Towards Usage Control Models: Beyond Traditional Access Control

Jaehong Park

Laboratory for Information Security Technology
George Mason University
4400 University Dr. Fairfax, VA 22030, USA
jaehpark@ise.gmu.edu, www.list.gmu.edu

Ravi Sandhu

SingleSignOn.Net, Inc. and
George Mason University
11417 Sunset Hills Road, Reston, VA 20190
sandhu@gmu.edu, www.list.gmu.edu

ABSTRACT

In this paper we develop the concept of Usage Control (UCON) that encompasses traditional access control, trust management, and digital rights management and goes beyond them in its definition and scope. While usage control concepts have been mentioned off and on in the security literature for some time, there has been no systematic treatment so far. By unifying these three areas UCON offers a promising approach for the next generation of access control. Traditional access control has focused on a closed system where all users are known and primarily utilizes a server-side reference monitor within the system. Trust management has been introduced to cover authorization for strangers in an open environment such as the Internet. Digital rights management has dealt with client-side control of digital information usage. Each of these areas is motivated by its own target problems. Innovations in information technology and business models are creating new security and privacy issues which require elements of all three areas. To deal with these in a systematic unified manner we propose the new UCON model. UCON enables finer-grained control over usage of digital objects than that of traditional access control policies and models. For example, print once as opposed to unlimited prints. Unlike traditional access control or trust management, it covers both centrally controllable environment and an environment where central control authority is not available. UCON also deals with privacy issues in both commercial and non-commercial environments. In this paper we first discuss access control, trust management, and digital rights management and describe general concepts of UCON in the information security discipline. Then we define components of the UCON model and discuss how authorizations and access controls can be applied in the UCON model. Next we demonstrate some applications of the UCON model and develop further details. We use several examples during these discussions to show the relevance and validity of our approach. Finally we identify some open research issues.

Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection – *Access controls*; K.6.5 [**Management of Computing and Information Systems**]; Security and Protection – *Unauthorized access*

SACMAT'02, June 3-4, 2002, Monterey, California, USA.

General Terms: Design, Security

1. INTRODUCTION

With today's revolutionary innovations in information technology and their impact on our society, we are encountering a series of new problems on security and privacy issues. Scientists have tried to resolve these problems by focusing on their own target issues. These efforts have produced significant results in their own areas and the area of information security overall. Access control is one of these areas and has been considered as a major issue in information security community since the beginning of the information security discipline. Access control literature has traditionally focused on the protection of data in a closed environment. The enforcement of control has been primarily based on identity and attributes of a known user or a process by using a reference monitor and specified authorization rules. More recently research in authorization for unknown users has been pursued under the name of trust management [3, 15, 16]. Trust management relates authorization to a user's capability and properties.

While both traditional access control and trust management have focused on the control of access to server-side objects, there have been other studies to control access to and usage of digital objects even after the objects are disseminated [9, 13, 14]. This area of study has come to be called digital rights management (DRM). Because of DRM's potential opportunity for commercial sector, current DRM solutions are largely focused on payment-based dissemination controls though its underlying technologies can be also used for controls of non-payment based dissemination.

Because each of access control, trust management, and DRM has focused on its own target problems and detailed solutions for these problems, we lack a comprehensive, systematic approach for controls on usage of digital objects regardless of specific circumstances. In addition, there are other problem spaces like privacy which are not directly covered within these disciplines. In this paper, we introduce a consolidated view of all these three areas and define a model called *usage control* that unifies all three areas. The term "usage" means usage of rights on digital objects. And the term "rights" includes rights for use of digital object and rights for delegation of the rights.

In section 2, we will discuss what usage control covers and how it relates to traditional information security areas. In section 3, we define each component of the UCON model. In section 4, we go on to discuss how traditional access control policies and DRM authorization processes can be mapped to UCON. In section 5 and 6, we use three examples to demonstrate how UCON models can

be applied in real world systems. Finally we conclude with some future research directions.

2. UCON SCOPE

In this section, we explain the scope of UCON based on payment options and different kinds of reference monitors. We also map other related information security issues onto the UCON framework to show what UCON covers.

