Towards movement-aware access control

Position paper

Maria Luisa Damiani
Dipartimento di Informatica e Comunicazione
University of Milan(I)
damiani@dico.unimi.it

Claudio Silvestri
Dipartimento di Informatica e Comunicazione
University of Milan(I)
silvestri@dico.unimi.it

ABSTRACT

The objective of spatially-aware access control models is to regulate the access to protected objects based on position information. In that last years, increasing attention has been paid to spatially-aware access control models for mobile and pervasive applications. Following the experience of design of the GEO-RBAC model, in this paper we want to look at those models with a critical eye and point out open conceptual and architectural challenges. In this paper, we first discuss architectural issues related to the development of a multi-domain access control system based on GEO-RBAC. Then we present the guidelines of a novel and space-centric modeling framework which aims at overcoming the conceptual limitations of the present model and similar solutions.

Categories and Subject Descriptors

H.2.8 [**Database Management**]: Database Applications—*Spatial Databases and GIS*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection; K.4.1 [**Computers and Society**]: Public Policy Issues—*Privacy*

General Terms

Management, Security, Theory, Legal Aspects

Keywords

GIS, Geospatial Data, Security, Privacy

1. INTRODUCTION

Spatially-aware access control techniques use position information to regulate the access of subjects to protected objects. Although those techniques can be used for different purposes, we believe that the most intriguing challenges are raised 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 in 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 markets increasingly demand a controlled and customized access to information services also based on position information.

In a previous work [11] we have classified spatially-aware access control techniques in three main classes referred to as object-driven, subject-driven, and hybrid respectively. A spatially-aware access control is said *object-driven* whenever the goal is the protection of geo-spatial objects independently from the actual position of subjects. We use the term object-driven to emphasize that position is an attribute of objects. A spatially-aware access control is said *subject-driven* whenever the goal is the protection of resources based on the position of mobile subjects. In that case, position is primarily an attribute of subjects. Whenever both the position of objects and subjects is relevant, the access control is said *hybrid* . Following that classification, in this paper we focus on the subject-driven perspective.

1.1 Research context

Access control in mobile applications presents various facets. Since the seminal paper of Dorothy Denning et al. [16], research has been developing along diverse directions. Major directions are briefly presented here below:

- *Secure location verification*. The problem is how to ensure that the user's position is trustworthy. 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. Various approaches have been proposed which, however, depend on the location sensing technology being used [28, 10, 22].
- *Location-based encryption*. Another line of research relates to 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 made available.
- *Location and context-based RBAC*. Research focuses on the specification of policy models which extend role-based access control (RBAC) with spatial and/or spatio-temporal constraints defined over the subject's position. The access is then authorized if those constraints are satisfied. [1, 25, 23, 13, 24].
- *Location-based digital rights management (DRM)*. DRM allows information owners to control the use and dissemination

SPRINGL 2008 Irvine, CA, USA

of electronic files via a license which defines the terms and conditions under which a file can be used. DRM is location-based if the licenses can contain spatial conditions. For example, Muhlbauer et al. [26] describe the design and implementation of a system for creating and enforcing licenses containing location constraints which 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.

1.2 Focus and contribution

In this paper we focus on the topic of location-based access control policies. Basically, a location-based access control policy consists of a set of rules regulating the access on the basis of the spatio-temporal context. Despite of the numerous models which have been developed in the last few years, only few prototypes are available while there are no significant experiences of use of those models.

In this paper we argue that current approaches present limitations which can represent an obstacle to the effective implementation and application of those models. We base our claim on the experience of design of the GEO-RBAC model [13, 6, 14]. GEO-RBAC is a comprehensive location-based access control model which extends RBAC with spatial constraints in compliance with geo-spatial standards. Currently, we are in the process of developing an architectural framework based on the GEO-RBAC model, called *GeoPolicy Server*. In this paper we want to look at the whole experience with a critical eye, and point out the conceptual and architectural issues which are still open. Although the focus is on a specific model, we believe that the experience can be of more general concern. The ultimate goal is to prospect research directions for the next generation of location-based access control systems.

