Usage control: a solution to access control in a distributed- network-connected environment

Patricia Ghann*, Changda Wang and Conghua Zhou
School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang, Jiangsu, 212013, China
*Corresponding author: pghann@gmail.com

***Abstract*—Computer and information technology has evaded our every aspect of life. Information technology is seen in all aspect of the individual from banking and investing to shopping and communicating through the use of the internet services such as emails and chat rooms. Organizations and industries also utilize computer and information technology to collect information on individuals leading to the creation of warehouse of databases that enable them to achieve their objectives. In a distributed network environment today, information security is a very important issue in ensuring a safe computing environment.**

Keywords-Access control, Usage control, Transition state, Obligation, Digital resource

I. Introduction

Information security as it is well known is aimed at ensuring Confidentiality, Integrity and Availability (CIA) in the use of information resources.[1][13] By confidentiality implies the need to protect information from unauthorized users; integrity is to prevent unauthorized modification of information while availability is to ensure that information is available and accessible to only authorized users. Over the years, research on information security has focused on controlling the use of information resource through various models that have been proposed; from traditional access control, with its derivatives such as MAC, DAC, RBAC to TM and DRM. [1-10]Access control has been a key component of security solution to supporting fine-grained articulated protection for shared data and resources by known users in a closed environment in the past. Trust management has worked on traditional access control by considering unknown users with regards to their credentials. The issue however is that, traditional access control has dealt with the protection of information resources in a closed environment by authorizing only known users. Trust management though gives consideration to unknown user, fails to protect information resources after dissemination and has focused only on sensitive information while ignoring B2C systems. Obviously the introduction of DRM sought to address the short falls of these earlier models, nevertheless it only concentrated on target problem like intellectual property right, using a client-side reference monitor as opposed to server-side reference monitor in traditional access control and trust management.[5-8][10] Even so, these earlier access control models have contributed tremendously in their own way to ensure confidentiality, integrity and availability in information security. With the advancement in computer and information technology, resulting in a complex distributed network connected environment, where information resource or digital resource is available and accessible through various devices such as personal digital assistants(PDAs), mobile phones, smart-cards, MP3 players to personal and mainframe computers, traditional access control such as mandatory access control(MAC), discretionary access control(DAC) and role-based access control(RBAC) have been found by researchers to be inadequate in the protection of digital or information resources.[1][5-9][13] As previously mentioned, Trust management and Digital right management have focused on target issues in their own perspectives. Therefore the need for a complete and comprehensive model, to ensure absolute protection of digital or information resource in a distributed network environment such as it is currently, has been inevitable. Usage control proposed by Sandhu and Park (2002), Park (2003) and Zhang (2006) seems to address most of the short falls of earlier models of access control and goes beyond in providing a comprehensive model that encompass previous models in an attempt to help solve the various challenges to information security currently.[5-8] This paper emphasizes on the significance of usage control in information and digital resource protection and the need for it implementation in industries and organizations such as B2B and B2C. Currently more critical than ever, industries and organizations need to share information or digital resources with many different parties, and yet have to guarantee that business-critical and privacy-sensitive information resources are not leaked to unauthorized parties or users.[8-10] The rest of this paper is structured as follows. Section 2 talks about traditional access control. Section 3 is about prior work, 3.1 talks about the shortfalls of traditional access control. Section 4 is about usage control, section 4.1 and 4.2 talks about Ucon model components and the main idea behind Ucon accordingly. Section 5 is about the transitions states of Ucon, 5.1 talks about enforcement of obligations in Ucon and section 6 and 7 is about conclusions and references respectively.