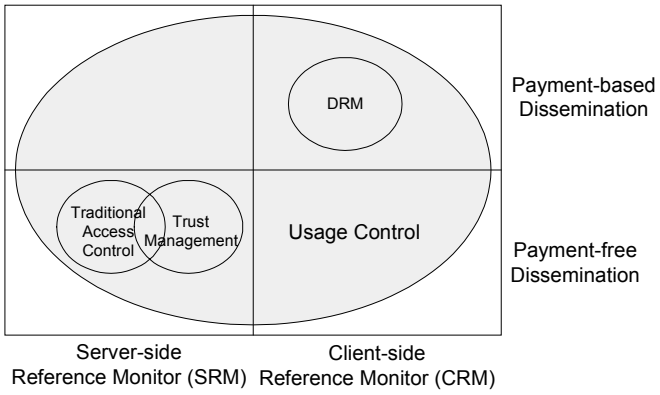

Figure 1. UCON Scope

2.1 The Control Domain and the Reference Monitor

Control Domain is an area of coverage where rights and usage of rights on digital objects are under control of a reference monitor. A reference monitor associates decision policies and rules for control of access to digital objects. It is always running and tamper resistant. Subjects only can access digital objects through the reference monitor. There are two types of control domains based on where the reference monitor is located. One is *Control Domain with Server-side Reference Monitor (SRM)* and the other is *Control Domain with Client-side Reference Monitor (CRM)*. Here, server is an entity that provides a digital object and client is an entity that receives and uses the digital object. Like a traditional reference monitor, a SRM resides within server system environment and mediates all access to digital objects. On the other hand, a CRM resides in the client system environment and controls access to and usage of digital objects on behalf of a server system. Note that there can be a control domain with both SRM and CRM. In fact, this is more likely to happen in real world systems because even with CRM implemented, a server probably wants to include some control functions in its own side for better control. UCON also covers this kind of hybrid control domain.

2.1.1 Control Domain w/ Server-side Reference Monitor (SRM)

A control domain with SRM facilitates a central means to control subjects' access to and usage of digital information objects. A subject can be either within same organization/network area or outside this area. In this environment a digital object may or may not be stored in client-side non-volatile storage. If the digital object is allowed to reside in client-side non-volatile storage, it means the saved client copy of the digital object doesn't have to be controlled and can be used and changed freely at client-side. For example, an on-line bank statement can be saved at a customer's local machine for his records and the server system (bank) doesn't care about customer's copy as long as the bank keeps original account information safe. However if the content of digital information itself has to be protected and controlled centrally, the digital information must remain at server-side storage and never be allowed to be stored in cleartext on client-side non-volatile storage. Traditional access control and trust management focus on this environment (at least implicitly).

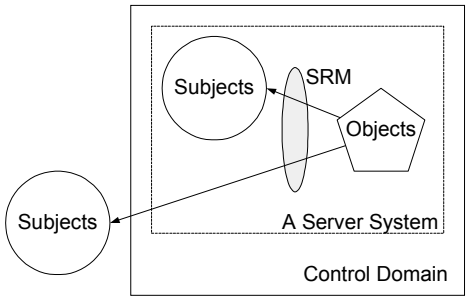

Figure 2. The Control Domain w/ SRM

2.1.2 Control Domain w/ Client-side Reference Monitor (CRM)

In a control domain with CRM environment, no reference monitor exists in server-side system. Rather, a reference monitor exists at the client system for controlling usage of disseminated digital information. In this environment digital objects can be stored either centrally or locally. Since there exists a CRM, the usage of digital objects saved at the client-side is under the control of CRM in lieu of the server. Digital rights management solutions belong to this environment. In real world implementation, CRM is likely to be combined with a viewer or a browser. One example might be Acrobat Reader with Webbuy plug-in. Webbuy functions as a CRM. Digitally encapsulated PDF files can be viewed through Acrobat Reader with Webbuy. The Webbuy controls access to the contents based on a valid license called Voucher.

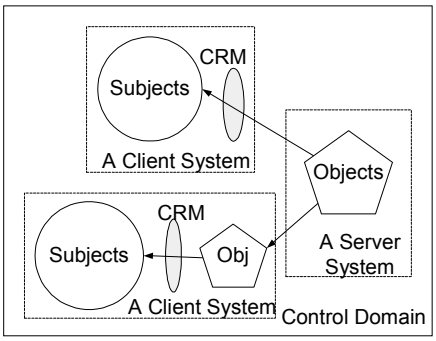

Figure 3. The Control Domain w/ CRM

2.2 Payment-based vs. Payment-free

We can distinguish two main purposes of digital information dissemination and its use. One is payment-based type (PBT) and the other is payment-free type (PFT). In PBT, authorization is done based on payment options. The main objective of PBT dissemination might be maximum distribution of digital objects for revenue increase. B2C mass distribution can be an example. In PFT, payment is not required but dissemination must be controlled for confidentiality or other security/privacy

requirements. Intelligence community or B2B can be an example. We also notice PBT and PFT can coexist in certain situations though this is not explicitly shown in figure 1.