The paper is organized as follows: the next section overviews the salient features of GEO-RBAC. Then we introduce the architecture of the GeoPolicy Server and present major open issues. In the subsequent section we discuss some conceptual limitations of the access control model and outline a novel modeling framework to overcome those shortcomings. The conclusive section reports some final considerations.

2. BACKGROUND: THE GEO-RBAC MODEL

We start recalling the key concepts of the GEO-RBAC model [13]. GEO-RBAC is based 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. We report two examples of authorization rules in two different application contexts: a) in a health organization, a doctor can be authorized to access patients' records only when inside the ward in which the patients are located; b) a location-based service can only be accessed when the service subscriber is inside a certain region.

In practice the access control strategy works as follows: first each role is assigned a role extent defining the zone in which the role is effective; hence 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*; finally a permission *p* is granted to a user only if *p* is assigned to a role which is enabled in the user's session.

Despite its simplicity, the implementation of this strategy raises challenging questions, for example how to deal with the heterogeneity and inaccuracy of location-sensing technologies. The problem is not trivial because position may be acquired at different precision and accuracy, expressed either in terms of coordinates or in symbolic way (e.g. Oxford street) and collected through either a centralized or distributed data acquisition infrastructure (e.g. mobile location server vs GPS) [20]. Even more importantly, the position granularity which is relevant for security purposes may be different from the one provided by the location sensing technology.

2.1 The position model

To address the above issues, the GEO-RBAC framework defines a *position model*. Basically the idea is to represent the position at two levels of abstraction, called real position and logical position respectively. The *real position* is the position actually available whose characteristics depend on the location-sensing technology being adopted. The *logical position* is ideally independent from the location-sensing technology, because it is obtained by mapping the real position onto a spatial object, such as a road or building. Such a mapping is obtained by calling a *location mapping function*. Location mapping functions (*lmf*) are application-dependent transformation functions 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. The ultimate advantage of such a design choice is to decouple the security view of the position information from the technological details.

At run-time, upon a user's request, the policy enforcement mechanism checks, for each user's session role, whether the spatial constraint associated with that role is satisfied, i.e. the logical position is contained in the role extent. If so, the status of a role is set to *enabled*. As the requested permission is assigned to an enabled role, then such permission is granted.

2.2 Role schema and role instance

The second key issue is how to design a clean and consistent RBAC-based access control model embedding the various notions of logical position, location mapping function and spatial constraint. For that purpose, the model introduces two key concepts: *role schema* and *role instance*. Those concepts are rooted in the classical dualism schema/instance which is at the basis of database and ontology modeling. In essence, in GEO-RBAC a *role schema* defines the intensional properties, i.e. attributes, of a set of *roles instances*. The role schema is described by a *name*, say doctor, and by the following attributes: the *role extent type* (e.g. hospital), the *logical position type* (e.g. room) and a *location mapping function* (e.g. lmf) returning an object of logical position type. A simple notation for the previous schema is:

$$Doctor(Hospital, Room, lmf)$$

A role instance is a role which is defined in compliance with schema specification and that can be assigned to users. A simple way to express that the role Doctor is defined over a spatial extent of type hospital and named *BestClinic* is:

$$Doctor(BestClinic)$$

Permissions, thus the right of executing operations on objects, can be assigned to both role schemas and instance. If assigned to role schemas, permissions are inherited by role instances.

From the modeling point of view the notion of schema adds flexibility and modularity. More in general, we believe that the introduction of a generalized concept of role schema can significantly enrich the expressiveness of RBAC-based models. While approaches have been developed to augment the notion of role with attributes, for example through the notion of parameterized role

[18, 19] or role credential [7], it still lacks a rigorous specification of the role schema/instance concept. On the other hand, Finin et al. [17] raise the ontological question on whether a role is a class or an instance. Perhaps, such an ontological dilemma could be more easily addressed if the notion of role schema and instance would be explicitly defined.

3. EXPERIMENTING WITH GEO-RBAC

Several location-based access control models exist in literature, yet, to our knowledge, none of them has been used in real applications. The crucial question is thus how to assess the convenience of those models and, more in general, the effectiveness of the location-based access control paradigm. Following an experimental approach, one way to address the question is to turn the access control model into an operational system and then evaluate the effectiveness of such a system in real contexts, based on some criteria.

