want to retrieve consumer usage log information. For example, an MP3 listener may object to the distributor knowing the specific listener's preferred musician or genre but the provider may want to analyze the usage pattern of individual listeners. Here, the system may need to enforce consumer ID anonymity while revealing usage patterns.

In addition, in many of DRM solutions business-to-consumer (B2C) transactions are the major concern. However, this fails to address issues in sharing of proprietary information between or among business organizations. To allow B2B transactions, we need ways to control other organization's use of digital information. This may require inter-organizational agreements on digital information sharing. For example, when two business enterprises are merged, there can be complicated proprietary information sharing among many related business such as law firms, financial organizations and system integration companies. The sharing of proprietary information may require certain enforcement for non-disclosure agreements of involved users or organizations.

These are just some of the many areas that can be considered in UCON systems. Although some DRM solutions have been successful, there is no single one that can be considered a standard reference in the community. This is not because the DRM solutions are bad, but rather because they lack a comprehensive approach to the general problem. After all, little research has been done on extracting consensus from UCON systems. To overcome this situation, we believe there should be a well-formed engineering framework that we can subscribe to and from which

we can analyze UCON systems. Here, by using a layered engineering framework, we attempt to separate the challenges into different levels and define each layer more clearly and completely. Layered approaches for information security have been used in the past to achieve better understanding of and reach solutions for target systems. The OM-AM framework [SAN00] is one of the recently proposed engineering frameworks with a layered approach and has been successfully applied in role-based access control (RBAC). In this paper we use the OM-AM framework to develop a layered UCON framework.

This paper does not provide any new solution mechanisms. Rather, we suggest a simple yet powerful way of viewing and solving UCON problems by using a layered framework. Also, we raise some issues that we believe deserve careful study. In the following sections, we first briefly review the OM-AM framework. We then map UCON systems into each layer of the OM-AM framework. At each layer, we articulate the major requirements and components that are likely to be crucial for UCON systems.

2. The OM-AM Framework

OM-AM stands for *Objective, Model, Architecture,* and *Mechanism*, respectively. *Objective* and *Model* layers articulate what the security objectives are and what should be achieved, while *Architecture* and *Mechanism* describe how to achieve these objectives and requirements. Figure 1 shows an OM-AM framework diagram. Intuitively, the OM-AM framework resembles an OSI 7 layer network protocol stack. Like OSI 7 layers, each OM-AM framework layer's mapping to adjacent layers is many-to-many. In other words, a model can be supported by multiple architectures, while an architecture can support multiple models. Also, the OM-AM framework is neither a top-down nor a waterfall-style software engineering process. Each layer deals with distinct and independent functions, and at the same time these functions are tightly related to other layers in some degree. The functions in each layer require different notions and abstractions to articulate their distinct concerns.

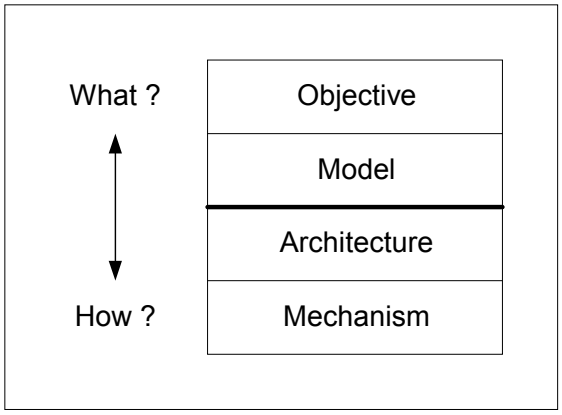


Figure 1. OM-AM Framework

Figure 2 maps Role Based Access Control (RBAC) systems onto OM-AM [SAN00]. Here, we can have multiple security objectives. There are a number of RBAC models that achieve these objectives. The RBAC96 model can achieve multiple security objectives and policies and can support both multi-level security (MLS) and discretionary access control policies. RBAC96

can be realized with user-pull and server-pull architectures in distributed systems. In turn, user-pull and server-pull architectures can also support other access control models such as attribute based access control. Finally, in the mechanism layer, there can be many techniques and protocols to support these architectures.

