From spatially-aware towards mobility-aware access control
Position Paper

Maria Luisa Damiani, Claudio Silvestri
University of Milan(I)
{damiani, silvestri}@dico.unimi.it

July 31, 2008

Abstract

Spatially-aware access control models regulate the access to protected objects based on the position of subjects at the time of the access request. Following the experience of design of the GEO-RBAC model, in this paper we want to look at spatially-aware access control models with a critical eye and point out the limitations of current proposals. We then present the guidelines of a novel approach which attempts to overcome those limitations and discuss major open issues.

1 Introduction

Spatially-aware access control techniques use position information to regulate the access to protected resources. Although those techniques can be applied in diverse application contexts, we believe that the most intriguing challenges are posed by mobile applications. Increasingly information resources need to be accessed by mobile individuals. For example, a growing number of employees in firms are becoming mobile workers. As workers leave the physical confines of their company's premises, the mobile devices they use expand the boundaries of the enterprise network [4]. This results into an increased security risk for the organization since corporate information can be accessed by malicious parties from any uncontrolled position and then improperly used. On the other hand, mobile applications, such as location-based services (LBS) for both the consumers and enterprise market increasingly demand a controlled and customized access to information services.

Spatially-aware access control in mobile applications presents various challenges. Since the seminal paper of Dorothy Denning & al. [8] who pioneered the vision according to which trusted position information can be used to ensure strong access control, research has developed along diverse directions. Four major research directions can be identified:

- Secure location verification. The problem is how to ensure that the user's position is what is claimed to be. For example, an adversary could transmit

a fake position in place of the real position and thus obtain the access authorization even though the access should not be permitted. Approaches are proposed which however strongly depend on the location sensing technology being used [12].

- Location-based encryption. Another line of research is concerned with the use of position information in key management [3, 2]. For example, Al-Muhtadi et al. [2] propose an approach in which protected computer files are encrypted with a secret key that is accessible only in the region in which the files are to be accessed.
- Location and context-based RBAC. Another line of research concerns the specification of role-based access control models augmented with spatial constraints over the user's position. Accordingly the access authorization is subordinated to the satisfaction of those constraints. Current research mostly focuses on the definition of policy models and location-based access control policy administration [11, 9, 1, 5].
- Location-based digital right management (DRM). DRM allows information owners to control the use and dissemination of electronic files via a license that defines the terms and conditions under which a file can be used. Licenses can contain spatial conditions. For example, Muhlbauer et al. [10] describe the design and implementation of a system for creating and enforcing licenses containing location constraints that can be used to restrict access to sensitive documents to a defined area. Documents can be loaded onto a portable device and used in the approved areas, but cannot be used if the device moves to another area.

In this paper we focus on the central topic of location-based access control models. A significant number of approaches have been proposed in literature in the last few years. To our knowledge, however, only few prototypes are available while the experiences of use of those models are very limited. In this paper we argue that the current location-based access control models present some important limitations, especially with respect to security and scalability, which can represent an obstacle to their effective use and application. We base our claim on the experience of design of the GEO-RBAC model. GEO-RBAC is a comprehensive location-based access control model which extends the RBAC model (Role Based Access Control) with geo-spatial standards. In this paper we want to look at GEO-RBAC, and through it at the class of location-based access control models, with a critical eye. The ultimate goal is to prospect research directions for the next generation of location-based access control models.

The paper is organized as follows: the next section provides background information on GEO-RBAC and discusses some limitations of the model; then in the subsequent section we outline a possible approach to overcome those shortcomings. We conclude with some final remarks about future plans.

2 Background information and critical analysis

2.1 GEO-RBAC

We start recalling some key concepts of the GEO-RBAC model [6]. GEO-RBAC is grounded on a straightforward idea, that is, the operations on sensitive data can only be performed within specified regions (hereinafter, referred to as *zones*) and those zones are related to the role of the user. For example a doctor can be authorized to access patient's records only when inside the ward in which patients are hosted. In practice the access control strategy works as follow: each role is assigned a *role extent* defining the zone in which the role is effective; a role r becomes effective in a session, that is, *enabled*, when the session user, who has been assigned role r, is located in the extent of r; a permission p is granted to a user only if p is assigned to a role which is enabled in the user's session.