Unfortunately turning a location-based access control model into an operational system is not straightforward. Rather the problem presents several challenges, first of all how to represent and enforce policies within a mobility context. Another issue is how to ensure a simplified policy administration. Policy management is complex because it is intertwined with spatial data management which typically requires ad-hoc tools and expertise. For example, a simple tool is to display on map the spatial content of policies. Indeed, the lack of suitable administration platforms may represent a serious impediment to the development and application of policies. A different issue is how to encourage the experimentation of the model possibly on a wide scale. For that purpose, a viable direction is to use a multi-domain access control environment to support management and use of multiple independent policies.

All those requirements call for a comprehensive architectural solution. In this section, we discuss how the above requirements are being addressed for the development of an access control system based on GEO-RBAC. Such a system is called *GeoPolicy Server*. We first present the main features of the GeoPolicy Server, in particular the policy representation strategy and the administration platform, then we discuss some open issues.

3.1 The design of the GeoPolicy Server

Ideally the GEO-RBAC polices can be represented using a policy specification languages, like X-GTRBAC [7], Ponder [15], OWL [17] and the industry standard XACML [27]. The shortcoming of such an approach is that there is no direct correspondence between the key constructs of the model, i.e. role schema and role instance, and the constructs of the language. The result is a loss of semantic expressiveness in the final, enforceable policy.

To preserve the semantic richness of the model, we propose an alternative approach called *Policy Mapper* [6]. The idea is to structure access control in two layers: conceptual and logical. Access control at the *conceptual level* enhances user experience by providing the ability to express spatial constraints more naturally, whereas the logical level enables enforcement by ensuring that we can interpret spatial constraint vocabulary and implement the resulting spatial constraints on the target system. In practice, the conceptual level provides a language for the specification of GEO-RBAC policies which are then mapped onto the policies at logical level. The policies at logical level are those that are enforced at run time. The Policy Mapper approach has been experienced to map the administrative operations defined in GEO-RBAC onto the X-GTRBAC language [8].

3.1.1 The Administration Workbench

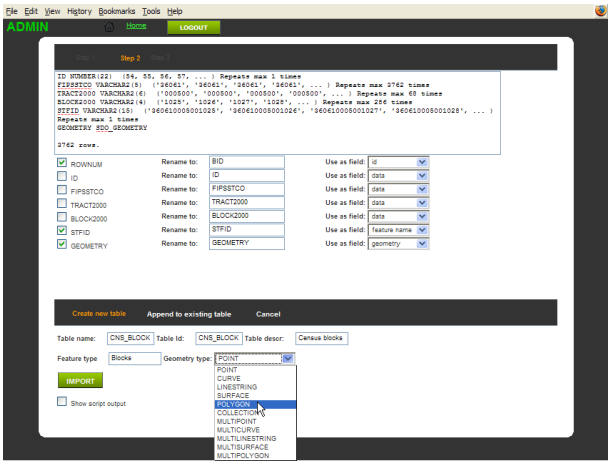

Figure 1: Interface to import spatial data sets into the Workbench

In the framework of the GeoPolicy Server, the *Administration Workbench* (simply Workbench) is the access control component which operates at conceptual level. The Workbench thus supports the specification and management of GEO-RBAC policies. The design of the Workbench results from an empirical analysis of the difficulties that an administrator can encounter during the specification of a GEO-RBAC policy. The Workbench consists of two sub-systems: the *off-line* and the *run-time* sub-system. The off-line sub-system supports policy specification; the run-time subsystem, the policy enforcement in a simulated mobile environment. Note that the objective of policy enforcement at this level is to enable the checking and the tuning of policies before those polices come into operation.

Policies are entered using the administrative operations of GEO-RBAC and then stored in a Policy Repository implemented using a spatial DBMS. The choice of a spatial DBMS has diverse motivations: to naturally integrate spatial objects into policies within a spatially-empowered environment; to leverage the set of functionalities that a spatial DBMS provides to ensure an adequate support for the spatial data management functionalities that may be needed during policy specification, such as data acquisition, coordinate conversion, spatial querying; to efficiently store and process large amounts of spatial data that may be needed for the specification of policies in a multi-domain environment. The run-time subsystem includes various tools which are useful to control how policies are enforced such as the *Location Server simulator*, providing position data about hypothetic users and the *Policy Decision Point* equipped with map-display capabilities.