2.3 UCON and Traditional Security Areas

Traditional access control, trust management, and DRM deal with their own target problems. Traditional access control enables controls primarily in a control domain where SRM exists and mainly focuses on payment-free environment. Access control typically deals with access of users who are previously known to the system (though capability based approaches may be an exception). Trust management deals with authorization process for the access of users who are previously unknown to the system. Trust management also mainly focuses on a control domain where SRM is available. DRM mainly focuses on payment-based disseminations though its underlying technologies can also be used for payment-free dissemination. Unlike access control or trust management, DRM enables controls in a control domain where SRM is not available. Unifying these three areas provides more than the sum of them. UCON not only includes these three issues but also covers related issues such as privacy.

3. UCON MODEL COMPONENTS

The UCON model consists of three core components and three additional components that are mainly involved in authorization process (see figure 4). Core components comprise subjects, objects, and rights. Each core component can be divided into several detailed components with different perspectives. Traditional access control policies also define similar components to UCON core components though the definitions of these components in various access control policies are somewhat different from each other and from those of UCON. Additional components include authorization rules, conditions, and obligations. In UCON system at least the authorization rules (specifically rights-related authorization rule which will be discussed in this section) have to be included for authorization. Conditions and obligations can also be used in authorization process.

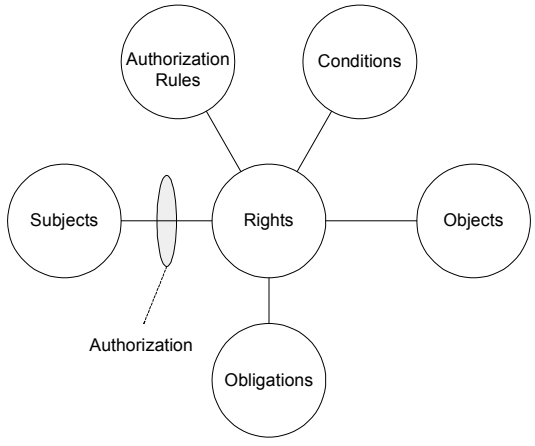

Figure 4. UCON Model Components

3.1 Subjects

Subjects are entities associated with attributes, and hold and exercise certain rights on objects. Attributes are properties of the subjects that can be used for the authorization process. Examples of attributes include identities, roles, credits, memberships, security levels, etc. A subject can be a user, a group, a role, or a process. A user is an individual entity that has certain rights on an object. A group is a set of users who holds same rights as a group. A role is a named collection of users and relevant permissions [12]. Groups and roles may have hierarchical relationships.

In UCON, the subjects can be *consumer subjects (CS)*, *provider subjects (PS)*, and *identifiee subjects (IS)*. Consumer subjects are entities who receive rights and objects and use the rights to access the objects. An e-book reader, MP3 music player/listener and even a distributor of digital objects can be a consumer subject. Provider subjects are entities who provide an object and hold certain rights on it. Examples of provider subjects include an author of an e-book, a distributor of the book, a primary physician, etc. The identifiee subjects are entities who are identified in digital objects that include their privacy-sensitive information. A patient in health care system is an example of an identifiee subject. Although the concept of identifiee subjects always exists in case of privacy-sensitive information, identifiee subjects may or may not be included within UCON systems based on other control policies.

3.2 Objects

Objects are entities that subjects hold rights on, whereby the subjects can access or use objects. Objects are also associated with attributes, either by themselves or together with rights. As for subjects, the attributes include certain properties that can be used for the authorization process. Examples of object attributes are security levels, ownerships, classes, etc. Object classes are used to categorize objects so authorization can be done based not only on individual objects but also sets of objects that belong to same class [11]. In some cases, objects or objects with attributes (i.e., classes) are associated with attributes together with rights. Examples of the attributes for objects with rights are credits, roles, memberships, etc. The credits may be used to define how many credits are required to obtain a certain right on a specific object. For example, “Harry Potter” e-book together with a read right may require $10 or the book with an additional print right may require $15.

In UCON, objects can be either privacy sensitive or privacy non-sensitive. A privacy-sensitive object includes individually identifiable information that can cause privacy problems if not used properly. An UCON object can be either original or derivative. The derivative object in UCON is different from that of other DRM literature. In DRM literature, the term “derivative” means derived (cited, quoted, or copied) from an original work to create another digital work that includes parts of the original work. In UCON, however, the derivative object is an object that is created in consequence of obtaining or exercising rights on an original object. For example, playing MP3 music file can create usage log information. This log data file is called a derivative object in UCON. Like the original object, this derivative object is also considered as an object and also holds UCON properties and relations with other components. Based on their format, objects can be documents (e.g., .doc, .pdf, .ps), audio (e.g., .mp3, .wav), video (e.g., JPEG, DVD, MPEG), executable files (e.g., games), etc. Each may require its own application tools to be used. The objects may or may not have hierarchy on them.