II. Traditional Access Control

Access control determines which subjects can access which resources under which circumstances. In the history of computer and information security, various attempts have been made to ensure trusted control in

Published by Atlantis Press, Paris, France.

terms information or digital resource usage. The earliest approach has been traditional access controls such as mandatory access control (MAC), discretionary access control (DAC) and role-based access control (RBAC).[1][5-8] In a distributed networking environment recently, access control still remains a major challenge for computer and information security. Providers of services, resources and digital content need to selectively determine who can access these and exactly what access is provided. Hence the objective of access controls. There has been much research with progress in access control for the past thirty years with emphasis centered on access control matrix. The concept of the access matrix is that a right is explicitly granted to a subject to access an object in a specific mode for example, read or write mode. This right exists whether or not the subject is currently accessing the object. It is also a presumption that, the right enables repeated access until it is finally revoked. According to research, access matrix is not explicitly represented in practical terms. Instead access control lists (ACLs), capabilities or access relations are used. A variety of DAC, MAC and RBAC models have emerged to accommodate a diverse range of real-world access control policies.[7-10] However, the practice of access control has grown very far away from the access matrix abstraction; nonetheless the core idea that, access is driven by rights granted to a subject to access an object had still remained. Traditionally, access control has focused on the protection of computer and information resources in a closed system environment. The enforcement of control has been primarily based on identities and attributes of known users by using a reference monitor and specified authorization rules [15]. In today’s network-connected, highly dynamic and distributed computing environments, digital information is likely to be used and stored at various locations, hence has to be protected regardless of user location and information location. Relaxing closed system requirement introduces the need to control access by previously unknown users.

III. PRIOR WORK

Trust management emerged as an enhancement on traditional access control by giving consideration to unknown users and utilizing their credentials in an open environment. However it focused on static entities with characteristics that do not change with time. Recent research came out with Digital right management which uses a client-side reference monitor to control usage of already disseminated digital objects. This model has brought out a significant new perspective on access control problems. Various efforts have been made by researchers to ensure trusted client-side computing. For example Microsoft’s Palladium and Intel-driven trusted computing platform alliance (TCPA) [TCPA 2002] originating from AEGIS [7][8][10]. These have gained serious attention and concern because of their potential impacts on security and privacy issues. Because of DRM's potential opportunity for commercial sector; current DRM solutions have been largely driven by commercial entities and are mainly focused on intellectual property rights protection which is based on payment functions. All these models discussed above have tried to protected information or digital resources in one way or another. The fact however remains, in a modernized and computerized era currently, where digital resource are available and can be shared and stored in various devices, these models are inadequate in ensuring access control and hence achieving confidentiality, integrity and availability.

Shortfalls of Traditional access control

Traditional access control models are not adequate for today’s distributed, network-connected digital environment.

- Authorization only – No obligation or condition based control
- Decision is made before access – No ongoing control
- No consumable rights - No mutable attributes
- Rights are pre-defined and granted to subjects

In view of the above enlisted problems of traditional access control, the need to have a flexible access control in a highly dynamic and distributed environment such as currently seems laudable. This is because information or digital resources can be located in various places and thus the need for a general client-side platform. The multi aspect nature of access control decisions in terms of subject and object attributes, obligations, conditions and the dynamism of subject and object attributes has necessitated the need for a more comprehensive model such as usage control by Sandhu and Park[5-8][10].

IV. USAGE CONTROL (UCON)

This is a model that addresses information security challenges faced in a modern application and computer environment by providing richer, finer and persistent controls on information or digital resources as compared to traditional access control policies and models. For example, print once as opposed to unlimited prints.[1][5-8][10] In contrast to traditional access control or trust management, it covers both centrally environment and an environment where central control authority is not available. UCON also deals with privacy issues in both commercial and non-commercial environments. The main advantage of ucon lies in its strength to express diverse access cases.

