Journal of Information Security, 2013, 4, 67-72
http://dx.doi.org/10.4236/jis.2013.42008 Published Online April 2013 (http://www.scirp.org/journal/jis)

The Package Concept for Enforcing Usage Control

Patricia Ghann, Changda Wang, Conghua Zhou
School of Computer Science and Telecommunication Engineering, Jiangsu University, Jiangsu, China
Email: pghann@gmail.com, changda@ujs.edu.cn, chzhou@ujs.edu.cn

Received December 5, 2012; revised January 3, 2013; accepted January 11, 2013

ABSTRACT

Access and usage control is a major challenge in information and computer security in a distributed network connected environment. Many models have been proposed such as traditional access control and UCONABC. Though these models have achieved their objectives in some areas, there are some issues both have not dealt with. The issue of what happens to a resource once it has been accessed rightfully. In view of this, this paper comes out with how to control resource usage by a concept known as the package concept. This concept can be implemented both with internet connection and without the internet connection to ensure continual control of resource. It packages the various types of resources with the required policies and obligations that pertain to the use of these different resources. The package concept of ensuring usage control focuses on resource by classifying them into three: Intellectual, sensitive and non-sensitive resources. Also this concept classifies access or right into three as: access to purchase, access to use temporally online and access to modify. The concept also uses biometric mechanism such as fingerprints for authentication to check redistribution of resource and a logic bomb to help ensure the fulfillment of obligations.

Keywords: Access Control; Usage Control; Policies; Obligation; User or Subject; Biometric Finger Print; Logic Bomb; Remote Client

1. Introduction

Computers and computer systems play a vital role in the lives of the individual. The use of computer systems is seen almost everywhere. For example, insurance companies, healthcare services, banking, education and many more. The advancement in computer and information technology has increased the amount of data collected, whereas the improvement in network infrastructure has resulted in the uncontrolled distribution of information. Although the impact of these technologies cannot be over emphasized, a critical issue in computer security concerns how data and resources can be protected. Access control and usage control are challenging issues that face information security currently. Access control has been given adequate attention by researchers in the past. Usage control on the other hand is a new concept proposed by Park and Sandhu (2000) that seeks to enhance on access control. By controlling who has access to which data, traditional access control mechanisms such as DAC, MAC and RBAC, dealt with just an aspect of the problem. Usage control has been proposed to argument access control by controlling what happens to data after access has been granted. UCON introduces authorization, obligation and condition for decision making as well as continuity of decision and mutability of attributes [1]. However it does not go beyond what happens to a particular resource once it has been "rightfully" accessed using UCON. For an example, imagine a subject is able to purchase an eBook online using UCON implementation system where the right to access is influenced by authorization, obligation and condition. After successfully paying for the eBook, it becomes his property however the subject has no right to redistribution since the subject is not the original owner and hence redistribution would result in loss of profit by the provider. This is also similar to the purchase of movie or music CDs online. That is, what measures should be implemented to ensure that, obligations and policies such as non-redistribution of resources are adhered to. In view of this, the paper explores the idea of obligation and proposes a method of ensuring the fulfillment of obligation on a remote client server which is one of the pressing issues facing information security. The rest of the paper is organized as follows; Sections 2.0 and 2.1 is about traditional access control and prior work respectively, Section 2.2 is about the limitations of traditional access control while Section 2.3 is about usage control. In Section 3 we introduce our method of ensuring the enforcement of obligation on a remote client server. Section 3.1 is about biometric fingerprint authorization, 3.2 is about logic bomb. Sections 4 and the last part are conclusion and references accordingly.

2. 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 terms of 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). 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 [2]. Hence the objective of access controls. There has been much research with progress in access control for the past thirty years with prominence centered on access control matrix. With access matrix, a right is unambiguously 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 presumed 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 often used [3]. A variety of DAC, MAC and RBAC models have emerged to accommodate a diverse range of real-world access control policies. 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 [4]. 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.

2.1. 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 [5]. 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 [6]. 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 [7-9]. 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 [10,11].

2.2. Limitations of Traditional Access Control

Traditional access control models are not adequate for today's distributed, network-connected digital environment [12].

- 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 [13]. 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.

2.3. 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. 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 [1]. The concept of usage control encompasses traditional access control, trust management and digital right management in a single framework. 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. This architecture provides a two-tier usage control over digital resources.