3.1.2 Multi-domain policy administration

GEO-RBAC Admin [14] is the multi-domain administration model which has been specified to allow diverse organizations manage their own policy in an independent and simplified manner. The model is centered on the concept of *spatial domain*. Indeed, in RBAC there is no consensus on what a domain is. Even less investigated is the notion of domain in the various context-aware extensions of RBAC. In our administration model, a domain is a first class element: besides a name, a domain has attributes. One attribute is mandatory, namely the reference space of the domain. Every policy is thus defined over a distinct spatial domain which establishes *the spatial extent of the policy*, say a city or a state. Each domain is then assigned at least one domain administrator. More-

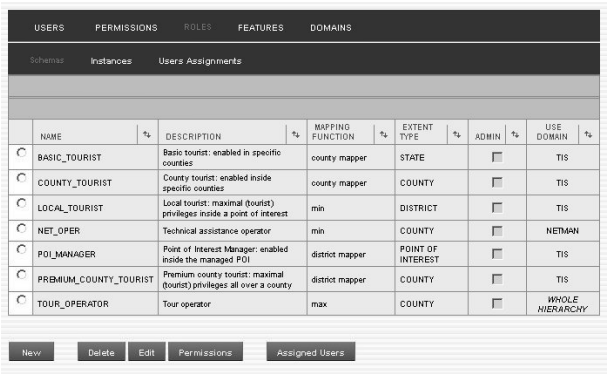

Figure 2: Interface for role schema administration

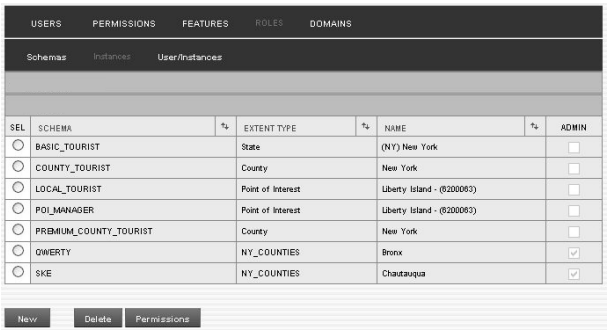

Figure 3: Interface for role instance administration

over, domains can be organized in a spatially-aware hierarchy.

Commonly, policy administration relies on the implicit assumption that domain administrators have a common set of abilities and that those abilities are sufficient to carry out the administration task. Unfortunately, whenever the policy relies on a complex model possibly requiring the integration of external data, such as contextual information, that assumption may be unrealistic. For example, the administration of GEO-RBAC policies is objectively complex. For instance, the specification of a role schema entails various operations including the definition of spatial objects and the programming of *lmfs* (i.e. location mapping functions). Those operations require programming and data management capabilities that go beyond the classical security expertise. For example, Figure 1 shows the Web interface for the *Import* operation which transfers external spatial data sets in a public format into the Workbench. Even though the *Import wizard* automatizes most of the operation, data management expertise is needed to fully understand the side effects of the operation.

To reduce the administrative burden, *GEO-RBAC admin* introduces a delegation mechanism to differentiate the administrative competences. Further it enables the sharing of administrative objects, like spatial objects and *lmfs*, among multiple administrators. In such a way, complex resources such *lmfs* can be managed, for example, only by system administrators and then made available to the domain administrators downward in the domain hierarchy. An advantage of such an approach is that it can be used for the development of role ontologies in a distributed setting.