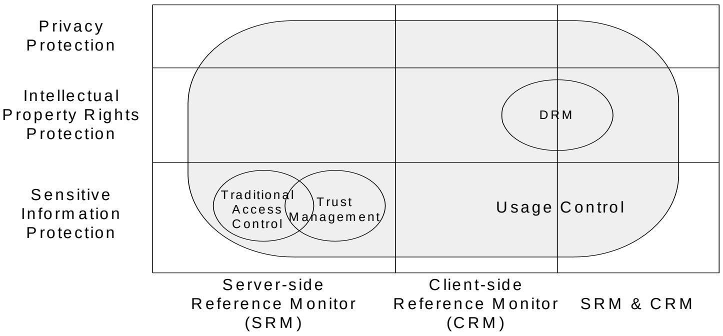
Privacy Protection
Intellectual Property Rights Protection
Sensitive Information Protection
DRM
Traditional Access Control
Trust Management
Usage Control
Server-side Reference Monitor (SRM)
Client-side Reference Monitor (CRM)
SRM & CRM

Figure 1, Coverage of Usage control.

The comprehensive nature of usage control or Ucon can be seen in the fig 1 above. The concept of usage control encompasses traditional access control, trust management and digital right management in a single framework.[1][5-8] As a result of this, Ucon's objectives include privacy protection, intellectual right protection and sensitive information protection. In terms of domain control and reference monitor, Ucon authorization system can be situated either on server-side reference monitor or a client-side reference monitor or on both. 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. This is always running and tamper resistant. This architecture provides a two-tier usage control over digital resources.

A. Ucon model Component

Ucon consist basically of eight components. These are subject, subject attributes, object, object attributes, right, authorization, obligation and condition. Authorization, obligation and condition are known as functional predicates. The uniqueness of ucon is the concept of mutability and continuity [1][5-8][10][11] which would be discussed later.

The next section describes these main componenet of Ucon as illustrated in fig 2 below.

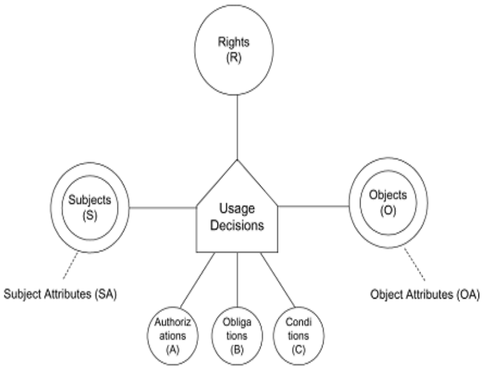

Figure 2 Ucon Model Components

1) Subject(S) and Subject Attributes (ATT(S))

A subject is an entity or a resource requester associated with attributes and holds or exercise rights on the target resource (object). Thus in usage control, an individual human being can be regarded as a subject in simple terms.[7][10] Subject attributes on the other hand refers to properties or capabilities that can be used in decision process. For example identities, group names, security clearance, roles, membership etc. There are three types of subjects based on the usage purpose. Consumer subjects (CS) are those who access an object or resource for consuming reasons for example a MP3 music listener. Provider subject (PS) is where the object resides and administers as well as enforces security on object. An identifiee subject (IS) possesses some kind of right on an object because it contains private or sensitive data of the identifiee for example patients in a health care system. This paper gives attention to consumer subject and hence uses the term subject to represent a requester.

2) Objects.(O) and Object Attributes (ATT(O))

Objects are entities that a subject holds or exercise right on. In other words, subject uses or accesses object. Object attributes are properties used in decision process such as the number of previous usage, the resource type, the security label etc. Object can also be classified as follows, target object; computational resource, network resource, digital information which may be copied, modified and distributed in network-connected computer environment, privacy sensitive and privacy non sensitive object and finally as original or derivative object.[1][7][8]

3) Rights(R)

These are privileges that a subject can hold and exercise on an object. It consists of a set of usage functions that allows a subject an access to a target object. Like subject and object, right can also be classified as consumer right(CR), provider right(PR) and identifiee right(IR). Ucon rights are similar to right in traditional access control expert that in Ucon, right does not exist in access matrix independently from a subject's activity. Instead the existence of right is determined when there is an access attempt by a subject and this depends on subject, object and environmental attributes as well as authorization, obligation and conditions.[5-8]

B. Main idea behind ucon

The main idea behind ucon is that, in ucon, policy statement as well as access decisions are based on three main factors; authorization, obligation and conditions in addition to continuity of access and mutability.