A usage decision in UCON is made by policies of authorizations, obligations, and conditions (also referred as UCONABC core models). In terms of continuity of decision, usage control can be enforced before or during an access process. The distinguishing properties of UCON, beyond traditional access control models are the continuity of access decisions and the mutability of subject and object attributes [14]. In UCON as compared to traditional access control, authorization decisions are not only checked and made before an access, but may be repeatedly checked during the access and may revoke the access if some policies are not satisfied, according to changes of the subject or object attributes, or environmental conditions. The concept of UCON fails to consider what happens to data or information after it has been granted in the absence of internet connection; in other words, the concept of mutability and continuity, only is achieved once a subject is using the internet. In light of this, we propose a means of ensuring the fulfillment of obligations a on a remote client server. We do this by a concept we have termed the "package concept". Much attention and research have focused on the architectural aspect of enforcing obligations without any attention on the information itself. As mentioned previously, Usage control does not answer the question of what happens to resource after it has been rightfully accessed and has now become the subject's property literally. Thus if a subject uses usage controls decision factors, authorization, obligation and conditions with mutability and continuity to rightfully access a music file, movie or a white paper, he can redistribute these resources since he has paid for it. This however would affect the provider or owner of such resource in terms of revenue generation. In the next section we introduce the package concept of enforcing obligation to ensure usage control.

3. The Package Concept of Enforcing Obligation and Ensuring Control of Resource on a Remote Client

We propose a system that would use the various architectural designs that has already been proposed so far to help ensure control of resource. A method that would help enforce obligation in remote client server by focusing on the resource itself. Firstly, we classify objects or digital resources as follows:

- Intellectual resource (INTELL)
- Sensitive resource (SEN)
- Non-sensitive resource (NSEN)

We make this division as most of the resources available on the internet basically fall within this classification. This classification is in line with the coverage of UCON, except that we have captured privacy protection under sensitive resources and other resources that do not belong to intellectual or sensitive resources as non-sensitive resources. This is to ensure that policies and obligations required for the accessibility of resources are formulated appropriately and attached to these resources; thus help a subjects to know what exactly they are going in for and what is required from them.

Based on the above classification, we formulate the appropriate obligations and encapsulated them with each group of resource. Thus instead of stating obligation and policies separately from a resource, obligation and policies covering these groups of objects or resource are stated and attached to each group by the service provider. Secondly, access to a particular resource must be through authorization using a biometric mechanism such as fingerprints. The subjects would have to input three different fingerprints from among ten fingers. This would ensure that resource is not given to an unauthorized person as the requested resource, would have subject's fingerprints embedded into it. Obligations consist of actions and time within which they are supposed to be fulfilled. This is to ensure that when access is granted, to a particular group of resource, the subject cannot give resource to any other person. For example if a subject want to purchase an eBook, movie or music CD, he is suppose to register, if the registration is by finger prints, the service provider accepts the finger prints and encrypt it into these resource before it access to purchase is granted. This is done so that subject cannot redistribute resources.

3.1. Biometric Authorization by Fingerprints

Biometrics is a general term used to describe characteristics or processes. As a characteristic, it is the measurable biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition. As a process it encompasses the automated methods of recognizing an individual based on measurable biological (anatomical and physiological) as well as behavioral characteristics. The above definition basically classifies biometrics into two main types as behavioral and physical biometrics. Behavioral biometrics basically measures the characteristics which are acquired naturally over a time and is mostly used for verification. For instance speaker recognition for analyzing vocal behavior, signature for analyzing signature dynamics and keystroke for measuring the time spacing of two typed words.

Physical biometrics on the other hand, measures the inherent physical characteristics on the individual and as such can be used for either identification or verification. Examples of physical biometric include; fingerprint for analyzing fingertip patterns, facial recognition for measuring facial characteristics, iris scan for analyzing features of colored ring of the eye and many more.

We propose a biometric authorization by fingerprints for analyzing fingertip patterns to help ensure usage control. This is because most sites require attributes of subject such as password and user name for authorization. This however can be stolen or verbally transferred to other people. However a random selection of three fingerprints from among ten fingers is difficult to steal or be verbally transferred to other people. A subject who wants to have access to a particular type of resource would have to provide a random sample of his or her three fingerprints. Once the fingerprints are collected, the type of access and the type of resources are selected by the subject.