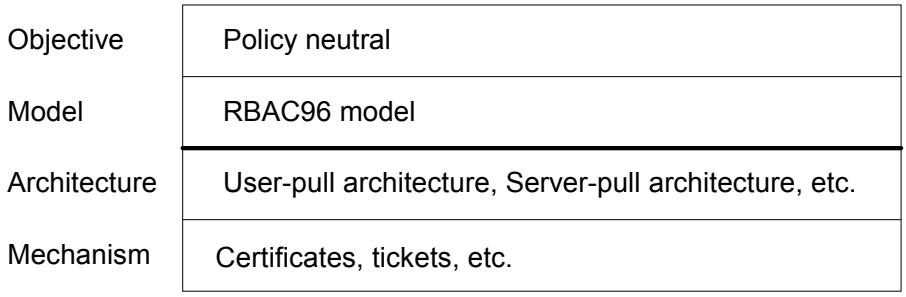


Figure 2. OM-AM Framework for RBAC Systems

3. The UCON Framework in the OM-AM Way

By viewing UCON in the OM-AM four-layered framework, we can divide our engineering approaches or scopes into different layers and address them separately. This does not mean that each layer is unrelated to each other. Rather, they are tightly related, and instances of each layer have many-to-many relations with instances in other layers. By dividing engineering focus into several layers, we can scrutinize the unique requirements and elements of each layer. Later, the aggregated framework of each layer can be referenced and each layer's instances can be implemented as needed. In the following subsections, we discuss UCON objectives, and articulate models, architectures, and mechanisms. In the first section, we discuss some of the major elements that should be considered for UCON objectives. In the second section, we elaborate on several components we think should be a part of UCON models. In the third section, we provide some major elements of UCON architectures and some major factors for an architectural taxonomy. Our previous work discusses some of these architectures. In the mechanism section, we list major technologies that should be considered in UCON mechanisms. The details of each mechanism are beyond this paper's scope and are not discussed.

3.1 The UCON Objective

In the real world, objectives for UCON solutions may vary. Each solution case has a different purpose to achieve. The details of their requirements can vary from case to case. Here, we discuss some major factors that should be considered a part of the objectives. These include payment-based or payment-free, dissemination scale, dissemination environment, prevention/detection, and assurance level factors. In addition to these factors, there can be many other factors that influence individual solution approaches. These factors may influence all or some layers of the model, architecture or mechanism. We believe that careful consideration of these factors will provide a better understanding of UCON system problems and therefore more accurate solution boundaries and requirements.

3.1.1 Payment-Based Type (PBT) vs. Payment-Free Type (PFT)

The purpose of dissemination can be categorized into two types: Payment-Based Type (PBT) and Payment-Free Type (PFT) [PAR00]. In PBT, payment function is required in order to access digital information. B2C mass distribution e-commerce system is one example of PBT dissemination. In PBT, the main focus is to increase revenue by maximizing the number of distributions. Here, some leakage of digital information is acceptable or even desirable for potential revenue increase.

In PFT, payment function is not required. However, dissemination of digital information needs to be controlled for confidentiality or other security requirements. B2B hub system and intelligence community distribution can belong to PFT. Unlike PBT, the purpose of PFT is to limit the distribution itself. In PFT, information leakage is not acceptable and should be prevented.

In PFT, instead of payment, access control policies such as Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-Based Access Control (RBAC) and Originator Control (ORCON) may be required to control dissemination and usage of the disseminated digital information. Adapting access control policies into UCON solutions may require certain changes to traditional access control policies/mechanisms or UCON systems. Also, in addition to either payment mechanism or access control mechanism, both PBT and PFT require certain kinds of attributes (e.g., territorial locations for DVD) that can be used for authorization.

The following table compares PBT and PFT.

Characteristics	PBT	PFT
Leakage	Acceptable or even desirable	Not acceptable
No. of copies per item	High volume	Low volume
Purpose	Revenue increase	Limiting dissemination itself
Access	By payment	By MAC, DAC, etc.

Table 1. Characteristics of PBT and PFT

3.1.2 Dissemination Scale

Based on the dissemination volumes of the digital information object, we can identify three scales of dissemination, small, medium, and large, as shown in Figure 3. In small-scale dissemination, each digital information item is distributed to approximately one to hundreds of recipients. Business-to-business (B2B) transactions and Intelligence community disseminations are typical examples of small-scale dissemination. In medium-scale dissemination, each digital information item is distributed to approximately 10^3 to 10^5 recipients. Technical texts or journals are objects typically disseminated at such a scale. In large-scale dissemination, each digital information item is distributed to approximately 10^6 to 10^8 recipients. Music files, such as MP3s, or electronic books are typically disseminated at large-scale.

The numbers given are not absolute values but indicate a general scale for distribution size. In general, the smaller the dissemination scale is the lower the tolerance for information leakage is. Again, the commercial sector is mainly interested in medium to large-scale dissemination, while the Intelligence community is mainly interested in small to medium-scale dissemination.

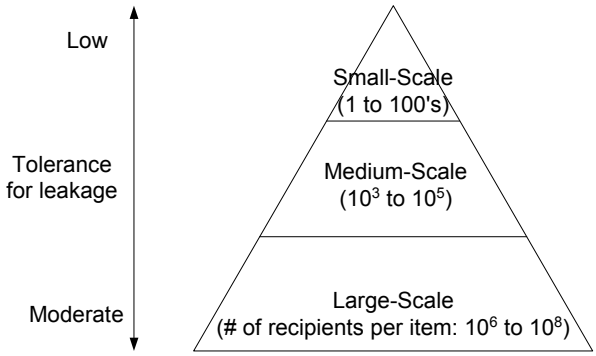


Figure 3. Dissemination Scale

3.1.3 Dissemination Environment

In UCON, dissemination can occur in various environments. Figure 4 shows four dissemination environments. They are closed (CED), open (OED), federated (FED) and personal (PED) environments. In CED, dissemination is done within a closed organization that is under the same central control. Internal distribution within either commercial or Intelligence organizations belongs to CED. Here, it is relatively easy to customize client-side systems (both software and hardware) or to use dedicated systems. In OED, dissemination is done to recipients outside the disseminating organization. B2B and B2C distributions are examples of OED. Here, it is hard to customize a general-purpose client-side system. In FED, dissemination is done from one hub organization to a limited number of recipient organizations. B2B disseminations may belong to FED. In FED, there are limited administrative controls over recipients based on the agreements between disseminator and recipient organizations. In PED, an individual sends digital information to recipients. Recipients may or may not belong to an organization (dashed line in figure 4). P2P disseminations may belong to PED.