We describe in some detail the *position model* adopted in GEO-RBAC, which is a key component of the system. The position model is designed to ensure a certain independence from the location sensing technology being adopted and that is important because position may be acquired at different precision and accuracy, using either a centralized or distributed data acquisition framework. Another major goal of the position model is to permit a simple and intuitive use of the position information, and thus of spatial constraints which otherwise may result complex to handle and understand by users. To address those issues, we represent position at two levels of abstraction called *real position* and *logical position* respectively. The real position is location-sensing technology dependent; the logical position is instead almost independent from the location-sensing technology. The logical position is obtained by mapping the real position onto a spatial object, such as a road or a building using a *location mapping function*. Location mapping functions (lmf) are application-dependent functions, possibly defined by the security administrator and associated with roles. Different roles can be associated with different *lmfs*, depending on the meaning of the role. For example the logical position of a car-driver (where car-driver is a role) can be the linear element representing the road segment along which the user is driving, while the logical position of a generic individual can be the neighborhood in which the individual is located. At run-time, a role is enabled is the logical position is contained in the role extent. Such a condition defines a *spatial constraint* .

In order to provide a clean specification of the various notions of logical position, location mapping function and spatial constraint, the GEO-RBAC model introduces the concept of *role schema* and *role instance*. Basically, the role schema defines the intensional properties of a set of roles instances. Role hierarchies and Separation-of-Duty constraints are then defined with respect to role schemas and role instances.

In the last few years a number of location-based access control models based on RBAC have been proposed in literature which supplement spatial constraints with other kinds of constraints, such as temporal and spatio-temporal constraints [11, 9, 1].

2.2 A critical perspective

While the position model of GEO-RBAC responds to the need of assuring a certain generality and independence of access control from the location sensing technologies, the overall protection mechanism provided by GEO-RBAC presents in some circumstances important limitations. Further, scalability may be difficult to ensure especially when location-based access control is applied in very dynamic organizations. In what follow we discuss those two aspects. It is important to consider that although the focus is on GEO-RBAC, the discussion is of more general concern.

2.2.1 Security issues

The first security issue we consider is related to the policy enforcement mechanism. Following the traditional models, policy enforcement in GEO-RBAC is instantaneous, that is once the access is authorized it cannot be revoked even though the contextual conditions which have led to the granting of the authorization have changed. Therefore, it may happen that an individual after being authorized to access a resource within a certain zone, leaves such a region even though the access has not been completed, thus infringing security norms. For example a doctor authorized to access streaming data in the hospital, can leave the hospital while a video is being downloaded. To maintain the control for the whole duration of the access, the position as well the policy must be continuously enforced. Continuous enforcement is a major characteristic of *usage control* systems. Usage control advances conventional access control in that policy enforcement is a process which evolves in time in response to actions and events. A problem that has not been addressed yet, is how to apply this paradigm in the mobile context. Relevant questions are, for example, how to model the continuous enforcement of position and how to keep track of the status of the system while the user is moving.

Another kind of thread that the present version of GEO-RBAC is not capable to contrast is *shoulder surfing*. Assume that an individual has regularly gained access from inside the correct zone; another individual can enter such a space and observe over the shoulder what the first individual does. This risk, referred to as shoulder surfing, is especially effective in crowded places because it is relatively easy to stand next to someone and look at the sensitive data being used, such as the PIN one enters at an automated teller machine.

A zone may be also entered by an adversary who gains access to information in a fraudolent way, for example using the identity of another individual. Although one can envision a physical access control at the entrance of each zone, this solution is not realistic in large organizations possibly open to public. Moreover zones not necessarily are physically bounded,thus the physical access cannot be easily controlled.

2.2.2 Scalability issues

When the GEO-RBAC model is used in dynamic settings in which the organization of space evolves and new zones are frequently created or suppressed, policies may be difficult to manage. The problem stems from the fact that when a new zone is added, the access control policy must be modified accordingly, in particular, roles are to be associated with that zone and then assigned to users. Similar operations are executed when a zone is suppressed. Note that, for how the model is defined,

the association user-role instance must be specified for each zone (i.e. role extent). That may result unnatural, because in the real world, the association user-role does have depend on space organization. Moreover, replicating the operation of role instance-user assignment for each zone creates redundancy. All that results in a significant administrative burden. It can be observed also that the problem cannot be solved by simply permitting a modular organization of GEO-RBAC policies as proposed in [5].