3.1.3 Interacting with the system

We now briefly illustrate how a domain administrator interacts with the GEO-RBAC Workbench through the Web interface of the

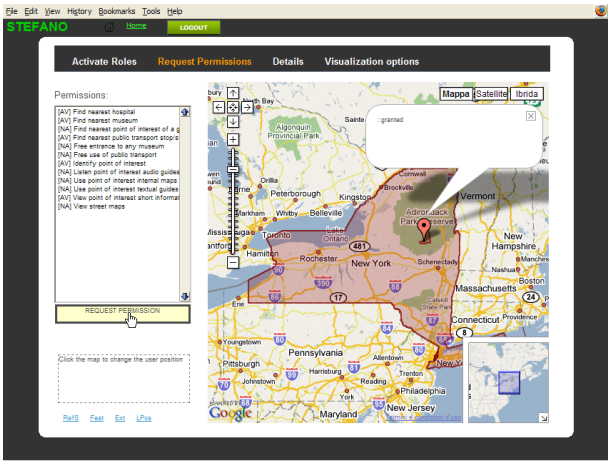

Figure 4: Enforcement of an access request

system. The user is identified by the pair *(login name; domain name)*. If the user has been assigned the role of administrator, then the user is allowed the execute administrative operations. Once connected, the administrator of that domain can select, from a list of spatial objects types, those that are needed for role specification. Thus the administrator can create for example role schemas by selecting from the available library the spatial objects and the functions of interest; hence permissions can be assigned to role schemas. Figures 2 and 3 show the Web interface for the administration of a role schema and a role instance respectively .

The administrator can then use the Workbench Run Time component to display on a map the result of the policy enforcement. Figure 4 shows the logical position of the user (small polygon) inside the extent of the enabled role (large dark area) as well as the access control decision. The spatial objects of the example are taken from the TIGER data set [9], while the maps are visualized using Google Maps API.

3.2 Open architectural issues

Usability. From the previous discussion it is apparent the concern for the aspects of usability in location-based policy administration. Such a concern is motivated by the consideration that access control in mobile applications present complexities which may hinder the effective utilization of those techniques in major applications such as LBS. While some steps have been made towards access control usability in RBAC [5], and also, as we have seen, in the GeoPolicy Server, the problem needs further investigation.

Efficiency. Typically, the efficiency with which policy enforcement is carried out is an issue which is not much addressed in literature. Nonetheless, from the experiments carried out in the Administration Workbench, in particular using the query processor of Oracle Spatial, it turns out that performance is critically affected by the efficiency with which spatial constraints are evaluated. Methods are definitely needed to bound the computational cost.

Compliance with standards. It is important to balance the application-oriented view with policy language standards. As part of future plans, the GeoPolicy Server is expected to evolve in the direction of a distributed access control framework in which GEO-RBAC policies specified at conceptual level are mapped onto XACML policies. We refer to the target architecture as *GeoPolicy Framework*. A possible architecture for the GeoPolicy Framework is illustrated in Figure 5. The system consists of the Administration Workbench for policy specification; and the Run Time Enforce-

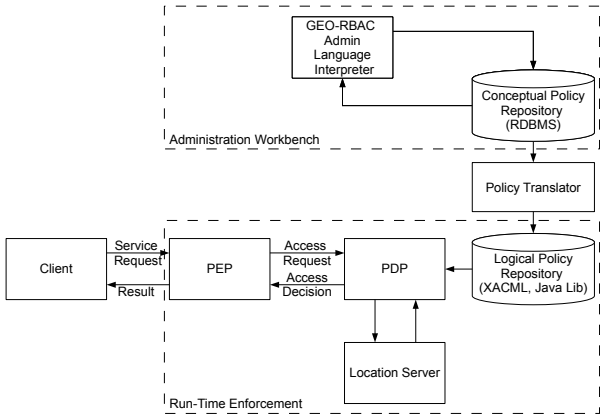

Figure 5: Reference architecture

ment (RTE). Polices specified at conceptual level are mapped onto XACML policies stored in Policy Repositories. The RTE comprises multiple Policy Enforcement Points (PEP) and Policy Decision Points (PDP). Following the standard architecture, a PDP receives an XACML request from the PEP, fetches the applicable policy(s) from a Policy Repository and evaluates the request not only against the applicable access control policies but also the user's position obtained form the Location Server. XACML extensions implemented as Java classes (e.g.: spatial containment operators) are stored in the Policy Repository.

4. BEYOND GEO-RBAC

Now we want to make a step ahead and look beyond GEO-RBAC. We start from the analysis of the conceptual weaknesses of the model. Then we outline a novel and space-centric conceptual framework for access control in mobile applications.