Resources or digital information are accessed on online in three main ways. These include the following:

- Access to purchase
- Access to read, listen or watch or download online
- Access to modify or use online

Access to Purchase: This type of access employs UCON pre-authorization by fingerprints as the decision factor. In this type of access, a subject may want to purchase an eBook, music or movie online. These types of resources are classified as intellectual resources. As a result, the main policy may be non-redistribution by subjects. To enforce this policy, the fingerprints of the subject are encrypted into the resource. Thus limiting redistribution by location; in other words, the subject would have to move from place to place in order to redistribute this resource.

Access to Read, Listen or Watch Online: Resources involved in this type of access include intellectual, sensitive and non-sensitive. Intellectual resource may include access to read a book, journal and articles. Sensitive resource can include access to read a bank statement or a medical report. Non-sensitive resource can include intellectual resource such as music, movie or wiki document. With this type of access, UCONABC model is very effective in ensuring usage control. With sensitive information like, bank statement and medical report, fingerprint of identifee subject is required in the form of pre-authorization and this is encrypted into the said resource before access is granted.

Access to Modify or Use: This type of access is mostly required in the health services; for instance, a doctor requiring patient's record for treatment, on the patient's day of appointment. Since the resource involve is sensitive, the doctor is requested for his fingerprint as a pre-authorization. There can also be ongoing check to ensure that the doctor is indeed authorized. Furthermore, since sensitive information is been handled, a logic bomb can be implement in the resource with an obligation that specifies the duration of access to such a record or resource. For example, a logic bomb can be implemented so that, the doctor is allowed a maximum of one hour on a patient, after which the record is temporary destroyed. When this happens, the doctor would be asked for his or her fingerprints again but this time around with a "mark" which would enable management to request for some explanations as well as investigations.

3.2. A Logic Bomb Mechanism

In order to ensure that obligations that are encapsulated with resources are fulfilled, we proposed a logic bomb to help accomplish this task. A logic bomb or slag code is a program, or portion of a program, which lies dormant until a specific piece of program logic is activated. The common activator for a logic bomb is a date. The logic bomb checks the system date and does nothing until a pre-programmed date and time is reached. At that point, the logic bomb activates and executes its code. The logic bomb can also be programmed so as to wait for a certain message from the subject. When the logic bomb sees that message, or when the logic bomb stops seeing that message, it activates and executes its code. The most dangerous form of the logic bomb is a logic bomb that activates when something doesn't happen. We therefore use a logic bomb programmed along these two dimensions; date and message from subject. With date, obligations that need to be fulfilled with certain durations can be implemented. For example delete within 90 days. This is however similar to the classic use for a logic bomb to ensure payment for software. If payment is not made by a certain date, the logic bomb activates and the software automatically deletes itself. With the message, the logic bomb would be programmed to receive fingerprints of user at certain random interval for verification especially in the case of access to purchase or modify. This would ensure that only authorized subjects have access to resource and minimized redistribution of resources. **Figure 1** is an illustration of how a particular resource can be accessed in the package.