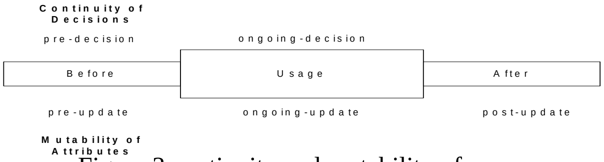

Figure 3 continuity and mutability of ucon

Mutability of attribute implies that subject and object attribute can change in time during access and this determines whether access should continue or not. In other words, ucon model enforces a security policy execution of access, during execution of access and after access execution. Therefore if access attributes are change while access is in progress and the security policy is not fulfilled, the Ucon authorization system revokes access granted and hence terminates usage [1][11].

1) Authorization This is a functional predicate over attributes that has to be evaluated for usage decision and indicate whether the subject is allowed to perform a requested right on an object or digital resource. Though traditional access controls utilized authorization, ucon authorization however can be pre-authorization(preA) or on-authorization(onA). PreA means that authorization is evaluated before access just like in traditional access control, while onA means authorization is done during the execution of access. Thus authorization predicate exert constraints on subject and object attribute in a form of logic predicate.[19]

2) Obligations These are functional predicates that verify compulsory requirement that a subject needs to perform either before, during or after an execution of access.[1-8] For instance, in order to access a company's white paper, a user is required to sign a privacy policy, to watch an advertisement in the cause of reading the paper and also to delete the paper from his or her computer within 10 days if user likes to download the paper.[1] As mention previously, obligation can be before during or after execution of access. Furthermore it also associates with access rights as well as with attributes of both subjects and objects, thus enabling flexibility and granularity in complicated usage cases. According to [1][2][4][22] obligations can also be viewed as follows; (A) Who must perform obligation actions, (B)To whom obligation should be applied, (C) When obligations should be performed and finally (D) A time period within which obligations needs to be fulfilled. A and B are referred to as the obligation subject(OBS) and obligation object(OBO) accordingly. The (OBS) refers to the entity that needs to perform the obligation action(OBA), while the (OBO) is the object on which the action is being performed. The relationship among these components was not specified in the original ucon model nonetheless, the obligation subject and the obligation object are not the same as the subject and object respectively. In reality, obligations are based on subjects and object attributes and also access rights in most security policies. But the fulfillment of obligation depends on the obligation subject and obligation object[1-4]. C refers to the obligation execution time; that is either pre, on or post obligation. D concerns the time within which obligation must be fulfilled by a subject. Based on the aforementioned, [1,2] define obligation as a tuple presented by OBL = (OBS, OBO, OBA, WHEN and DURATION). In my opinion however, the tuple should include condition C. This is because conditions must be favorable to fulfill obligations.

3) Conditions These are environmental attributes very crucial for access decision process. Though not directly related to subject and object attributes and not given so much significance in most access control literature. Without these environmental attributes, there would be no access decision. Conditions can be pre or ongoing as proposed by the original ucon model.[5-8] However the model does not consider the dynamic nature of these environmental attributes and their effects on access control decisions. For instance what happens to access decision in the case of system failure due to power outage or a unforeseen event and what effect has this, on the other access control functional predicated introduced previously.

V. Transition state of Ucon

According to the original ucon model, the following transition states are identified in the fig 4 below.