4.1 Critical analysis of GEO-RBAC

4.1.1 Limitations of the enforcement mechanism

Following the traditional access control 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 are changed. Therefore, it may happen that an individual, after being authorized to access a resource within a certain region, leaves such a region even though the access has not been completed, thus infringing security norms. An example is useful to clarify the problem. Assume that our access control is applied to control the access to LBS, in particular to services based on the *push* model. Under the push model, information is provided to the LBS subscribers on a continuous basis. For example, a service of push type is to notify traffic jams to car-drivers. Assume that the service can be only accessed while the car-driver is inside a city. As the user moves, it may happen that the user is no longer in a position which authorizes him/her to access the service. In order to maintain the control for the whole duration of the access, the position as well the policy must thus be continuously enforced.

4.1.2 Physical presence

Location-access control does not prevent an individual from entering the region in which the information access can be granted. Depending on the application context, that may lead to security breaches. For example, consider the case in which a doctor is allowed to view X-Ray images only inside the lab. Assume that an individual, say $Alice$, has regularly gained access to the X-ray images from inside the correct region; another individual, say Bob, can enter the room, and look at the images requested by $Alice$ although he does not have any authorization. To prevent such a risk, one could envision some form of physical access control, for example based on biometrics, at the entrance of each zone. Such a solution is not realistic in large organizations, possibly open to public. Alternative forms of control over the physical presence of individuals are needed.

4.1.3 Are roles enough?

GEO-RBAC relies on the notion of spatial role. Spatial role is an abstract concept which enables a simple representation of spatial constraints. Yet, whenever GEO-RBAC is used in a dynamic environment in which space organization evolves and new zones are frequently created or suppressed, the notion of spatial role presents important limitations. In particular spatial roles are not flexible enough, because as space evolves, spatial roles are to be modified accordingly; similarly the user-role assignment relation must be updated. The result is that the policy is complex to manage. On the other hand, location-based access control can be ideally embedded into paradigms other than RBAC. A more general formulation of location-based access control would thus be desirable to improve the flexibility and applicability of those models.

4.2 A new vision

The above requirements call 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 the conceptual limitations of GEO-RBAC, while maintaining the focus on mobile applications. Differently from Kulkarni at al. [24] we do not propose a context-based RBAC framework which substantially modifies the nature of RBAC itself. Rather we envisage a novel modeling framework which is *space-centric* instead of being role-centric. The key concept in the new vision is that of *security zone* (*s-zone* in brief). The *s-zone* concept captures the intuition that there are regions inside which one can execute operations that in other places would be forbidden.

4.2.1 Security zones

Indeed a s-zone is not dissimilar from the notion of role extent in GEO-RBAC. The key difference is the shift of concern from the notion of role to that of s-zone. In the new vision, a s-zone becomes a first order concept. The position of an individual is the s-zone in which that individual is located. Moreover, individuals can move across s-zones. S-zones are hierarchically organized, i.e. a s-zone can recursively contain smaller zones. The root of the hierarchy is the application space, say the clinic; the leaves are the smaller regions in which a user can be located. For example a clinic may consist of one or more labs, offices and patients rooms. Depending on the security requirements, a distinct s-zone may be defined for example for each lab and also for the set of labs as a whole (similarly for offices and patients' rooms). The position of an individual in the application space can thus be described at varying resolution.

4.2.2 Objects in s-zones

An *object* is an information resource to protect, for example the patients' records in the early example. The idea is to ensure a stronger protection by keeping objects in "safe places" The "safe place" is the metaphoric translation of the concept of s-zone. We

say that an object o is assigned a s-zone z if o can be accessed from within z. Between objects and s-zones there is a many-to-many relationship, thus an object can be assigned to multiple zones and vice-versa.

We observe that an object assigned to a nested s-zone is not automatically assigned to the outer s-zones. For example, if an object o is assigned to s-zone A, and A is spatially contained in B, then it does NOT follow that o can be accessed from B. The vice-versa holds, i.e. objects assigned to a region can be also accessed from inside inner regions.

4.2.3 Local policy

To ensure a flexible policy management in a spatially evolving context, the policy is distributed across s-zones. Each s-zone is assigned a *local policy*. The local policy regulates the access to the objects being assigned to the s-zone.