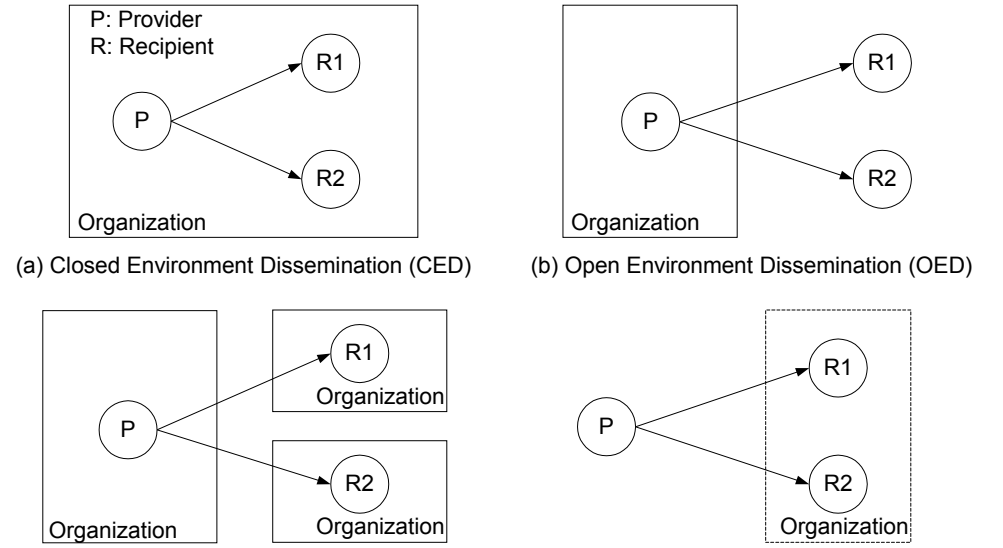


Figure 4. Dissemination Environment

In addition to dissemination environments, we may also think about aggregation environments where collecting digital information for future dissemination is done. However, in some sense, aggregation and dissemination can be considered as occurring in the same environment but with different semantics. Both aggregation and dissemination distribute certain information to other parties and can belong to any of the above dissemination types.

3.1.4 Prevention and Detection

The main approaches to information security solutions are prevention, detection, or both. Figure 5 shows a diagram for security attacks and protections. By implementing a prevention filter in the security system, we can protect digital information from these attacks. However, as shown in the figure, some attacks break through prevention mechanisms and thus access the digital information. If these breakthroughs cannot be avoided, then well-defined security mechanisms should be implemented to trace the attackers. One popular tracing mechanism would be watermarking technologies. The detection and tracking filter can detect attacks and trace them back by using watermarking techniques. Prevention and detection & tracking can coexist. In some cases, they must coexist.

In figure 5, the gray arrow depicts the tracking process. However, current available technologies (e.g. watermarking technologies) are still premature to guarantee the tracking of the dissemination and re-dissemination of digital information. The dashed line in the figure shows those attacks that subvert detection and the tracking process.

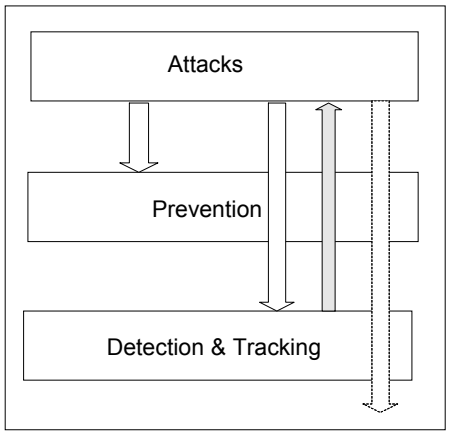


Figure 5. Prevention vs. Detection and Tracking

3.1.5 Assurance Level

Information assurance can be another important element in UCON systems. *High assurance* will require stricter controls on dissemination and usage on the disseminated digital information and will provide better protection for digital information. To do that, we may need to implement hardware-based tools for client-side applications. However, there are situations where high assurance is not always required. In many cases, *adequate assurance* may be enough for security purposes. As mentioned above, in commercial mass-distribution systems, some leakage may be acceptable or even desirable for marketing purposes. Adequate assurance may be achieved with software-based client-side applications. Obviously, software-based approaches are likely to be

easier for distribution and implementation into client-side systems than hardware based approaches.

3.2 The UCON Model

Next, we identify several key components for UCON systems and discuss the relationships among the components. In the UCON model layer, we do not consider how to implement UCON solution systems using these key components. This is left to the architecture and mechanism layers.

