A New Modeling Paradigm for Dynamic Authorization in Multi-domain Systems*,**

Manoj Sastry[1], Ram Krishnan[2], and Ravi Sandhu[3]

[1] manoj.r.sastry@intel.com
[2] rkrishna@gmu.edu
[3] sandhu@gmu.edu

Abstract. The emergence of powerful, full-featured *and* small form-factor mobile devices enables rich services to be offered to it's users. As the mobile user interacts with multiple administrative domains, he acquires various attributes. In such dynamic usage scenarios, attributes from one domain are interpreted and used in another domain. This motivates the need for dynamic authorization at the time of interaction. In this paper, we investigate the requirements of multi-domain interactions and explore a new paradigm for modeling these requirements using the UCON model for Usage Control [5]. We propose extensions to UCON in order to accommodate dynamic authorizations requirements.

Keywords: Authorization, Multi-domain, UCON, Attribute-based Access Control.

1 Introduction

The advent of small form-factor, high performance computing devices and high bandwidth ubiquitous networks is enabling users to be connected anytime, anywhere with access to rich services. As users become increasingly mobile, they transcend multiple security domains[1]. Context acquired in one domain can be interpreted and used at other domains for access decisions. Our objective in this paper is to investigate dynamic requirements for multi-domain interactions and explore a new paradigm for modeling these properties. Traditional attribute-based access control models have two major limitations: a. In a single domain setting, attributes are typically pre-defined. b. In a multi-domain setting, such models require extensive a-priori agreement of attribute semantics across these systems. We use the term Dynamic Authorization in this paper to collectively refer to the components required for supporting just-in-time authorization.

2 Characteristics of Multi-domain Interactions

In this section, we identify some of the desirable characteristics for user interactions with multi-domain systems using a concrete example. Alice walks into a

** A detailed version is available at http://www.list.gmu.edu/confrnc/misconf/DA.pdf

[1] For simplicity, we will often abbreviate 'security domain' simply as 'domain'.

V. Gorodetsky, I. Kotenko, and V.A. Skormin (Eds.): MMM-ACNS 2007, CCIS 1, pp. 153–158, 2007.

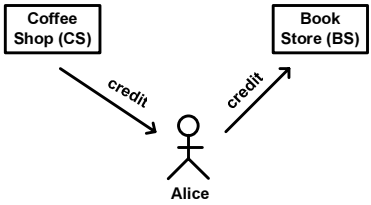

Fig. 1. Coffee Shop Example

Coffee Shop (CS) and engages in a transaction worth $100. As an appreciation, the CS provides a 'credit' worth $10. This 'credit' could be used at various other stores like the Bookstore (BS). Alice later uses this 'credit' towards purchasing a book at the BS. Fig. 1 illustrates this scenario. In this example, 'credit' is the context acquired by Alice from the CS and this affects access decision at the BS. We now identify three key characteristics of multi-domain interactions:

1. Multi-domain interactions: Subjects and Objects interact with multiple systems and this is a key characteristic in mobile commerce. E.g. Alice interacts with the CS and the BS which are administratively different domains.
2. Information could be dynamic and transcend systems: Due to mobility, information or context may move from one system to another and could affect access decisions at other systems. E.g. Alice obtained a 'credit' from the CS system and used it to purchase a book from the BS system.
3. No prior configuration: In order to interpret information across multiple domains, systems may have to exchange semantics of this information. But in mobile scenarios, information may be dynamically created and hence a-priori agreement of semantics is not desirable. It must be interpreted at authorization time. E.g. The CS issued 'credit' to Alice. The following day, CS may issue 'coupon' which may be semantically different from 'credit'. Further, the following characteristics are also desirable:

3 New Modeling Paradigm for Dynamic Authorization

Our new paradigm is to propose modeling requirements for the three key characteristics discussed earlier: 1. Multi-domain interactions, 2. Information could be dynamic and transcend systems, 3. No prior configuration. We believe that these three characteristics are missing from current approaches to dynamic authorization. Characteristics 1 and 2 brings in a notion of "Multi-Domain Attributes" which are attributes that need to be interpreted across multiple domains. Characteristic 3 brings in a notion of "Dynamic Attributes" which are created dynamically and are not pre-defined. In the coffee shop scenario, the 'credit' attribute was dynamically created by the coffee shop just for that day when Alice interacted with the system. Hence the bookstore cannot write authorization policies to use 'credit' ahead of time. The bookstore needs to interpret the semantics of

'credit' just when Alice uses it to buy a book. Here 'credit' is also an attribute that can be used at multiple domains (CS and BS). Thus it is a Dynamic, Multi-domain attribute. Note that Dynamic Attributes are new-born attributes (name-value) as opposed to the notion of *attribute value changing dynamically.*

4 The Extended UCON$_{ABC}$ Model

We now examine the major components of the UCON model: attributes, obligations, conditions and authorizations. [5] discusses the UCON model in great detail. Fig. 2 shows an extended UCON model or EUCON that accommodates multi-domain interactions. In the following subsections, we explore each of the EUCON components in detail to support dynamic authorization.