A key issue is how to ensure an efficient enforcement of the policy. Classically, the policy is enforced whenever an individual issues an access request. Such an approach, if applied to our context, has a major shortcoming in that it requires the computation of the user's position at each request. Since that operation may be costly and also redundant if the user does not move frequently across s-zones, we propose a different approach. The idea is to dynamically bind permissions to individuals, through *binding rules*.

Binding rules are triggered when an individual enters a s-zone, and the effect is to assign the user a set of permissions for the time the user is inside the s-zone based on the conditions specified in the rules. Afterwards, whenever an individual in a s-zone asks for a permission, the request is matched against the set of permissions assigned to that individual in such a zone. Each zone policy is thus enforced separately from the other policies in response to events like the user's entering event.

4.2.4 Advanced spatial constraints

In our scenario, any s-zone can be entered by any individual, because there is no physical control at the entrance of zones. Depending on the applications, it may be important to mitigate the risk of unauthorized observation. For that purpose, we propose the use of advanced spatial constraints. Those constraints specify contextual conditions which must be satisfied for a permission to be granted. 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.

Presence constraints. Presence constraints are to control the presence of foreigners in a s-zone. For example, consider again the case of a health organization: a presence constraint can state that the authorization of displaying X-ray images is granted only if there is no individuals in the s-zone other than doctors. An important aspect to consider is that presence constraints are to be evaluated on a continuous basis, because the individuals located in a zone can vary dynamically. Moreover, as the constraints are no longer satisfied, the granted authorizations may be revoked.

Path constraints The history of the user's movements can be useful to detect the presence of intruders. The path of an intruder is likely to present anomalies, for example a zone is visited too many times. Therefore if those anomalies are detected, and those anomalies are due to an attack, then the intrusion can likely be blocked. The history of the user's movements consists of the sequence of s-zones which have been traversed by the user. The enforcement of paths constraints presents several issues. For example, who maintains the history of users' movement? And also: are path constraints defined globally, and thus valid everywhere, or are those constraints specific of certain s-zones?

4.2.5 Location-based usage control

The problem is how to ensure a continuous enforcement of the position and policy while the user is moving.

There are two aspects which seem particularly complex: the first is to devise a mechanism for the efficient continuous evaluation of spatial constraints. For example: are continuous spatial queries different from continuous spatial constraints? Although some work on continuous constraints is reported in literature [29], the problem still presents several challenges. The second issue is related to the model specification, i.e. how to embed such a notion of continuous control into a language. A few proposals of usage control languages based on temporal logic exist in literature [21, 30], yet those formalisms are too complex for a real use in applications.

A first approach to deal with the continuous enforcement problem in the GEO-RBAC framework is presented in [12]. Specifically, we propose an extension of GEO-RBAC with the notion of *long permission*, that is a permission which has a duration, and an adaptive mechanism for controlling on a continuous basis, spatial constraints. In this new and space-centric vision we are discussing about, however, the issue is apparently more complex.

5. CONCLUSIONS

Location-based access control is a relatively recent paradigm for the protection of resources in mobile applications. From the modeling and architectural viewpoint, there are several challenges that need to be addressed for the access control paradigm to be effectively applicable in real contexts. Among these, we emphasize the need of advanced security metaphors taylored on the mobile context as well of architectural frameworks supporting simplified management of location-based policies and efficient policy enforcement. An important issue is how to safeguard *location privacy* while ensuring a secure access. The problem stems from the fact that the Policy Decision Point is aware of user's position and thus can disclose such information to third parties without user's consent. As a final consideration, we observe that the shift of concern from the notion of position to that of movement enables a natural convergence between logical and physical access controls, which are typically managed separately in an organization. That paves the way to a new and unified approach to access control in the mobile setting.

6. REFERENCES

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

[2] J. Al-Muhtadi, R. Hill, R. Campbell, and M. D. Mickunas. Context and Location-Aware Encryption for Pervasive Computing Environments. In *Proc. 3rd 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. 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] E. Bertino, S. Calo, H. Chen, N. Li, T. Li, J. Lobo, I. Molloy, and Q. Wang. Some Usability Considerations in Access Control Systems. In *Proc. Symposium On Usable Privacy and Security (SOUPS)*, 2008.