In our viewpoint, a UCON model is divided into two sides: a consumer side and a provider side. Each side consists of the six major components of Subject, Object, Rights, Condition, Obligation, and Authorization where the Object component is common to both sides as shown in Figure 6. Dividing UCON models into a consumer and provider side is intuitive and may be the one most crucial step in building UCON models. By doing so, we can clarify the definition of each component and the relationships among them. For example, since consumer subject and provider subject have different roles in the UCON model, their rights (consumer rights and provider rights) are likely to be quite different from each other. In fact, in the DRM community, we have seen the term "rights" used vaguely. In terms of the term "DRM", whose rights are they? And who manages the rights? These are some of the questions that we have to answer in UCON models. The details of each component and their relationships are discussed below.

The UCON system should be *fair-to-subjects* of both consumer and provider sides. This means that these two sides should be weighted equally during their design, implementation, and use in a UCON system in contrast to many commercial DRM solutions that lack this fairness intentionally or accidentally.

Note that this is not a complete description of UCON models. Rather, this is a preliminary study on the subject and we intend to provide general ideas on UCON models. Studies on a more comprehensive model require further clarification and refinement and are left to future work.

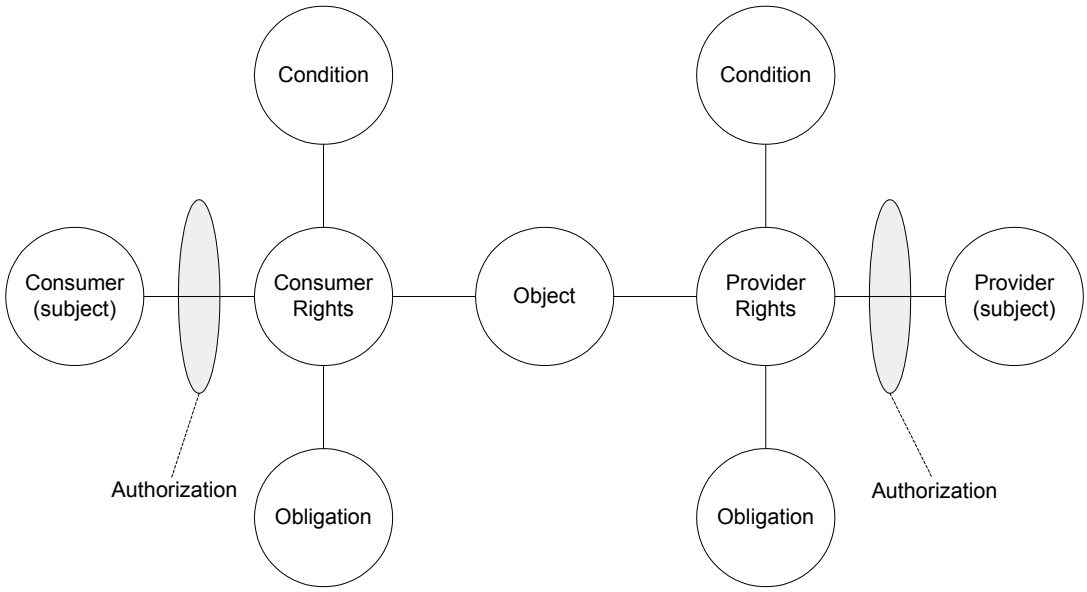


Figure 6. A UCON Model and Components

3.2.1 Model Components

The ***subject*** is an entity that exercises certain rights on objects. A subject can be either a *consumer subject* or a *provider subject*. The consumer subject is the one who receives objects and uses them based on possessed rights. In the digital world, the consumer does not consume digital objects. What is actually consumed is the consumer's rights on digital objects. These rights can be either "use of digital objects for consumers themselves" or "propagating digital objects for others". The provider subject is the one who provides the digital object and has certain rights on the object. The originator (creator of the digital object), distributor or even recipient can be a provider. The subject can be a user, a group, a role, a department, an organization and so on.[*] In the typical definition of access control literature, a user is an individual entity that has certain rights on objects. A group is a set of users and may have a hierarchy in it. A role is a named collection of users and a relevant collection of permissions [SAN96]. A role can also have a hierarchy in it.

The ***object*** is a digital information resource that the subject holds rights on. The types of objects are various. They include document (e.g., .doc, .pdf, .ps), audio (e.g., .mp3, .wav), video (e.g., JPEG, DVD, MPEG), and executable files (e.g., games), etc. Each may require its own application tools to be used. In the file system, an object can be a file, a set of files, a directory, of a set of directories. Semantically, an object can be a single unit or a set of units. A unit can consist of a set of sub-units of contents with or without hierarchy. The structure of an object is tightly related to rights on the object and will influence hierarchies of related rights. Regardless, literature that carefully defines the object itself and its relationships to both other objects and other components is scarce. Therefore, we need to analyze the structure of objects for the relationship among rights. The definition of the object should be further explored for better control on usage rights.

The ***rights*** component is one of the core components of UCON models. Like subject, rights also can be divided into two parts*: consumer rights* and *provider rights*. As mentioned above, the term "rights" is quite subjective and not clearly defined or used. For example, in the DRM community, providers or distributors are represented as rights holders. What is meant by the term "rights" in "rights holder"? What kind of rights are they? Who holds what rights and whose rights? Are the rights different from users' (consumers') rights? All these series of questions are caused by an ambiguous definition of rights. Obviously, what it should mean is a subject who has provider or consumer rights. To reduce this kind of ambiguity and for better understanding and clarification of rights, rights may have to be classified into different groups with clear definition of each group.

