# Spatially-Aware Access Control Model: A Step towards Secure and Energy-Efficient Mobile Applications

Vladimir Oleshchuk

*Department of Information and Communication Technology, University of Agder, Postboks 509, N-4898 Grimstad, Norway; e-mail: vladimir.oleshchuk@uia.no*

**Abstract**

Role Based Access Control (RBAC) Model has been found to be quite useful and has drawn a lot of research interest over the last fifteen years. It was recently defined as NIST/ANSI Standard. Traditional RBAC considers user to role as well as role to permission assignments to be static in nature with respect to space and time. However it was observed that in the context of mobile applications, spatial context plays an increasingly important role both in defining and enforcing more elaborated security policies since in many applications locations of participants should directly influence access control decisions. Recent years many extensions of RBAC to deal with spatial context have being proposed. However another benefit of location awareness (not considered yet in existing extensions of RBAC) is an ability to provide more energy-efficient (more "green") solutions. In this paper we consider extensions of RBAC and propose to use location both as a security and an energy-related parameter. We discuss some applications and directions of future research.

**Keywords:** location-based access control, RBAC, mobile security, authorization model.

*Journal of Green Engineering,* Vol. 2, 125–138.

## 1 Introduction

Mobility of users and resources introduced by wireless connectivity creates new challenges to design secure systems, particularly in handling access to mobile resources and services by mobile users. However, energy is another important key performance metric for mobile systems. Since security solutions may require extensive computations they will as a rule increase energy consumption. In fact there are attacks on mobile systems that are aimed to deplete batteries of individual devices. Therefore for such systems, security and energy-efficiency should be considered together and new models that capture both security and energy concerns are need to be developed [9,13,17].

Generally, in mobile setting we assume mobility of both users and resources. It means that users may change their locations while requesting access to resources and resources themselves may change their locations. Different locations may have different levels of trustworthiness or they may belong to different administrative domains. Therefore resources and services available for users may differ in different locations depending on security policy requirements. For many organizations it is naturally to constrain access to resources to particular locations, e.g. they may demand that a medical student is not allowed to read a patient's medical record unless there is a physician presents at the same location. Furthermore, due to the sensitive information contained in the patient's medical records, a medical student is only authorized to access them from designated areas within the hospital building. Thus, if the medical student requests to read the patient's medical record from other locations than those that are specified in security policy (for example, from the outside of designated area), such as a hospital cafeteria or reception, the access request will be denied (even though the physician is present). The traditional access control models aimed to control user's access within fixed networked systems may not be sufficiently flexible to cope with the dynamics introduced by mobility.

Over the years, Role-Based Access Control (RBAC) [5,6] has established itself as a generalized approach for handling access control in computer systems and differs from traditional identity based access control models in that it takes advantage of the concept of role relations. For these models, access to data and resources are based on the organizational activities and responsibilities, or roles, which users possess in a system. In RBAC, a user's ability to access computer resources are determined by the user's association with roles, and by these roles' permissions to perform operations on objects.

The paper is organized as follows. In Section 2 we give brief review of related work. We introduce generalized SRBAC model in Section 3. Section 4 presents the formalism used to specify spatial domains and spatial conditions. In Section 5 we demonstration how GSRBAC model can be applied to define emergency aware role-based access control, and lastly, Section 6 summarize the paper.

## 2 Related Work

Recent years many solutions were proposed to extend RBAC to deal with mobility.

In [10, 11], the authors extend the RBAC model by specifying spatial restrictions on permissions assigned to roles which enables a role to have permissions assigned to it dependent on the location. Spatial constraints on permissions assigned to a role can be beneficial when specifying the access control policy in mobile environments where the location (or spatial dimension) in which a user access services from is a key security parameter [12]. The authors have extended the RBAC model, and introduced a formal model that allows specifying spatial constraints on permissions associated with roles in different location.

In [4] the authors propose a spatially-aware RBAC model called GEO-RBAC. In the proposed approach authors authors propose the notion of spatial roles which are defined as roles with spatial extents defining the boundaries of the space in which the role can be assumed by the users. In this approach roles are activated based on the position of the user.

Another location aware RBAC model has been proposed in [15]. Authors show how the different components of the core RBAC model are related to location, how existing operations need to be changed and what new operations are needed. They left elaboration of role hierarchies and separation of duty constraints for future work.

Several authors have proposed models that combine both spatial and temporal aspects [1, 3].