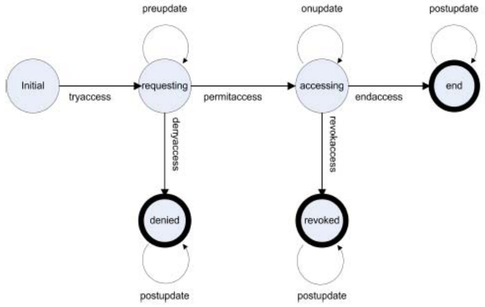

Figure 4 Transitions of ucon

The states include the following; initial, requesting, accessing, denial, revoked and end states.[1][2-8] The initial state is the original or natural state of the system. This implies that at this state, access request is not generated. Requesting state indicates that access has been generated but is however waiting for usage decisions by the system. Denial state occurs when the system upon considering it usage decision is not satisfied. Accessing state implies the system has granted access and consequently subject or user is accessing the target object. The ucon model illustrate that termination of access is in two folds; either by revolking access due to the fact that the system is no more statisfied with subject's action or the subject ends the session normally. ucon supports decision continuity which implies that during a usage session, multiple ongoing checks could occur. Nonetheless in the transition state in fig 4, this is not captured. As it does not explicitly illustrate these ongoing checks as well as ongoing transitions.[1-2] Hence the proposal of expanded Ucon state transitions. According to [2], fig 4 does not indicate the actions that triggers an ongoing decision checking during usage session. Thus the state in which the system checks policy rule, in the course of a session, similar to the requesting state is not illustrated or mentioned; indicating that the accessing state and the state concerned with checking ongoing policy rules have been merged and termed as the accessing, while the trigger action that triggers the reevaluation of attributes is hidden. As a consequent, an expanded model of state transition of ucon, where the accessing state of original ucon is divided into two states; accessing and ongoing checking in that order is put forward. Thus indicating that, triger action transit the system from the accessing state to the ongoingcheck state. This is illustrated in fig 5.

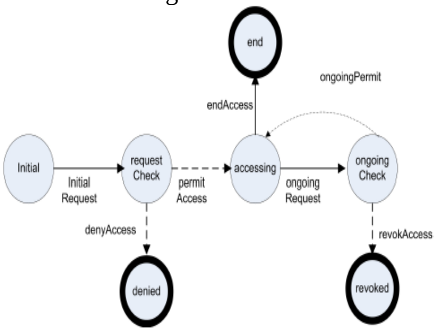

Figure5 Expanded Ucon state transition

From fig 5, [2], considers actions/transition as system obligation indicating that, the required updates are stated in the obligation rule of the corresponding state. Thus when update obligation is controllable, then there is no need for fulfillment check. [2] Also introduces a new state; ongoingCheck state and two transitions namely; ongoingRequest and ongoingPermit. Thus, when a user or subject is exercising the access to a resource, the system is seen to be in the accessing state. Due to this, any changes or update of subject, object or environment attributes would trigger ongoingRequest transition and consequently move the system to ongoingCheck state; where decision such as onA, onB and onC or a combination of any is made and new set of attributes would have to be evaluated. Also the system can revoke usage through revokeAccess transition or continuously grant access to the subject through ongoingPermit transition after the system returns to the accessing state. This implies that, update occurs in the ongingCheck state directly and has no effect what so ever on the current evaluation as the new update would be checked in the accessing or revoked state later on. The issue however is that, both of these models has not considered the situation where in the course of accessing a resource, there is a power failure or system failure and the effect of this on the transition state as well as the reputation of the subject since environmental attribute are not static.

1) Enforcement of oBligation of ucon

With the increasing use of modern communication technologies in both the public and commercial sectors, adequate handing of personal data is of a serious concern. This is due to the fact that, data is distributed across many public and commercial databases and stored in many applications.[2-4] In order to ensure, controlled usage of data, usage control in its core model introduced oBligations which must be fulfilled during usage decisions in order to determine the continuity or termination of access to a digital resource as mentioned previously.

For instance a distributed system is said to be made up of a set of actors. An actor here implies an information system or an information device such as a mobile phone possessing the following characteristics: an owner; who is responsible for the behavior of the actor and exist in an encapsulated state; indicating that one actor cannot observe the state as well as the operations of another actor. Also an actor can take an action which basically consists of operations on data. These actions could be storage, distribution, different kinds of read access (including playing music or watching videos), modification of payload and metadata as well as processing such as computation of statistics. Another type of action is communication; involving the sending and receiving of messages that are otherwise not subject to usage control. For example request for digital resource or notification. Considering the mobile computing field, an actor can have changing roles from time to time.