In the commercial sector, a few attempts to identify rights and to classify those rights into some category have been made. Most of their classifications are based on functional characteristics of rights. For example, ContentGuard has proposed XML specification for rights management called eXtensible rights Markup Language (XrML) [XRM00]. In XrML, rights or digital property rights have been categorized into five logical rights groups: transport rights, render rights, derivative work rights, file management rights, and configuration rights. In ODRM from IPR Systems Pty [IAN00a, IAN00b], rights have been divided into three groups: use rights, transfer rights, and reuse rights. In both examples, these functional classifications have provided core structures for their metadata language for rights (especially for consumer rights) management. While functional characteristics-based classification is important in UCON systems, there may be some other classification that is also crucial for UCON systems. Some of

[*] In access control literature, a process is also considered as a subject. We exclude this possibility in our subject definition at this time because viewing the subject as a real world entity rather than including digital processes of computer systems is enough or even better in understanding or explaining UCON systems.

the basis for these classifications may include subject type, the origin (creation) of rights, hierarchy, and positive or negative rights.

Based on the subject type, consumer rights and provider rights can exist. In UCON models, the provider has provider rights on an object to define usage rules and conditions for consumer rights on the object. The consumer holds consumer rights to use services on an object. Based on origin of rights, (consumer's/provider's) *legal rights* and *procurable rights* can exist. Legal rights are what consumers or providers are given from an authority outside the system such as law and do not require any extra action other than using them to acquire the rights. For example, by law, patients may have rights to restrict certain doctors' access to his or her personal history files without any kind of authorization process. So, the legal rights of a consumer subject are likely to be the provider subjects' obligation or vice versa. Procurable rights are given from other entities within the system and need some actions to acquire rights such as payment. For example, a consumer may hold procurable rights to access a MP3 file after credit card payment.

In addition to these classifications, rights may have a hierarchy in it. The hierarchy of rights can be tightly related to the structure of related objects. It may or may not have inheritance and can be either aggregation hierarchy or generalization/specialization hierarchy. Like in role-based access control, we may have to consider a named set of rights that may have a hierarchy. Like permission in RBAC, the named set of rights can be an abstraction of a set of subject's rights such as an employee's privileges or project manager's duties.

We are confident of agreement on the need for above three components (subjects, objects and rights) in UCON systems since they are also crucial elements in typical access control systems. In addition to this, we believe the following components are also as important as the above three for UCON models. Obligation is one, and is hardly acknowledged as a core component of UCON. ***Obligation*** is what a subject should have to do to exercise rights on an object. Consumer subject may have to accept metered payment agreements for the usage on certain digital information or should report usage log information to provider subject. Another example is that the consumer subject must agree on a payment (deducting the amount of charge from her account) upon access to a digital information object. Here, consumer's obligation may be part of provider's legal rights. Likewise, consumer's legal rights are likely to be parts of provider's obligations and vise versa as described above. Notes that this may not be true in case of procurable rights.

Unlike privileges in access control, rights in UCON are more than just read and write. Instances of UCON rights can be numerous. Some of the examples are view, execute, print, copy, transfer, move, edit, embed, delete, install, lend, sell, and so on. In UCON systems, when a subject exercises rights on an object, there can be certain conditions that limits the usage of the rights. The ***condition*** is what the system should verify at authorization process along with authorization rules before allowing usage of rights on a digital object. Conditions may contain either dynamic or static information. *Dynamic condition* is stateful while *static condition* is stateless. Examples of a dynamic condition include the number of usage times (e.g., can read 5 times, can print 2 times), usage log (e.g., already read portion cannot be accessed again), and whatever has to be checked at each time of usages for updates. Static condition examples include accessible time period (e.g., office hour), accessible location (e.g., workplace), allowed printer name, and those that do not have to be checked at each time of usages for updates.

The ***authorization*** process also has to be performed before the system allows a subject to access the digital object. To do this, ***authorization rules*** must exist which can be referred to. Authorization rules are a set of requirements that should be satisfied before allowing access to or use of digital objects. Authorization rules and conditions are similar in their usage, but different in their purpose. Both are used as decision factors. However, authorization rules are a set of decision factors used to check whether a subject is qualified for the use of certain rights on an object, whereas condition is used to check whether existing limitations and conditions of usage rights on an object are valid, and has to be checked upon the use if updates are necessary or not.

Examples of Authorization rules include multi-level security label, permission-role assignment rule, payment approval, etc.

3.2.2 Examples of UCON Components

The following table 2 shows some examples that can be instances of each component of UCON models. The detail of instances also should be included within completed UCON models so they can be considered at the time of UCON system implementations.