4.1 EUCON Attributes

In UCON, attributes are properties of subjects and objects which are used for usage decisions. We now investigate and classify EUCON attributes.

We can classify attributes based on time at which an attribute is defined:

Pre-defined Attributes: These are similar to the conventional notion of attributes. The semantics of these attributes are pre-defined by the administrator.

Dynamic Attributes: These are attributes that are defined just-in-time. E.g. The CS system might define new incentives like 'credit' at different times on different days dynamically. For instance, the CS could create a 'coupon' attribute on the following day which has a different meaning than a dollar value like 'credit'.

We can also classify attributes based on scope as follows:

Local Attributes: These are attributes whose semantics can be interpreted only within the domain where it was defined. It has no meaning or visibility anywhere outside the system in which it is defined. E.g. The CS system may have a Local Attribute called 'id' which may have no meaning outside the CS system.

Multi-domain Attributes: Multi-domain Attributes are attributes whose semantics can be interpreted across multiple domains. E.g. The book store was able to interpret the semantics of 'credit' that was issued by CS.

This classification gives us four possible combinations as follows:

Pre-defined Local Attributes (PLA): PLA's are exactly the same as how current attribute-based models (including UCON) define attributes. Traditionally, PLA's have served the purpose of access control in a single system (or domain).

Pre-defined Multi-domain Attributes (PMA): Current approaches to access control in distributed systems have the notion of PMA's. This involves prior agreement of attribute semantics across all the domains *a-priori*. As discussed earlier, this is clearly not flexible and is not suitable for dynamic scenarios.

Dynamic Local Attributes (DLA): DLA's allow systems to dynamically create attributes interpretable within the same system. Typically such an action is

deemed as an administrative task. However, we believe emerging next-generation applications (like context-aware applications) would demand DLA's. In the coffee shop scenario, on a different day CS may create a new 'discount' attribute that could be used by Alice in the coffee shop itself in the future. This 'discount' may not exist all the time. Note that DLA's may or may not be persistent.

Dynamic Multi-domain Attributes (DMA): DMA is fundamentally a new approach to modeling emerging usage scenarios. As discussed earlier, systems may define attributes dynamically that needs to be interpreted at multiple domains. This requires authorization policies to be created dynamically. In the coffee shop scenario, a new attribute called 'credit' was dynamically created at some time and Alice received it. Further, Alice was able to use this attribute at the bookstore. The bookstore dynamically interpreted the semantics of 'credit' by interacting with the coffee shop and authorized purchasing a book with 'credit'. DMA could apply to both subjects and objects. In the coffee shop scenario, it is

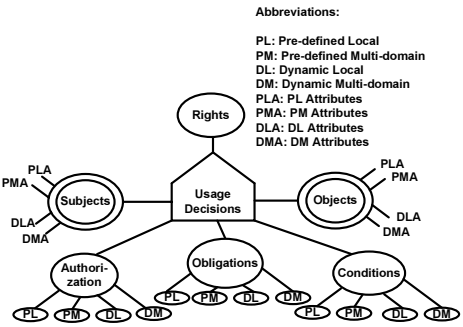

Fig. 2. Extended UCON Components

clear that 'credit' is the DMA of a subject (Alice). Here is another scenario to appreciate the generality of DMA's for subjects:

Airport Security: In airport scenario, a passenger interacts with multiple systems. Further each system (security, shops, airlines, etc.) may define their own attributes dynamically. For example, suppose that the security check-in system in an airport and the airline systems are multi-domain systems with no a-priori configuration. When Alice checks-in through the security system, she obtains a DMA called "cleared=true". This DMA could then be used by Alice at the airline's boarding system to board the airplane.

Following is an example of DMA's for objects:

Airport Security: Following the airport security example discussed for subjects, when Alice checks in at airport security, all the objects that she carries (e.g. luggage, laptop, etc.) could obtain a DMA "cleared=true". Alice can use this DMA at the airline system in order to board the flight with her objects.

4.2 EUCON Authorizations

In UCON, the authorization component contains rules based on subject and object attributes. We discussed that attributes could be classified into four different categories. Because authorization involves constructing rules based on subject and object attributes, we have a similar notion for EUCON authorizations:

Pre-defined Local Authorization: Current UCON's authorization would fall under this category. These rules have served the needs of traditional systems.