[6] R. Bhatti, M. Damiani, D. Bettis, and E. Bertino. Policy Mapper: A Simplified Approach for Administration of Location-based Access Control Policies. *IEEE internet Computing*, 12(2), 2008.

[7] R. Bhatti, A. Ghafoor, E. Bertino, and J. Joshi. X-GTRBAC: an XML-based policy specification framework and architecture for enterprise-wide access control. *ACM Transactions on Information and System Security (TISSEC)*, 8(2):187–227, May 2005.

[8] R. Bhatti, J. B. D. Joshi, E. Bertino, and A. Ghafoor. X-GTRBAC Admin: A Decentralized AdministrationModel for Enterprise-Wide Access Control. *ACM Transactions on Information and System Security*, 4, 2005.

[9] U. C. Bureau. http://www.census.gov/geo/www/tiger/.

[10] Y. Cho and L. Bao. Secure access control for location-based applications in wlan systems. In *Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on*, pages 852–857, 2006.

[11] M. Damiani and E. Bertino. Access Control Systems for Geo-spatial Data and Applications. In E. Ferrari, A. Belussi, B. Catania, and E.Clementini, editors, *Spatial Data on the Web: Modeling and Management*. Springer, 2007.

[12] M. Damiani, E. Bertino, and C. Silvestri. An approach to supporting continuity of usage in location-based access control. In *Proc. 12th IEEE International Workshop on Future Trends of Distributed Computing Systems, October 2008*, Oct. 2008.

[13] M. L. Damiani, E. Bertino, B. Catania, and P. Perlasca. GEO-RBAC: a spatially aware RBAC. *ACM Transactions on Information and System Security*, 1(1):Art. 1, 2007.

[14] M. L. Damiani, E. Bertino, and C. Silvestri. Spatial Domains for the Administration of Location-based Access Control Policies. *Journal of Network and Systems Management*, DOI 10.1007/s10922-008-9106-0, September 2008 (online).

[15] N. Damianou, N. Dulay, E. Lupu, and M. Sloman. The Ponder Policy Specification Language. In *Proc. Policy 2001: Workshop on Policies for Distributed Systems and Networks*, 2001.

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

[17] T. W. Finin, A. Joshi, L. Kagal, J. Niu, R. S. Sandhu, W. H. Winsborough, and B. M. Thuraisingham. ROWLBAC: representing role based access control in OWL. In *Proc. SACMAT*, 2008.

[18] M. Ge and S. L. Osborn. A Design for Parameterized Roles. In F. C. and S. P., editors, *Research Directions in Data and Applications Security XVIII, IFIP TC11/WG 11.3 Eighteenth Annual Conference on Data and Applications Security*, 2004.

[19] L. Giuri and P. Iglio. Role Templates for Content-Based Access Control. In *ACM Workshop on Role Based Access Control*, 1997.

[20] J. Hightower and G. Boriello. Location Systems for Ubiquitous Computing. *Computer*, 34(8), 2001.

[21] M. Hilty, A. Pretschner, D. A. Basin, C. Schaefer, and T. Walter. A policy language for distributed usage control. In *ESORICS*, pages 531–546, 2007.

[22] J. Hwang, T. He, and Y. Kim. Secure localization with phantom node detection. *Ad Hoc Netw.*, 6(7):1031–1050, 2008.

[23] J. Joshi, E. Bertino, U. Latif, and A. Ghafoor. A Generalized Temporal Role-Based Access Control Model. *IEEE Transactions on Knowledge and Data Engineering*, 17(1):4–23, January 2005.

[24] D. Kulkarni and A. Tripathi. Context-aware role-based access control in pervasive computing systems. In *SACMAT '08: Proceedings of the 13th ACM symposium on Access control models and technologies*, pages 113–122, New York, NY, USA, 2008. ACM.

[25] 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.

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

[27] OASIS. eXtensible Access Control Markup Language (XACML). www.oasis-open.org/committees/xacml/.

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

[29] Z. Xu and H.-A. Jacobsen. Adaptive location constraint processing. In *SIGMOD Conference*, 2007.

[30] 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(4):351–387, 2005.