How to Access a Particular Resource

1) Input three finger prints
2) Upon acceptance of fingerprints

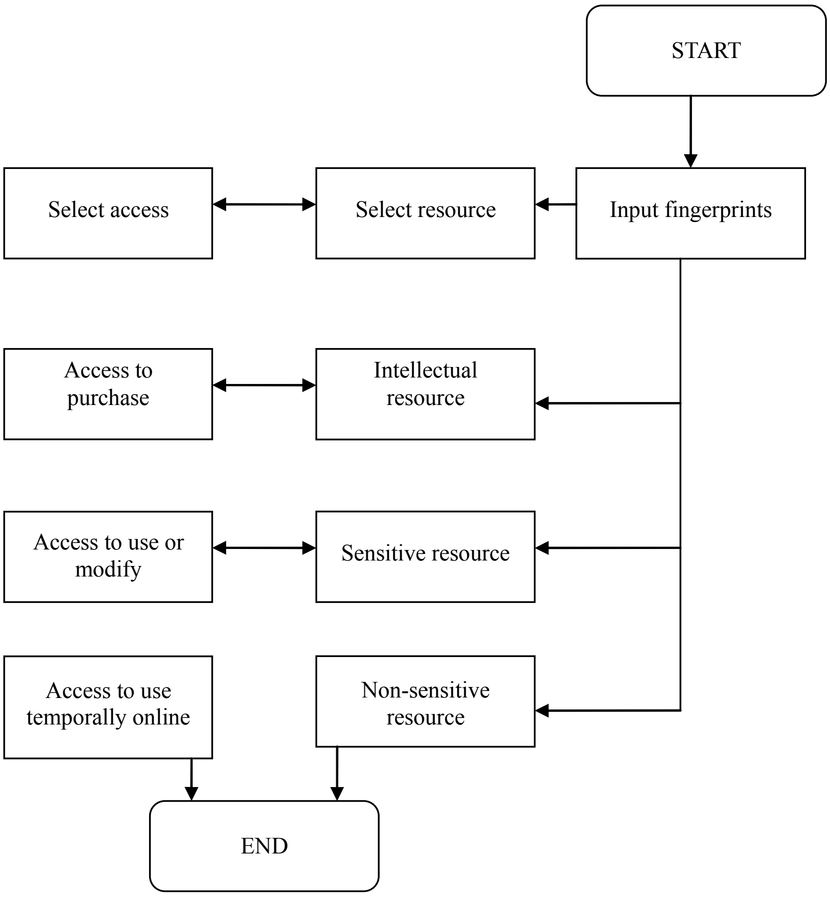

Figure 1. Packaged concept of resources with different access.

3) Select type of resource

- If access is to purchase an intellectual or sensitive resource, fingerprints are encrypted into resource before resource is accessed for purchase.
- If access is to modify, fingerprints are obtained for authorization and encrypted into modified section for accountability.
- If access is to use online, fingerprints is obtained for authorization and access is permitted based on UCONABC.

With usage control, actions are classified into two. Actions performed by a subject and actions performed by the system. These actions are as follows:

1) Tryaccess(s, o, r): generating a new access request (s, o, r), performed by subjects.

2) Permitaccess(s, o, r): granting the access request of (s, o, r), performed by the system.

3) Denyaccess(s, o, r): rejecting the access request of (s, o, r), performed by the system.

4) Revokeaccess(s, o, r): revoking an ongoing access (s, o, r), performed by the system.

5) Endaccess(s, o, r): ending an access(s, o, r), performed by a subjects.

6) Preupdate(attribute): updating a subject or an object attribute before granting access or after denying an access, performed by the system.

7) On update (attribute): updating a subject or an object attribute during the usage phase, performed by the system.

It should be emphasized that onupdate actions may be performed repeatedly by a system in order to continuously update an attribute and s, o, r refers to subject, object and right respectively.

A logical model of UCON consist of a 5-tuple; M = (S, PA, PC, AA, AB) where

S is a set of sequences of system states

PA is a finite set of authorization predicates built from the attributes of subjects and objects

PC is a finite set of usage control predicates built from the system attributes

AA is a finite set of usage control actions

AB is a finite set of obligation actions

A logical Formula is also defined in UCON by the following in BNF grammar:

$$\o ::= a|p(t1, \cdots , tn)|(\neg \o)|(\o \wedge \o)|(\o \rightarrow \o)|\square \o|\lozenge \o|O\o|\o U\o|\blacksquare \o|\blacklozenge \o|O\o|\o S\o|,$$

where a is an action, p is a predicate of arity n, and t1, ...

tn are terms.

If in a state sequence sq of a model M, a state s satisfies a formula ø, we write M, sq, s| = ø. The satisfaction relation |− is defined by induction on the structure of ø and only for s0 ∈ sq. specifically, $M, sq, s0 \mid= p$ if f s0 [[p]], where $p \in PA \cup PC$.

Access to Purchase: an e-book online the following rules are applied

1) Permitacess(s, o, purchase) → ♦tryaccess(s, o, purchase) ∧ (s. fingerprints ≥ 3) ∧ (encrypt.o.intell)

2) Permitaccess(s, o, purchase) → ◊onupdate(s. fingerprints ≥ 3) ∧ ◊(endaccess(s, o, purchase) ∨ revokeaccess(s, o. purchase))

The first policy says permit access once a subject tries access and has input his fingerprints to be encrypted into the resource to be purchased. The second policy says although the subject has purchased the resource, he is expected eventually to provide his fingerprints at some point when accessing. Otherwise access is ended or revoked indicating that he is not the rightful owner of the resource.