3.3 Rights

Rights are privileges that a subject can hold on an object. Rights consist of a set of usage functions that enables a subject's access to objects. The authorizations of rights require associations with subjects and objects. Rights may or may not have a hierarchy. Like subjects and objects, rights can also be divided into *consumer rights (CR)*, *provider rights (PR)*, and *identifiee rights (IR)*. The rights include rights for access and use of objects and rights for delegation of rights. In this paper, we do not discuss delegation rights. Obviously, there should be further research on delegation rights in UCON in future.

UCON rights can be divided into many functional categories. The two most fundamental rights categories might be a view and a modification. They are denoted as V and M respectively so we write R = {V, M}. Modification includes change to an existing digital object and creation of a new object that reuses an original digital object. The range of V and M is denoted as C = {0,1, α} where "0" means closed to everybody (no one can access), "1" means open to everybody (everyone can access), and "α" means access approval is selective or controlled. The openness of the control or availability of object to public is expressed as $0 < \alpha < 1$ which means that 1 is most open to public and 0 is least open. Here, V and M can be either 0, 1, or α (V = {v| v ∈ C}, M = {m| m ∈ C}). This gives 9 possible combinations of view and modification controls, that is C_{mv} = {(m,v)| m ∈ M, v ∈ V}. However, since a subject cannot modify an object without viewing it, M cannot be more accessible than V, so C_{mv} = {(m,v)| m <v or m=v}. This rules out 3 of 9 combinations resulting in C_{mv} = {(1,1), (α,1), (0,1), (α,α), (0,α), (0,0)}. Since C_{11} means no control and C_{00} means no usage, we further discard these two cases. This gives us four possibilities to consider as follows C_{mv} = {(0,1), (α,1), (0,α), (α,α)}.

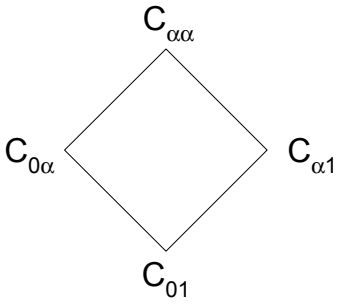

Figure 5. UCON Rights Combinations

Figure 5 shows these four possible combinations of rights control in UCON. α is most complicated to implement and 1 will be the easiest one. Each case may be suitable for different business cases. C_{01} is view only. Sample e-book is an example. In $C_{0\alpha}$, modification is not allowed and view is allowed selectively. E-book or MP3 distributions, digital library with member-only services are some examples. In $C_{\alpha 1}$, view is open to public but modification is allowed selectively. In $C_{\alpha\alpha}$, both view and modification are selective. Note that {(1,0)} is not possible in $C_{\alpha\alpha}$. Healthcare information system can be an example where only authorized doctors can see or update certain patients' data. There have been several studies on functional rights in DRM communities [4, 5, 7, 8]. These rights are developed as part of metadata modeling mainly for commercial business systems such as B2C e-commerce systems. Rather than defining detail of functional rights which will be largely dependent on target business model, we have used simple classifications of rights to provide a foundation for further discussion on rights models for different purposes and different business models.

3.4 Authorization Rules

Authorization rules are a set of requirements that should be satisfied before allowing subjects' access to objects or use of objects. There exist two kinds of authorization rules. They are *Rights-related Authorization Rules (RAR)* and *Obligation-related Authorization Rules (OAR)*. The RAR is used to check if a subject has valid privilege to exercise certain rights on a digital object. Examples include identities or roles verification, capabilities or properties checking, proof of payments, etc. The OAR is used to check if a subject has agreed on the fulfillment of an obligation which has to be done after obtaining or exercising rights on a digital object. Examples include metered payment agreement, usage log report agreement, etc. The authorization rules are different from conditions. The 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 the condition is used to check whether existing limitations and status of usage rights on an object are valid and whether those limitations have to be updated.

3.5 Conditions

Conditions are a set of decision factors that the system should verify at authorization process along with authorization rules before allowing usage of rights on a digital object. There are two types of conditions: *Dynamic conditions* and *Static conditions*. Dynamic conditions include information that may have to be checked for updates at each time of usage. Static conditions include information that does not have to be checked for updates. Dynamic conditions are stateful and the static conditions are stateless. Some examples of dynamic conditions are the number of usage times (e.g., can read 5 times, can print 2 times), and usage log (e.g., already read portion cannot be accessed again). Some examples of static conditions are accessible time period (e.g., business hours), accessible location (e.g., workplace), and allowed printer name.