Pre-defined Multi-domain Authorization: This involves constructing rules based on Pre-defined Multi-domain Attributes. Current approaches to authorization in multi-domain systems take this approach. Attributes are pre-defined and authorization rules are constructed at multiple domains based on these attributes.

Dynamic Local Authorization: This involves constructing rules based on Dynamic Local Attributes. In the coffee shop scenario, a dynamic local authorization rule could be constructed so that subjects (e.g. Alice) who obtained 'credit' cannot obtain another incentive say 'coupon' at the same time.

Dynamic Multi-domain Authorization: This involves constructing dynamic authorization rules by interpreting Dynamic Multi-domain Attributes. E.g. The bookstore needs to interpret 'credit' dynamically and construct dynamic multi-domain authorization rules. Exactly how such policies are constructed is an enforcement level issue and restrictions should not be made in the policy model.

4.3 EUCON Obligations and Conditions

In UCON, obligations are actions a subject needs to perform before an access can be granted. For example, a subject may be obligated to 'agree' to a license before an object can be accessed. In UCON, conditions are system level factors that need to hold for access to be granted. For example, a server's load should be below a threshold value in order to accept new client connections.

Similar to attributes, in EUCON we can classify both obligations and conditions as: Pre-defined Local, Pre-defined Multi-domain, Dynamic Local, Dynamic Multi-domain. Pre-defined local and dynamic local obligations and conditions are similar to their attribute counter-parts. We discuss the other two below:

Pre-defined Multi-domain Obligations (and conditions): These are pre-defined obligations (and conditions) interpretable across multiple systems. Note that these are obligations (and conditions) on using Multi-domain Attributes.

Dynamic Multi-domain Obligations: These are obligations defined dynamically and are interpreted at multiple systems at authorization time. Again note that these are obligations on using Multi-domain Attributes at different systems. E.g. Suppose that there are two coffee shops: the coffee shop that issued 'credit' – CS and a coffee shop located within the book store – CS@BS. When Alice uses her 'credit' at BS, there could be an obligation that Alice needs to engage in a transaction with the CS@BS before 'credit' could be used at the BS.

Dynamic Multi-domain Conditions: These are conditions on using Multi-domain Attributes at different systems. Following Dynamic Multi-domain Obligations, say that Alice fulfills her obligation. The BS could then dynamically discover a condition on using 'credit' that current 'credit' usage on all coffee shop systems has not exceeded $1000 and the 'credit' expires on 05-25-2007.

5 Related Work

Many related work exists in the arena of dynamic authorization ([2], [1], [4], [6], [3]). We only discuss two of them here. In [1], a Contextual Attribute-Based Access Control model is proposed. The authors define Transaction Attributes (TA) as attributes that a subject obtains as part of a transaction. These TA's would fall under our Pre-defined Multi-domain category. In [2], the authors identify requirements for access control in open environments similar to ours. They survey extensions that have been proposed in general in different access control models. However our modeling paradigm of creating and interpreting attributes dynamically across multiple systems is substantially different.

6 Conclusion and Future Work

In this paper, we explored a new paradigm for modeling dynamic authorizations in multi-domain systems. Current access control models including UCON predefine their components and we demonstrated with compelling usage scenarios that such static definitions would not serve the needs of mobile and dynamic multi-domain interactions. We proposed extensions to the UCON model to express dynamic authorization policies. A formal EUCON model for multi-domain interactions needs to be specified. Enforcement and Implementation models supporting dynamic authorization need to be studied.

References

1. Covington, M., Sastry, M.: A Contextual Attribute-based Access Control Model. In: Meersman, R., Tari, Z., Herrero, P. (eds.) On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops. LNCS, vol. 4278, Springer, Heidelberg (2006)
2. Damiani, E., Vimercati, S., Samarati, P.: New Paradigms for Access Control in Open Environments. In: 5th IEEE Intl. Symposium on Signal Processing and Information, IEEE Computer Society Press, Los Alamitos (2005)
3. Freudenthal, E., Pesin, T., Port, L., Keenan, E., Karamcheti, V.: drbac: Distributed Role-based Access Control for Dynamic Coalition Environments. In: Proceedings of 22nd ICDCS, pp. 411–420 (2002)
4. Lepro, R.: Cardea: Dynamic Access Control in Distributed Systems. SYSTEM 3, 4 (2003)
5. Park, J., Sandhu, R.: The UCON$_{ABC}$ Usage Control Model. TISSEC 7, 57–64 (2004)
6. Hayton, R.J., Bacon, J.M., Moody, K.: Access Control in an Open Distributed Environment. In: IEEE Symposium on Security and Privacy, pp. 3–14. IEEE Computer Society Press, Los Alamitos (1998)