All these approaches (except [15]) were proposed after Hansen and Oleshchuk [10, 11] put spatial constraints only on users' ability of activating roles. In [15] the authors assume mobility of users and objects and consider spatial inclusion conditions both for users and objects. However the described approach does not deal with proximity conditions that may be satisfied only in proximity to some (possibly mobile) subjects or objects. All this approaches assign locations to the roles to specify where these roles can be activated.

In our approach, locations are assigned to permissions associated with roles such that set of permissions available within the same role in different locations may be different (even empty). It generally will reduce number of roles needed to be specified.

Some proposed approaches [1, 3] combine both spatial and temporal dimensions. However in this work we focus only on spatial side since this is a distinct property of mobile systems while temporal dimension is essential for all assess control models.

## 3 Generalized SRBAC

In this paper we consider a Generalized SRBAC (GSRBAC) model that is an extension of SRBAC model introduced in [10,11]. Since the time of introduction of SRBAC, various spatial-aware models were proposed (see Section 2). However some important features dictated by current and future real-world applications such as, for example, handling access request in proximity of specific devices or users that are themselves are mobile are still missing. This is the motivation behind the proposed extension of SRBAC abbreviated as GSRBAC. GSRBAC differs from SRBAC in the following two aspects: it allows the specification of spatial constraints on location of resources/services where users may access them, and it allows the expression of requirements to the user to be in proximity of some specific subjects or objects in time of request to get access granted (be together with other users playing a specific role or be close to specific equipment, car, etc.). The second case cannot be specified in the security policy by mapping into physical locations (it can be satisfied anywhere as far as proximity property is satisfied). The example of such scenario may be in the case of emergency as it is described later in the paper (Section 5).

The proposed GSRBAC model consists of the following five basic components: $USERS$, $ROLES$, $PRMS$, $SESSIONS$ and $LOC$ representing the sets of users, roles, permissions, sessions and locations respectively where location set LOC contains both users' locations denoted as $ULOCS$ and services' locations denoted as $RLOCS$. Users from $USERS$ are considered to be mobile units that can access mobile resources (services) to request some operations. $ROLES$ describes a set of roles defined as a set of permissions that may be guarded by spatial constraints to control accessibility of mobile resources (objects). Availability of spatial permissions to the user assigned to the role will depend on locations of both the user and the resource in the time of request. $PRMS$ is a set of permissions to access resources/services to

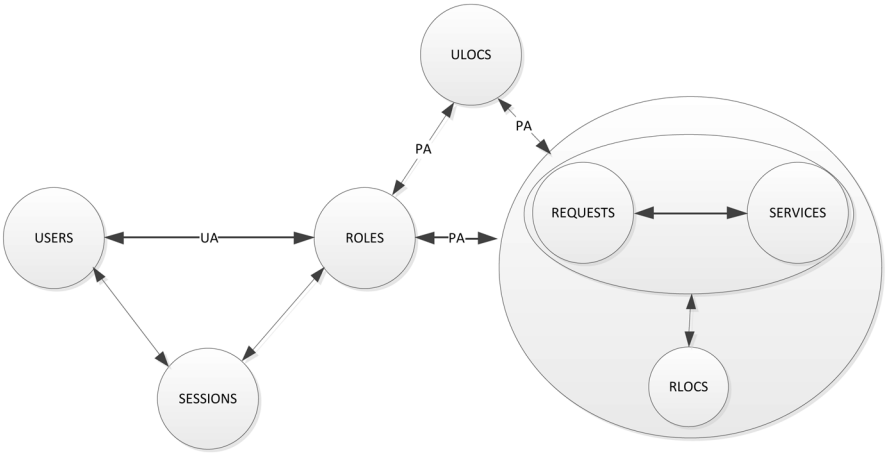


Figure 1 The core GSRBAC model.

perform a specific operation if location of resource or service satisfies spatial requirement. Locations in $LOCS$ are specified by means of symbolic expressions called location expressions that describe location domains identifiable and verifiable by the system implementing GSRBAC (more details in Section 4). The requirement to be identifiable and verifiable by the system means that the system can identify and verify by technological means the claimed location of the user or resource in the time of request. It is a necessary condition since otherwise spatial constrains defined in security policies cannot be enforced.

The GSRBAC model discussed in this paper that deals with mentioned above features is shown in Figure 1.

The model defines several functions and relations on the sets $USERS$, $ROLES$, $PRMS$, $SESSIONS$, $LOCS = ULOCS \cup RLOCS$ needed for specification and implementation of GSRBAC. The user assignment relation $UA$ represents the assignment of a user from $USERS$ to roles from $ROLES$. The permission assignment relation $PA$ represents the assignment of permissions to roles based on location of both users and services.

Definition 1 gives formal descriptions of some important functions and relations.