3.6 Obligations

Obligations are mandatory requirements that a subject has to perform after obtaining or exercising rights on an object. In real world implementation, however, this may have to be done by agreeing on the fulfillment of obligations before obtaining the rights and at the time obligation-related authorization rules are checked. For example, a consumer subject may have to accept metered payment agreements before obtaining the rights for the usage of certain digital information or should agree on providing usage log information to a provider subject before reading an e-book or listening a music file. Traditional access control has hardly recognized the obligation concept. Recent DRM solutions are likely to include obligation functions though many of them implement the obligation functions only partially and implicitly.

4. ACCESS CONTROLS AND AUTHORIZATIONS IN UCON

In UCON, authorization rules, conditions, and obligations are involved in authorization process. Based on the involvement of these components, UCON has 4 possible cases for authorization processes. Figure 6 shows these variations. Note that a higher case includes all the lower cases' components in its authorization process. A0 is authorization with rights-related authorization rules only. Traditional authorization processes fall under this case. Traditional access control and trust management utilize this case in their authorization process. We can support Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role-based Access Control (RBAC) with A0 authorization process. A1 is authorization with conditions. In A1, RAR and conditions are utilized for authorization process. By utilizing conditions as part of authorization process, A1 case provides finer grained authorizations. A2 is authorization with obligation and obligation-related authorization rules (OAR). A2 utilizes obligation and OAR as well as RAR for authorization process. By including obligation concepts in authorization process, A2 can provide better enforcement on exercising usage rights for both provider and consumer subjects. A3 is authorization with both conditions and obligations. This also includes RAR and OAR. Many DRM solutions utilize both conditions and obligations though they may not explicitly define these components. In most DRM solutions, RAR doesn't utilize access control policies because of their payment-based authorization process. In UCON, both payment-based authorizations and access control policy based (or payment-free) authorizations are covered. In this paper, we further discuss A0 authorization process because this is where traditional access control policies and basic authorization process of DRM solutions are covered.

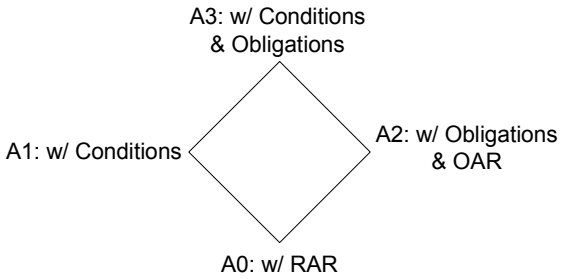

Figure 6. UCON Authorization Combinations

In UCON model, subjects (S), objects (O) and objects with rights (O + R) can be associated with certain attributes (At). In UCON A0, authorization process can be done in three ways based on the kinds of attributes used in authorization rules (AR). These three ways are as follows.

- Case 1: R(S,O) = AR(At(S), At(O))
- Case 2: R(S,O) = AR(At(S), At(O + R))
- Case 3: R(S,O) = AR(At(S), At(O + R)) + AR(At(S), At(O))

Here, R(S,O) means a set of authorized rights for subject S on object O. In case 1, authorization is done by checking certain authorization rules based on subjects' attributes and objects' attributes. In case 2, attributes of subjects and attributes of objects with rights are used in authorization rules for authorization. In case 3, attributes of subjects, attributes of objects, and attributes of objects with rights are used for authorization process.

Access control policies can be explained in UCON authorization process as parts of A0 authorization. In classical mandatory access control policies, authorization is governed on basis of security level of subjects and objects in the system. MAC policies can be enforced in UCON by using these security levels as attributes of subjects and objects components so these attributes can be compared based on authorization rules. Bell-LaPadula's security properties [2, 10] such as no read up or no write down (or together with no write up) can be included in authorization rules.

- MAC policies in UCON authorization:
  R(S,O) = SecurityProperty(securityLevel(S), securityLevel(O))

Discretionary access control also can be supported in UCON authorization. In UCON, the subjects can be users, groups, processes, etc. Unlike MAC, in most DAC literature, users and subjects are used interchangeably without clear distinctions in their definitions. DAC policies govern the access of users to the object based on the identity of users or group of users and identity of objects or group of objects. The access modes such as read, write, or execute are granted to a user if the user has privilege to use a specific access mode on an object. Either access control list (ACL) or capability list can be used for authorization rules.