Component	Examples
Subject	Publisher, patient, reader, distributor, doctor, author, musician, etc
Object	Digital document, audio file, video file, game file, etc.
Rights	• Consumer rights: view/play, print, edit, copy, etc. • Provider rights: Collect usage fee and usage log information, change usage rules (fee rates), etc
Obligation	• Consumer subjects have to accept metered payment agreement for the usage of certain digital information • Consumer should report usage log information to provider subject • Consumer subject has to agree on payment (deducting the amount of charge from her account) upon access to a digital information object • Consumer has to agree on report of local system configuration information • Provider has to inform consumer that usage log has to be reported to him or her • Provider has to inform consumer of usage rates • Provider has to agree on distributor's share of profit
Condition	• # of usage times (exercise rights 5 times) - stateful • Accessible parts based on usage log - stateful • Accessible time period • Accessible location • Allowed printer name
Authorization Rule	• Security label • Role certificate • Attribute certificate • Payment

Table 2. UCON Model components and examples

3.3 The UCON Architecture

Commercially, several UCON solutions have been developed. Each of them has their own architecture(s). However, some research has been done to identify and discuss more generalized security architectures that can cover problem space comprehensively and can be used as a reference in future studies. We believe these architectural studies will provide solid foundations for better understandings and more concrete solution approaches on UCON systems. These architectures are likely to be tightly related to target objectives, models and relevant mechanisms.

Here, we identify key elements that will act as core components in UCON architectures and present a taxonomical diagram for general solution architectures and some sample architectures. Key elements of UCON architectures include digital container, virtual machine, control set, and control center (clearing house). Note that how these key elements are implemented is not a concern of architecture layer. It has to be resolved in mechanism layer. Besides these key elements, we identify three decision factors for our architectural taxonomy example. There can be other decision factors that can create other taxonomies for UCON architectures. For example, the architecture taxonomy and example architectures shown here are not focused on federated environment dissemination. Taxonomy and architectures for FED may have different characteristics and decision factors.

3.3.1 Architecture Elements

In UCON system, digital information is encapsulated within 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* [PAR00].

The ***digital container*** [SIB95, KAP96] is one of the key elements of UCON architectures. A digital container is a tamper resistant, cryptographically scrambled and wrapped digital information object that is designed to protect embedded digital information in it and control the usage of the contents. 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.

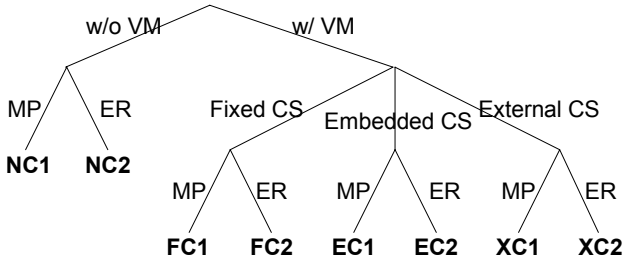
The ***virtual machine (VM)*** is another key element of UCON architectures. It can be defined as a trusted, tamper-resistant, recipient-side application software or hardware component that runs either standalone or on top of vulnerable computing environment. In UCON systems, a virtual machine includes a viewer application and a mechanism to verify the validation of usage rights in available control sets and may require network connections to get requested digital objects or control sets. Digital container can only be accessible within the virtual machine. Virtual machine only allows the use of verified rights. By using a virtual machine, we can restrict the usage of rights on digital objects. For instance, we can disable the print function, save function, and save-as function within the virtual machine.

The ***control set*** is where all the usage rights, subject and object information, obligations, conditions, and authorization rules are defined. Upon requesting use of digital object, contents of control set are used to verify validation of usage rights within virtual machine. In UCON architectures, control set can be either pre-set in virtual machine, embedded in digital container along with the digital object or defined independently in separate digital container. In real world solutions, certificates or credentials can be used to include control set. As an alternative to certificates or credentials, watermarking technologies can be used to include control set information.

The ***control center*** is where usage rights (control sets) and usage history are stored and managed. The control center provides recipients control information that the recipients can use for access to digital information. Providers store control set information at a control center. Upon the service requests, a virtual machine checks available control sets locally and if necessary, it connects to the control center to receive relevant control sets. In payment-based DRM solutions, the control center is also acts as a clearinghouse where payment functions are managed for access to digital information.

3.3.2 Architectural Taxonomy Example

Park et al. [PAR00] has defined a UCON architecture taxonomy that consists of eight security architectures based on the three major factors. They are virtual machine (VM), control set (CS), and distribution style. In figure 7, 'without VM architectures' (NC1, NC2) do not have control functions while they can have tracking functions. NC1 and NC2 are shown for comparison purpose. In 'with VM architectures', three styles of control sets are introduced. 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. Fixed CS, Embedded CS and external CS can coexist with each other in VM. The last decision factor is distribution style. There are two distribution styles: message push (MP) style and external repository (ER) style. In MP style, digital information is sent to recipients either physically or electronically. In ER style, digital information is stored at dissemination server and retrieved from network-connected recipients.