3 A new vision

The above requirements calls for comprehensive modeling and architectural solutions which go beyond the services offered by current location-based access control systems. In this section we outline a possible approach to overcome those limitations. Salient concepts of the proposal are: *secure zone*, *presence* and *path* constraints, *location-based usage control.*

3.1 The secure zone concept

The implicit assumption in GEO-RBAC is that there are regions inside which one may have special authorizations, i.e. can invoke operations that in other places would not be possible. Because such an assumption is actually the key idea behind location-based access control, it seems reasonable a model centered on the concept of *secure zone*. Indeed a secure zone is not much dissimilar from the notion of role extent in GEO-RBAC. What makes the difference is the shift of concern from the notion of role to that of secure zone. In the new vision, secure zone becomes a first class concept. A secure zone (simply zone) can be defined as a place, not necessarily physically bounded, which *contains* protected resources. We say that a protected resource is *securely contained* in a zone if such a resource can be accessed from within that zone. For example if a document is securely contained in a zone, then an individual located in that zone may be allowed to read it. A resource can be securely contained in multiple zones, even spatially unrelated.

An individual can be inside or outside a given zone. Moreover individuals move across zones. In particular an individual can *enter* into and *exit* from a zone. Zones can be also defined at different levels of granularity. For example the hospital is a large grained zone while the doctor's office is a fine grained one. Even the movement of the user across zones can be described at different granularities. For example, we can describe the path of a user u saying that first u enters the hospital, then u enters the doctor's office inside the hospital. An important property is that the secure containment relation is not propagated from a nested zone to an external zone. Therefore if a document d is securely contained in a zone A, and A is spatially contained in B, then it does NOT follow that d is securely contained in B.

To permit a more effective management and enforcement of policies, each zone is assigned its own *zone policy*. Such a policy includes the following two components: a set of permissions over the protected objects contained in the zone; and a set of *binding rules*, which dynamically assign permission to users located in that zone. Binding rules are triggered when an individual enters the zone and the effect is to assign the user a set of permissions for the time the user is inside the zone based on the conditions specified in the rules. For example a simple binding rule

for zone z can state that only the users who play a role of radiologist are allowed to display the X-ray images securely contained in the lab z. If John enters z and John is a radiologist then John will be assigned the permission to display X-ray images. Thus, whenever John asks for a permission, such a request is matched against the set of permissions assigned to John in that zone.

Each zone policy is thus enforced separately from the others policies in response to the events enter-into/exit-from.

3.2 Advanced spatial constraints

In our scenario, any zone can be entered by any individual, because there is no physical control at the entrance of zones. To mitigate the risk of shoulder surfing and physical intrusion, we propose the use of advanced spatial constraints. In particular, we introduce two classes of constraints called *presence constraints* and *path constraints* respectively. In what follows we discuss the meaning of those constraints and some relevant issues related to their enforcement.

3.2.1 Presence constraints

Whenever a user, say John is in a zone, some other individual (foreigner) in the neighborhood can observe what John does. If that observation can lead to the infringement of the security norms one might consider to forbid or suspend the user's access. Presence constraints are instrumental to controlling the presence of foreigners in a zone. A presence constraint takes the form:

$$c = [z, n, condition]$$

where z is a zone, n is an integer number equal or greater than 0, and $condition$ a possibly empty boolean expression over user attributes. The constraint $[z, n, cond]$ is satisfied is there are at most n neighbors in zone z satisfying condition $cond$. For example $[z, 0, -]$ is satisfied if there are no neighbors in z. An important aspect to consider is that presence constraints are to be evaluated on a continuous basis because the neighbors located in a zone can vary dynamically as result of the entering and exiting of individuals into/from zones. Moreover, as a constraint is no longer satisfied, granted authorizations may be revoked. Issues related to the continuity of control will be discussed in the next section.

3.2.2 Path constraints

The history of the user's movements can be useful to detect the presence of intruders. The path of an intruder likely presents anomalies, for example a zone is visited many times or the permanence time in a zone is high. Therefore if those anomalies are detected, and those anomalies are due to an attack, then the intrusion can be likely blocked. The history of the user's movement consists of the sequence of zones which have been traversed by the user. Given a path p, represented by the sequence $[z_1, t_1][z_2, t_2]...[z_n, t_n]$ where z_i is the zone at the maximum granularity being entered by the user at time t_i for $i \in [1, n]$, a path constraint basically defines a condition over p. Specifically a path constraint takes the form:

$$c = [uset, cond]$$

where $uset$ denotes a set of users the constraint is applied to, and $cond$ is the condition over the path. The constraint c is satisfied by user u if u is in $uset$ and the condition $cond$ applied to the path of u is true. An interesting aspect concerns the enforcement of path constraints. While presence constraints are local to each zone and thus are enforced by the local enforcement mechanism, the users' paths are to be handled at global level. That lead to envisage a hybrid architectural framework, in which distributed and centralized policy enforcement coexist.