- DAC policies in UCON authorization:
  R(S,O) = ACL/Capabilities(ID/groupID(S), ID/groupID(O))

The UCON model also can support role-based access controls in its authorization process. In RBAC, role is a collection of users and a collection of permissions. The permission is a collection of objects and rights. In UCON, role can be assigned to attributes of subjects and attributes of objects with rights. Within permission, if rights are associated with classes of objects, each object doesn't have to be assigned to rights explicitly. In addition to this, identity information can be used as an attribute of object. This can provide fine-grained access of roles. For example, with a professor role, professor Dolittle may have to have rights to read GPA records of all students in school. Certainly, in addition to read rights, he may also need to update students' grades but only grades of those who take his classes. By using multiple attributes on both objects and objects with rights, UCON can apply finer-grained role-based access control. Constraints can be used for authorization rules. They may include role hierarchy, separation of duties, etc. As shown below, role is already assigned to subjects and permissions (O + R). The UCON authorization doesn't cover RBAC administration process. Permission-role assignment and User-role assignment should be handled in UCON administration models which are not discussed in this paper.

- RBAC in UCON authorization:
  R(S,O) = Constraints(Role(S), Role(O + R))
  R(S,O) = Constraints(Role(S), Role(Class(O) + R))
  R(S,O) = Constraints(Role(S), Role(O + R))
  + Constraints(ID/groupID(S), ID/groupID(O))

Authorization process in commercial DRM solutions usually involves payment, not traditional access control policies. DRM doesn't have any distinction of subject and users in its usage.

Authorization is done when a subject holds enough credit to use certain rights on specific objects. This can be applied in UCON authorization process by using credits as attributes of subjects and objects. In addition, there can be other properties such as memberships that can be used in accordance with credit for authorization process.

- DRM authorization in UCON
  R(S,O) = creditCompare(Credit(S), Credit(O + R))

In this section we have demonstrated how traditional access control policies and DRM authorizations can be mapped into UCON authorization process. Obviously, there can be other authorization processes based on different authorization policies.

5. APPLICATIONS IN UCON

Digital objects that have to be protected in information system are likely to have relationships with consumer, provider, and optionally identifiee subjects. Each side has its own rights on the objects. To protect their own rights, each side may need to limit usage of the rights of other sides. To apply the UCON model in real world, we have to separate these subjects by putting the objects component at the center of the model diagram and by having each subject on one side of the objects component. Using this separation of subjects, UCON clearly shows relationships between subjects and objects and between subjects themselves. This separation is shown in figure 7 and 8. Figure 7 is a UCON model diagram for privacy non-sensitive objects and figure 8 is for privacy sensitive objects. The UCON model for privacy sensitive objects includes an additional subject called identifiee and relevant rights. Figure 7 and 8 are based on the following legends.

PNO: Privacy Non-sensitive Object
PSO: Privacy Sensitive Object
Cx: Consumer x
Px: Provider x
Ix: Identifiee x
yR: y Rights
yAR: y Authorization Rule
yC: y Condition
yOB: y Obligation
where x = {x| R, AR, C, OB}, y = {y| C, P, I}

We will use 2 examples and demonstrate how UCON models can be applied for privacy non-sensitive and privacy sensitive digital information. One simple example is a popular MP3 music file distribution. This example can be explained with Figure 7 that has provider and consumer subjects sides. Suppose a music composer (say Bob) wants to sell his new song through a distributor, and a buyer (say Alice) wants to buy the song from the distributor. In case of the relations between Bob and the distributor, Bob will be a provider subject (PS) and the distributor will be a consumer subject (CS). Bob will have certain provider rights (PR) that are agreed at the time of a contract with the distributor. The distributor will have rights (CR) to distribute the MP3 song (PNO) and get certain profits from the sales. Likewise, in case of Alice and the distributor, Alice will be a consumer subject and the distributor will be a provider subject. Then Alice has rights (CR) such as play right for the song and the distributor will have rights (PR) such as copy and disseminate rights on the object. In this case, Alice may be required to pay ahead (CAR) to obtain a play right but only on a specific player (CC) which is selected by her. In addition, she may have to agree on submission of her usage log report to the provider (COB). On the other hand, the distributor can have rights to collect consumers' usage log information. This shows that in UCON system, a consumer's obligation is likely to be a provider's right and vice versa.