Access to Modify: (Doctor-patient relationship) the following rules can be applied

1) Permitacess(s, osen, modify) → ♦tryaccess(s, osen, modify) ∧ (s. fingerprints ≥ 3) ∧ (encrypt. osen)

2) Permitaccess(s, osen, modify) → ◊onupdate(s. fingerprints ≥ 3) ∧ ◊(endaccess(s, osen, modify) ∨ revokeaccess(s, osen, modify))

3) Endaccess(s, osen, modify) → ◊postupdate(records. fingerprints)

4) Revokeaccess(s, osen, modify) → postupdate(records. fingerprints)

Access to Use Temporary: e.g. watch, listen and read the following rules can be applied

1) Permitacess(s, o, watch) → ♦tryaccess(s, o, watch) ∧ (♦ob1 ∧ ♦ob2 ∧ ⋯ ∧ ♦obi)

2) Permitaccess(s, o, watch) → ◊onupdate(s. fingerprints ≥ 3) ∧ ◊(endaccess(s, o, watch) ∨ revokeaccess(s, o. watch))

The first policy regarding this type of access is, permitaccess to watch once there is a tryaccess and the necessary obligations is fulfilled like click and advertisement every 30 minutes. The second policy states that in the event that the resource is downloaded and used off-line, the subject needs to fulfill some obligations. For example delete movie or music within 90 days. To ensure that is obligation is adhere to; we use a logic bomb and program it to explode within the stipulated time. This will limit unauthorized redistribution of resource to some extent and hence protect resources.

4. Conclusion

To ensure that control is still exerted on resources no matter the location, the package concept is proposed to be used with UCONABC to enforce usage control. With the implementation of biometric fingerprints and logic bomb in a particular resource, the unauthorized dissemination or redistribution of resources can be minimized and obligations would be enforced through the package concept.

REFERENCES

[1] A. Lazouski, F. Martinelli and P. Mori, “Usage Control in Computer Security, a Survey,” *Computer Science Review*, Vol. 4, No. 2, 2010, pp. 81-99.

[2] J. Park and R. Sandhu, “A Usage Control (UCON) Model for Social Network Privacy,” 2010.

[3] J. Park, X. Zhang and R. S. Sandhu, “Attribute Mutability in Usage Control,” *Proceedings of IFIP TC*11/*WG, Eighteen Annual Conferences on Data and Application Security*, Kluwer, Vol. 144, 2004, pp.15-29.

[4] J. Wu and S. Shimatoto, “Usage Control Based Security Access Scheme for Wireless Sensor Network,” *Proceedings of IEEE International Conference on Communication* (*ICC* 2010), Cape Town, 23-27 May 2010, pp. 1-5.

[5] M. Sastry, R. Krishnan and R. Sandhu, “A New Modeling Paradigm for Dynamic Authorization in Multi-Domain Systems,” In: *Communications in Computer and Information Science*, Springer, Berlin, 2007, pp. 153-158.

[6] R. Alnemr, *et al*., “Enabling Usage Control Reputation Objects, A Discussion on e-Commerce and Internet of Services Environments,” *Journal of Theoretical and Applied Electronic Commerce Research Electronic Version*, Vol. 5, No. 2, 2010, pp. 59-79.

[7] W. Shin and S. B. Yoo, “Secured Web Services Based on Extended Usage Control,” In: *PAKDD Workshops*, *Lecture Notes in Computer Science*, Springer, Berlin, 2007, pp. 656-663.

[8] B. X. Zhao, *et al*., “Towards a Time—Based Usage Control Model,” W3C Privacy and Data Usage Control Workshop, Cambridge, 2010.

[9] C. Moucha, E. Lovat and A. Pretschner, “A Virtual Usage Control Bus System,” *Journal of Wireless Mobile Networks*, *Ubiquitous Computing and Dependable*, Vol. 2 No. 4, 2010, pp. 84-101.

[10] C. Bettini, S. Jajodia, X. S. Wang and D. Wijesekera, “Obligation Monitoring in Policy Management,” *Proceedings of 3rd IEEE International Workshop for Distributed Systems and Networks Policy*, Monterey, 2002, pp. 2-12.

[11] D. Basin, *et al*., “Monitoring Usage Control Policies in Distributed Systems,” *IEEE*, 2011, pp. 88-95.

[12] D. Basin, *et al*., “MONPOLY: Monitoring Usage Control Policies,” *Lecture Notes in Computer Science*, Vol. 7186, 2012, pp. 360-364. doi:10.1007/978-3-642-29860-8_27

[13] E. Maler, “Controlling Data Usage with User—Managed Access (UMA),” W3C Privacy and Data Usage Control Workshop, Cambridge, 2010.

[14] G. D. Bai, *et al*., “Context-Aware Usage Control for Android,” *6th international ICST Conference on Security and Privacy in Communication*, Singapore, 7-9 September, 2010, pp. 326-343.