3.3 Location-based usage control

The problem is how to ensure a continuous enforcement of the position and of the policy while the user is moving. Continuous enforcement is one of the distinguishing features of usage control models, in that the permissions granted to a subject can expire or be revoked along with the usage of the object upon occurrence of certain events [13]. At operational level, this change in perspective has important consequences: it means that policy enforcement is not performed by an access control function, returning yes/no depending on whether the subject's access request matches the application-dependent policy, but rather by a usage control process which evolves in time in response to actions and events. The specification of a location-based usage control mechanism is still an open issue. In particular the main problem is to replace the position model defined in GEO-RBAC with a movement-model which takes into account the mobility of users in bounded zones. A first study has been recently presented in [7]. In such a work we propose an extension of GEO-RBAC with the notion of *long permission*, that is a permission that have a duration, and an adaptive mechanism for controlling on continuous basis, the constraint of spatial containment.

4 Conclusions

In this paper we have discussed the limits of current location-based access control models and presented possible directions of research for the development of more advanced solutions. From a modeling and architectural point of view, the research theme presents many challenges. Among these, a major challenge is to define a usage control mechanism as operational engine underlying spatial constraints evaluation. On the other hand it is important to consider that the shift of concern from the notion of position to that of movement enables a natural convergence between logical and physical access control which are typically managed separately in an organization. That paves the way to a new and unified approach to access control in the mobile context.

References

[1] S. Aich, S.Sural, and A. K. Majumdar. STARBAC: Spatio temporal Role Based Access Control. In *OTM Conferences (2) 2007: 1567-1582*, 2007.

[2] J. Al-Muhtadi, R. Hill, R. Campbell, and M. D. Mickunas. Context and Location-Aware Encryption for Pervasive Computing Environments. In *Proceedings of the Third IEEE International Workshop on Pervasive Computing and Communication Security*, 2006.

[3] M. J. Atallah, M. Blanton, and K. B. Frikken. Efficient techniques for realizing geo-spatial access control. In *Proc. of the 2nd ACM Symposium on Information, computer and communications security (ASIACCS '97)*, 2007.

[4] T. Berfall. Mobility versus security-getting the balance right. http://www.bcs.org/server.php?show=ConWebDoc.3057, 2006. Last visit: Sept. 2007.

[5] M. L. Damiani, C. Silvestri, and E. Bertino. Hierarchical domains for the decentralized administration of a spatially-aware access control system. In *Proc. of the 3rd International Conference on Availability, Reliability and Security (ARES2008), Barcellona*, 2008.

[6] M.L. Damiani, E. Bertino, B. Catania, and P. Perlasca. GEO-RBAC: A spatially Aware RBAC. *ACM Transactions on Information and System Security (TISSEC)*, 10(1), 2007.

[7] M.L. Damiani, E. Bertino, and C. Silvestri. An approach to supporting continuity of usage in location-based access. In *Proc. of the12th International Workshop on Future Trends of Distributed Computing Systems*.

[8] D.E.Denning and F.P. MacDoran. Location-Based Authentication: Grounding Cyberspace for Better Security. *Computer Fraud and Security, Elsevier Science Ltd.*, February 1996.

[9] M. Kumar and R. Newman. STRBAC - An approach towards spatio-temporal role-based access control. In *Communication, Network, and Information Security*, pages 150–155, 2006.

[10] A. Muhlbauer, R. Safavi-Naini, F.Salim, N.P. Sheppard, and M. Surminen. Location constraints in digital rights management . *Computer Communication*, 31(6):1173–1180, 2008.

[11] I. Ray, M. Kumar, and L. Yu. LRBAC: A Location-Aware Role-Based Access Control Model. In *ICISS*, pages 147–161, 2006.

[12] N. Sastry, U. Shankar, and D. Wagner. Secure Verification of Location Claims. In *Proceedings of the ACM Workshop on Wireless Security (WiSe 2003)*, 2003.

[13] X. Zhang, F. Parisi-Presicce, R. Sandhu, and J. Park. Formal Model and Policy Specification of Usage Control. *ACM Transactions on Information and System Security*, 8:351387, 2005.