VM: Virtual Machine
MP: Message Push
ER: External Repository
CS: Control Set

NC1: No control architecture w/ MP
NC2: No control architecture w/ ER
FC1: Fixed control architecture w/ MP
FC2: Fixed control architecture w/ ER
EC1: Embedded control architecture w/ MP
EC2: Embedded control architecture w/ ER
XC1: External control architecture w/ MP
XC2: External control architecture w/ ER

Figure 7. UCON Architectural Taxonomy

3.3.3 Architecture Examples

Figure 8 shows two sample architectures defined in above architecture taxonomy. In EC2, the control set is embedded in the digital container and always comes with the related digital object. The encapsulated digital information with control set is stored at the external repository and can be retrieved from recipients or consumers. Here, if local storing of distributed digital container in non-volatile storage is not allowed, distributor can change or revoke the consumers' previously granted rights even after the distribution. In this case, consumers have to connect external repository every time they want to access digital information. In XC1, a distributor send digital information object to consumers and control set to a control center. A consumer acquires control sets from the control center. These control sets are distributed independently and used to access

digital information object. Here, there are two possibilities in network connection options. One is that a recipient always has to connect to control center to get usage rights. In this case, the usage rights are for one time use only. The other case is that a recipient has to connect control center occasionally to get proper usage rights. In this case, usage rights can be used either for a limited number of times, for a limited time period, or as long as a certain conditions are satisfied. In latter case, there can be a rule that one-time only connection is all required for use of digital objects. This is the case when a recipient receives a set of rights without expiration.

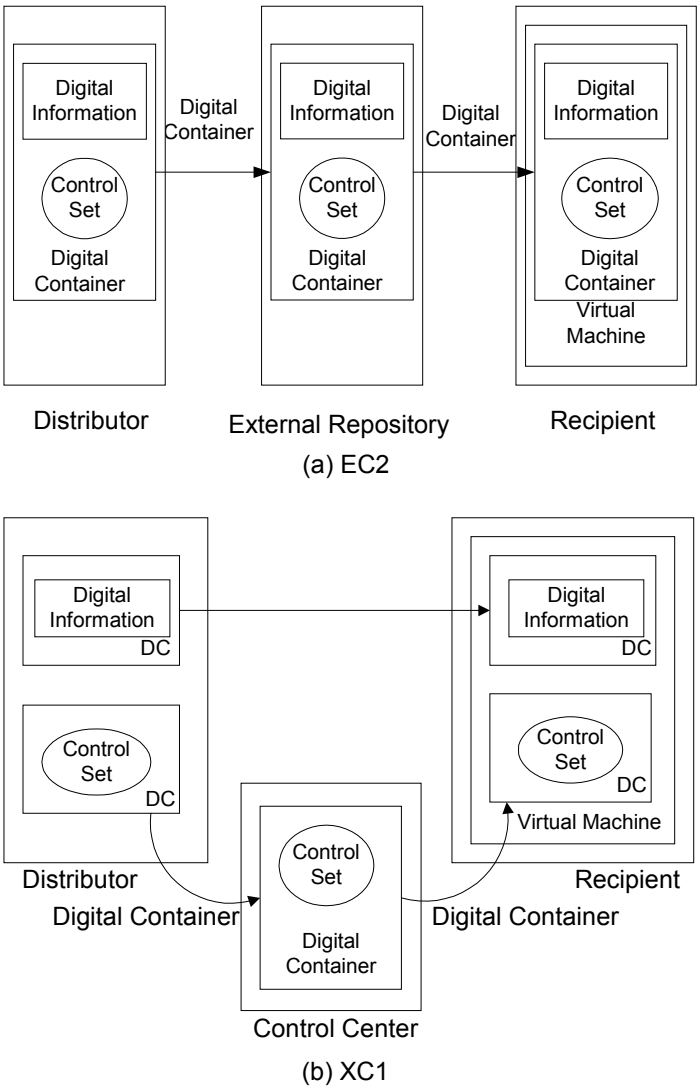


Figure 8. UCON Architectures

3.4 UCON Mechanism

UCON mechanisms are fundamental technologies that make all the UCON systems work. These technologies are used to support all the requirements and functions of UCON systems. Most of UCON mechanisms are separate areas of technologies and used in many other

information security areas. They are too many to list. Some of them are metadata languages, access control policies and technologies, watermarking technologies, tamper resistant technologies, cryptographical digital container technologies, software-based or hardware-based virtual machine technologies, anonymity technologies, electronic payment technologies and etc. Here, we briefly discuss a few of these mechanisms that are crucial for UCON systems. The detail of each mechanism is out of this paper's scope and is not discussed here.

3.4.1 Metadata Languages

Metadata is a data of data which means that metadata includes semantics of the data. Metadata language is a language specification used to present metadata. In general, metadata language reflects large portion of model semantics. To build metadata language for UCON systems, it is critical that UCON model has been well defined and described in detail. Metadata language is used in UCON systems as a tool to express all of the components in UCON models: subject, object, rights, obligation, condition and etc. For UCON systems, there exist a few metadata languages published. So far, XML seems to be the most favorite tool for UCON metadata languages. XrML of ContentGuard uses XML specification and has defined the detail description of usage rights and other components of UCON models in Data Type Definition (DTD) file for digital rights management [XRM00]. ODRL is another metadata language specification that attempts to be used in DRM solutions [IAN00a, IAN00b].