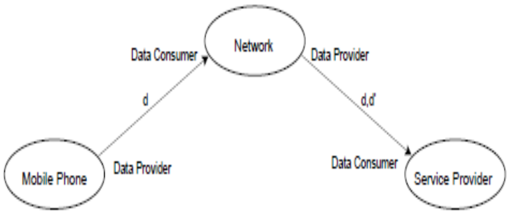

Figure 6 changing role of an actor

Fig 6 is a location-based service with location information d coming from a GPS receiver in a mobile phone. In order to provide the service, the network infrastructure in turn requests location from the mobile phone. Here the mobile phone is considered as the data provider and the network infrastructure as the data consumer. d is then sent to a service provider possibly with other data d^1 for further processing. In this situation, the network infrastructure now becomes the data provider where as the service provider is now regarded as the data consumer. In the above example, the owner of the mobile phone, who is also a subscriber might want to issue some restrictions base on what happens to the data once it is given to the network infrastructure. For instance, if the subscriber requires that data be deleted by service provider after processing, the network infrastructure would have to stipulate this requirement in a policy when giving the location data to the service provider. Thus in order to ensure the controlled usage of data or digital resource, the owner of data or digital resource must specify the necessary requirement globally or on a per-transaction basis that must be satisfied by subjects. This requirement is expressed in a laid down policy and can be of four types with regards to sources. The data provider's or owner's own interest, the data owner's preferences, governing laws and regulations or agreement with another actor who has previously sent the data. According to [2-4], these requirements can be classified into two as, provisions and oBligations. Provisions are the requirements or conditions that concerns with the past and present or requirement that needs to be satisfied before authorization. This has however been dealt with greatly by traditional access control. OBligation on the other hand is a new concept of usage control. It refers to future requirements or conditions that have to be fulfilled by the subject or system after decision has been made. In other words, obligations put constraints on operations of data with respect to time, cardinality, the occurrence of certain events, actions, the purpose for which data is used, technical or governance restrictions and the importance of updates. In terms of enforceability, [13][22] also classify obligations as controllable obligations, non-controllable obligations, observable and non-observable obligation. Controllable obligations are obligations for which the data provider can ensure that, the subject executes respective operations only under the specified restrictions. These are also referred to as system obligations and can be achieved by using trusted platform such as the one used in DRM. In contrast to this are observable obligations which the data provider can observe to see if they are been adhere to. Mechanism for observing the fulfillment of obligations ranges from non-technical such as audits to technical mechanism that employ the use of trusted system to alert data providers of the actions of a subject or consumer, for example a trusted logging mechanism or the use of watermarks to identify the source of illegal copies. In cases where it is difficult to detect, for example whether a data has for a matter of fact been deleted or destroyed by a subject, observability could be exploited for enforcement. Thus the data provider can observe to see whether an approximation of an obligation is violated and hence take a compensating action. This may be in the form of rectifying the violation through penalty like lowering the trust or the credibility rating of the subject or even through some form of legal action.

VI. CONCLUSIONS

Though usage control is a breakthrough as compared to traditional access control models used in the past, in a distributed network connected environment as such currently, the implementation and enforcement of it lies greatly on users of digital resource, providers of digital resources and the designers of information systems or device. To achieve the objective of usage control everyone has to play their part since that is the only way to ensure confidentiality, integrity and availability of digital resources.

REFERENCES

[1] A.Lazouski, F.Martinelli, P.Mori, Usage Control in Computer Security: A survey. 2010.

[2] B. Katt, X. Zhang, R. Breu, M. Hafner, J.-P. Seifert, A general obligation model and continuity: Enhanced policy enforcement engine for usage control, in: SACMAT.08: Proceedings of the 13th ACM Symposium on Access Control Models and Technologies, ACM, New York, NY, USA, 2008.