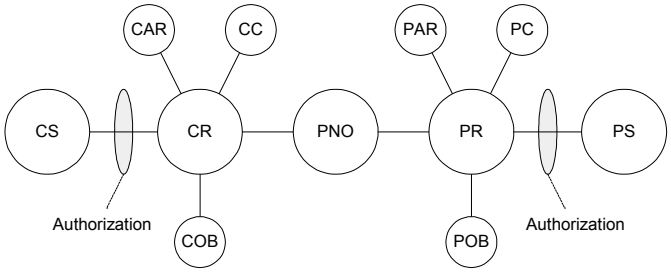

Figure 7. UCON Model for Privacy Non-sensitive Objects

One good example for the control of privacy sensitive objects might be a healthcare system. We consider a healthcare system called PCASSO to demonstrate the UCON model for privacy sensitive objects. The PCASSO project is developed by UC San Diego and SAIC under the support of NIH [1]. The main purpose of the project is to develop a healthcare system that provides secure access to highly sensitive patient information over Internet. Access control of PCASSO mainly utilizes labels and roles. Patient records are labeled with one of 5 security levels including Low, Standard, Deniable, Guardian Deniable, and Patient Deniable. As a provider subject, the primary care provider provides patient medical record (PSO). In addition, the primary care provider decides security level of patient medical information. Care providers (primary, emergency or others), guardians, researchers, and even patients can be consumer subjects. In PCASSO, the patient role can be either a consumer subject or an identifiee subject. As a consumer subject, a patient can read his medical record if it is not patient deniable. As an identifiee subject, the patient can review (IR) access log information on his record. Note that the patient doesn't have rights to decide use and disclosure of his medical information in PCASSO.

According to recent regulation called the Privacy Rule from the US Department of Health and Human Services (HHS), healthcare providers such as doctors, hospitals are required to obtain a patient's written *consent* before using or disclosing the patient's personal healthcare information to carry out treatment, payment, or healthcare operations (TPO) [6].* To use or disclosure the patient's medical information for other reasons than TPO, healthcare providers are required to obtain written *authorization* documents. In Privacy Rule, authorization is more detailed and specific than consent. In PCASSO, neither consent nor authorization is included in the system. Moreover, usage and disclosure of patient medical information is entirely up to a primary care provider. For better control of all parties on patients' healthcare information and for better privacy protection, these consent and authorization should be part of identifiee rights in UCON model. Also, it should be the patient who holds those identifiee rights.

* The Privacy Rule became effective on April 2001. Most health plans and health care providers that are covered by this rule must comply with new requirements by April 2003.

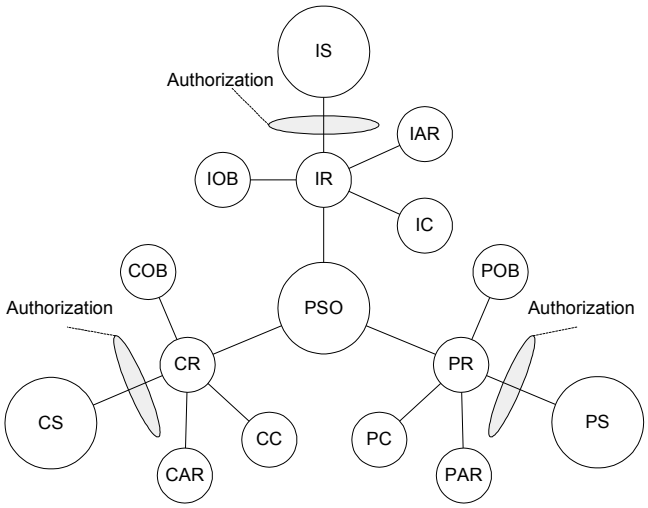

Figure 8. UCON Model for Privacy Sensitive Objects

6. REVERSE UCON

As mentioned above, obtaining or exercising usage rights on a digital object may create another digital information object (derivative object) which also needs controls for the access to and usage of it. Some examples are payment info, usage log, etc. The usage control on these derivative objects is reversed in its control direction in such a way that the provider subject becomes a consumer subjects and vice versa. This reversed usage control is called reverse UCON and the rights are called reverse rights. Furthermore, obtaining or exercising the reverse rights on these derivative objects may also creates another derivative objects and reverse (more correctly inverse) rights on it.

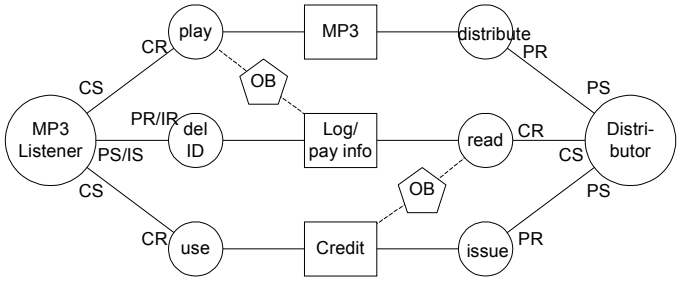

Figure 9. An Example of Reverse UCON

Figure 9 shows an example of reverse UCON. Some components are omitted in this diagram for the sake of simplicity. Suppose Alice wants to listen a MP3 music file. To obtain play rights, she as a consumer subject (CS) may have to agree on payment-per-play (OB: obligation) and provide credit card information. Upon her exercise of the play rights, she has to report her usage log on the MP3 file (OB). In UCON, this payment information and log information are also considered as objects (derivative objects) and as part of UCON model. Now Alice becomes both a provider subject (PS) and an identifiee subject (IS) of the log/payment information and may hold certain rights (PR and IR) on them such as a right that she can delete her ID of log information. The distributor may have rights to collect log information either by putting an obligation on consumer rights or by giving consumer rights to get some store credits on log reports. If Alice has rights to get some store credit based on her play times, then it is now distributor's obligation as a provider subject to issue certain credit to Alice.