3.4.2 Access Control Mechanisms

In UCON systems, two major authorization mechanisms will be electronic payment and access control mechanisms. In information security, access control is one of the traditional areas of concerns. The three best-known access control policies are MAC, DAC, and RBAC. As mentioned briefly in the objective layer section, these access control policies may require different mechanisms to be implemented in UCON systems. The ORCON access control policy is also of interest to UCON. In ORCON systems, distributors other than originator always have to request an originator's approval before re-dissemination of digital object to third parties. Traditional ORCON policies [GRA89, MCC90, ABR91, SAN92] have been discussed only for the centrally controllable system domains such as host-based systems and client-server systems by utilizing some form of non-discretionary access control list [ABR93]. However, in current UCON system environment where there may be no central control authority available, so traditional ORCON systems are not applicable as they are. For instance, in case of B2C environment, requesting and approval of re-dissemination cannot be done by checking central control authority or reference monitor because after dissemination, the digital information can be accessible in off-line mode without connecting to the distributor or provider.

3.4.3 Watermarking Mechanisms

There are two main usages of watermarking technologies in UCON systems. On one hand, digital watermarking technologies can be used to embed control set information into digital objects. By doing so, UCON systems can use digital watermark for control purposes. On the other hand, digital watermark or more correctly digital fingerprint is used to mark the identity of digital objects with information such as author's name, recipient's name, and distributor's name for detecting and tracking of unauthorized use of distributed digital information [KOB97, ZHA97].

There might be certain requirements to utilize watermarking technologies because of its technological characteristics and limitations. For example, watermarking technologies are largely dependent on the type of digital objects. Text, image, audio, or video requires different technologies for watermarking. Also, the size of digital object is another important factors that enable digital watermarking possible. If the size of digital object is smaller than the size of information that is going to be embedded, it will be very difficult to embed the information. In addition to these, in case of mass distribution, embedding unique watermark information (fingerprint) in each copy of original digital information object is not practical yet [DWO99].

4. Conclusion

In this paper, first we have reviewed OM-AM framework. Then we mapped UCON systems into layers of OM-AM framework. At each layer, we defined major elements that should be included in it and raised some issues for each of elements and layers. Obviously, what we have identified and discussed in this paper is our initial grasp on this subject and is not a complete work. Our goal in this paper is to visualize problem spaces in the form of layered framework and provide a foundation for commonly accepted understandings of UCON systems. Achieving a consensus on UCON framework and major factors of each layer for UCON systems would be of significant benefit to researchers and practitioners in UCON or DRM community for further studies and developments. We believe this layered approach and further research on the details of each UCON framework layer will provide solid foundation for developing and deploying UCON solutions.

References

[ABR91] 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.

[ABR93] Abrams, Marshall., "Renewed Understanding of Access Control Policies", Proceedings of the 16th National Computing Security Conference, pp. 87-96, 1993.

[COX96] Cox, Brad. Superdistribution, MA: Addison Wesley, 1996.

[DWO99] Dwork, Cynthia, Copyright? Protection?, The Mathematics of Information Coding, Extraction, and Distribution, The IMA Volumes in Mathematics and its Applications, vol. 107, pp. 31-47, 1999. NY: Springer-Verlag.

[GRA89] Graubart, Richard., "On the Need for a Third Form of Access Control", Proceedings of the 12th National Computing Security Conference, pp. 296-303., 1989.

[IAN00a] Iannella, Renato., "Open Digital Rights Management", Position paper for the W3C DRM Workshop, 2000, Online, Available: http://www.iprsystems.com.

[IAN00b] Iannella, Renato., "Open Digital Rights Language", 2000, Online, Available: http://odrl.net/odrl-08.pdf.

[KAP96] Kaplan, Marc. "IBM Cryptolopes, Superdistribution and Digital Right Management", 1996, Online, Available: http://www.research.ibm.com/people/k/kaplan/cryptolope-docs /crypap.html.

[KOB97] Koblin, Jens., Kockelkorn, Michael. The IMPRIMATUR Multimedia IPR Management System, 1997, Online, Available: http://www.imprimatur. alcs.co.uk/newstore.htm.

[MCC90] McCollum, Catherine J., Judith R. Messing., and LouAnna Notargiacomo., "Beyond the Pale of MAC and DAC – Defining New Form of Access Control", Proceedings of the Symposium on Research in Security and Privacy, IEEE Computer Society Press, 1990.

[PAR00] Park, Jaehong., Ravi Sandhu., and James Schifalacqua., "Security Architectures for Controlled Digital Information Dissemination", Proceedings of the 16th Annual Computer Security Applications Conference, December, 2000.

[SAN92] 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.

[SAN00] Sandhu, Ravi., "Engineering Authority and Trust in Cyberspace: The OM-AM and RBAC way", Proceedings of the 5th ACM workshop on Role-Based Access Control, ACM, Berlin, July, 2000.

[SIB95] Sibert, Olin. et al. "The DigiBox: A self-Protecting Container for Information Commerce", Proceedings of USENIX Workshop on Electronic Commerce, New York, July, 1995.

[XRM00] ContentsGuard Inc., "XrML: Extensible rights Markup Language" 2000, Online, Available: http://www.xrml.org.

[ZHA97] Zhao, Jian. Applying Digital Watermarking Techniques to Online Multimedia Commerce, In Proc. of the International Conference on Imaging Science, Systems, and Applications, Las Vegas, June, 1997.