[3] Claudio Bettini, Sushil Jajodia, X. Sean Wang, Duminda Wijesekera, Obligation Monitoring in Policy Management

[4] M. Hilty, D. Basin, A. Pretschner, On obligations, in: Proceedings of ESORICS 2005.

[5] J. Park, Usage control: A unified framework for next generation access control, Ph.D. Thesis, George Mason University, Fairfax, VA, USA, 2003.

[6] X. Zhang, Formal model and analysis of usage control, Ph.D. Thesis, George Mason University, Fairfax, VA, USA, 2006.

[7] J. Park, R. Sandhu, The UCON ABC usage control model, ACM Trans. Inf. Syst. Secur. 7 (1) (2004) 128.174.

[8] J. Park, R. Sandhu, Towards usage control models: Beyond traditional access control, in: SACMAT.02: Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies, ACM, New York, NY, USA, 2002, pp. 57.64.

[9] R. Sandhu, K. Ranganathan, X. Zhang, Secure information sharing enabled by trusted computing and PEI models, in: ASIACCS.06: Proceedings of ACM Symposium on Information, Computer and Communications Security, ACM, New York, NY, USA, 2006.

[10] R.S. Sandhu, J. Park, Usage control: A vision for next generation access control, in: MMM-ACNS, in: Lecture Notes in Computer Science, 2003.

[11] J. Park, X. Zhang, R.S. Sandhu, Attribute mutability in usage control, in: DBSec, Kluwer, 2004.

[12] W. Yao, K. Moody, J. Bacon, A model of OASIS role based access control and its support for active security, in: SACMAT.01: Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies, ACM, New York, NY, USA, 2001.

[13] A. Pretschner, M. Hilty, D. Basin, Distributed usage control, Commun. ACM 49 (9) (2006) 39.44.

[14] X. Zhang, F. Parisi-Presicce, R. Sandhu, J. Park, Formal model and policy specification of usage control, ACM Trans. Inf. Syst. Secur. 8 (4) (2005) 351.387.

[15] S.D.C. di Vimercati, S. Paraboschi, P. Samarati, Access control: Principles and solutions, Softw. Pract. Exper. 33 (5) (2003) 397.421.

[16] R. Sandhu, Engineering authority and trust in cyberspace: The OM-AM and RBAC way, in: In Proceedings of 5th ACM Workshop on Role Based Access Control, ACM, 2000, pp. 111.119.

[17] W. Ku, C.-H. Chi, Survey on the technological aspects of digital rights management, in: Information Security, 2004, pp. 391.403.

[18] H.L. Jonker, S. Mauw, J.H.S. Verschuren, A.T.S.C. Schoonen, Security aspects of DRM systems, in: 25th Symposium on Information Theory in the Benelux, 2004, pp. 169.176.

[19] M. Sastry, R. Krishnan, R. Sandhu, A new modeling paradigm for dynamic authorization in multi-domain systems, in: communications in Computer and Information Science, vol. 1, Springer, Berlin, Heidelberg, 2007, pp. 153.158.

[20] L. Lamport, The temporal logic of actions, ACM Trans. Program. Lang. Syst. 16 (3) (1994) 872.923.

[21] W. Shin, S.B. Yoo, Secured web services based on extended usage control, in: PAKDD Workshops, in: Lecture Notes in Computer Science, vol. 4819, Springer, 2007, pp. 656.663.

[22] Z. Zhang, L. Yang, Q. Pei, J. Ma, Research on usage control model with delegation characteristics based on OM-AM methodology, in: NPC.2007: Proceedings of Network and Parallel Computing Workshops, 2007, pp. 238.243.

[23] P. Gama, P. Ferreira, Obligation policies: An enforcement platform, in: POLICY.05: Proceedings of the Sixth IEEE International Workshop on Policies for Distributed Systems and Networks, IEEE Computer Society, Washington, DC, USA, 2005, pp. 203.212.