Control and protection of rights and usage of rights on the derivative objects have been hardly recognized or discussed in information security literature. In UCON, reverse UCON can be viewed as part of the UCON model and is not different from ordinary UCON in its model specifications. In general, derivative objects are likely to include privacy-related information. Adequate controls on derivative objects will be crucial for better privacy treatment. By handling derivative objects in UCON system, at least security and privacy issues can be discussed systematically within a common framework.

UCON systems are likely to be implemented and managed under the control of one of three subject sides: consumer, provider or identifiee. This implies it's hard to guarantee availability of adequate control mechanisms implemented for the other two sides on the rights and usage of rights. There can be also a third party who develops/manages UCON system on behalf of all of PS, CS and IS sides. Therefore, to make a sound reverse UCON system available, there should be either a voluntary commitment from a development/management group or legal enforcement. In its implementation, UCON system may have to include following mechanisms for reverse UCON.

- To provide ability to review detail of derivative objects which are going to be created.
- To provide ability to refuse creation of derivative objects (the consumer may have to give up or reduce exercising original rights).
- To provide ability to restrict reverse usage by blocking certain part of derivative objects (i.e., identity) or by allowing only aggregated information of individual objects.
- To provide ability to monitor reverse usage on derivative objects (this may cause another round of reverse UCON).

7. CONCLUSION AND FUTURE WORK

In this paper we have introduced a new concept called usage control for controlling access to and usage of digital information objects. Usage control encompasses traditional access control, trust management, and digital rights management and goes beyond them in its scope. By unifying these three areas, UCON offers a promising approach for the next generation of access control. UCON model covers both security and privacy issues of current business and information systems requirements in a systematic approach. In this paper we have provided a foundation for further research and development on UCON as well as a promising future direction of access control.

Obviously, what we have presented in this paper is not a complete model description. We notice that delegation of rights is one of crucial issues that should be covered within UCON model. In addition, there should be a clear description of administration issues. We believe by developing more concrete models and by articulating delegation and administration issues in the models, UCON will provide more comprehensive solution approaches for the area of usage control.

Acknowledgement

The work of both authors is partially supported by the National Science Foundation.

8. REFERENCES

[1] Baker, Dixie. et al., "PCASSO: Applying and Extending State-of-the-Art Security in the Healthcare Domain", Proceedings of the Annual Computer Security Applications Conference, 1997.

[2] Bell, D., and La Padula, L., "Secure Computer Systems: Mathematical Foundations and Model", MITER Report, MTR 2547 v2, Nov. 1973.

[3] Blaze, Matt., J. Feigenbaum and J. Lacy., "Decentralized Trust Management", Proceedings on IEEE Symposium on Security and Privacy, 1996.

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

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

[6] Department of HHS, "Standards for Privacy of Individually Identifiable Health Information", Online, Available: http://aspe.os.dhhs.gov/admnsimp/final/pvcguide1.htm, 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/people/k/kaplan/cryptolope-docs /crypap.html.

[10] Sandhu, Ravi. "Lattice-Based Access Control Models." IEEE Computer, Volume 26, Number 11, November 1993, pages 9-19

[11] Sandhu, Ravi., and Samarati, Pierangela., "Access Control: Principles and Practice" IEEE Communication Magazine, pp 40 – 48, September 1994.

[12] Sandhu, Ravi., Edward Coyne, Hal Feinstein and Charles Youman, "Role-Based Access Control Models." *IEEE Computer*, Volume 29, Number 2, February 1996, pages 38-47.

[13] Schneck, Paul., "Persistent Access Control to Prevent Piracy of Digital Information", Proceedings of the IEEE, Vol. 87, No. 7, July 1999.

[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] Week, Stephen., "Understanding Trust Management Systems", Proceedings on IEEE Symposium on Security and Privacy, 2001.

[16] Winsborough, William., Kent Seamons and Vicki Jones., "Automated Trust Negotiation", Proceedings of the DARPA Information Survivability Conference and Exposition 2000, 1999.