**Definition 1 (GSRBAC).** *The GSRBAC model consists of the following components:*

- *USERS, ROLES, PRMS, SESSIONS, ULOCS and RLOCS, represent the finite set of users, roles, permissions, sessions, user locations and service/resource locations respectively.*
- $PRMS = REQUESTS \times SERVICES$ *where REQUESTS denotes all requests users can send to services denoted as SERVICES.*
- $LOCS = ULOCS \cup RLOCS$*, where ULOCS represents users locations and RLOCS represents resource locations.*
- $UA \subseteq USERS \times ROLES$*, the relation that associates users with roles.*
- $assigned\_users(r : ROLES) \rightarrow 2^{USERS}$*, the mapping of a role onto a set of users. Formally, users assigned to role r can be found as* $assigned\_users(r) = \{u \in USERS | (u, r) \in UA\}$.
- $assigned\_roles(u : USERS) \rightarrow 2^{ROLES}$*, the mapping of a user onto a set of roles. Formally, roles assigned to a user u can be found as* $assigned\_roles(u) = \{r \in ROLES | (u, r) \in UA\}$.
- $PA \subseteq ROLES \times ULOCS \times PRMS \times RLOCS$*, the relation that defines what permissions of a role from ROLES are available to a user in location from ULOCS when an accessed resource is in location from RLOCS. That is* $(r, ul, p, sl) \in PA$ *means that if user u has assigned role r she can utilize permission* $p = (req, srv)$ *to access service* $srv$ *when u is in the location ul and* $srv$ *is in the location* $sl$.
- $assigned\_perms(r : ROLES, l : ULOCS) \rightarrow 2^{PRMS \times RLOCS}$ *describes spatial permissions assigned to role r in location ul. Formally,* $assigned\_perms(r, ul) = \{(p, rl) | ul \subseteq ul'$ *for some* $(r, ul', p, rl) \in PA\}$.
- $user\_sessions(u : USERS) \rightarrow 2^{SESSIONS}$ *maps a user onto a set of sessions.*
- $session\_roles(s : SESSIONS) \rightarrow 2^{ROLES}$ *maps each session to a set of roles.*
- $avail\_session\_perms(s : SESSIONS, ul : ULOCS) \rightarrow 2^{PRMS \times RLOCS}$ *shows the permissions available in a session s in location ul. Formally,* $avail\_session\_perms(s, ul) = \bigcup_{r \in session\_roles(s)} assigned\_perms(r, ul)$.
- $auth\_user(r : ROLES, ul : ULOCS) \rightarrow USERS$ *identifies users assigned to roles with permissions available in ul. Formally,* $auth\_user(r, ul) = \{u | (u, r) \in UA$ *and* $(r, ul', p, sl) \in PA$ *and* $ul \subseteq ul'\}$.

Definition 2 describes the extension of GSRBAC to a hierarchical GSRBAC by defining the concept of role hierarchies where roles inherit permission from their junior roles.

**Definition 2 (Hierarchical GSRBAC).** *Relation RH, defined as* $RH \subseteq ROLES \times ROLES \times ULOCS$*, is a partial order on roles, with respect to location, called dominance relation, denoted as* $\succeq_{(loc)}$*, where* $r_i \succeq_{(loc)} r_j$ *for* $r_i, r_j \in ROLES$ *and* $loc \subseteq LOCS$*. It means that role* $r_i$ *inherits all permissions of* $r_j$ *in location loc, that is,* $assigned\_perm(r_j, loc) \subseteq assigned\_perm(r_i, loc)$ *that is permissions of* $r_j$ *available in loc are also available for* $r_i$ *in loc, and all the users of* $r_i$ *are also users of* $r_j$*.*

However, in order to enforce the principle of least privilege the notion of spatial Separation of Duty (SoD) in the presence of hierarchies needs to be defined. We define both Spatial Static SoD (SSSoD) and Spatial Dynamic SoD (SDSoD), where roles are mutually exclusive reliant on the location in which a user is situated. That is, two roles with assigned permissions may be mutually exclusive for a given location, however, for another location a user may be authorized to activate these two roles, since the set of permissions assigned to the roles may be different for distinct locations.

**Definition 3 (SoD).**

- $SSSoD \subseteq 2^{ROLES} \times 2^{LOCS} \times N$ *is a set of triples* $(rs, ls, n)$ *where each* $rs$ *is a role set,* $ls$ *is a normalized (defined in Section 4) location set, and* $n$ *is an integer,* $n \geq 2$*, with the property that no user can be assigned to* $n$ *or more roles from the set* $rs$ *in location* $ls$*. Formally:* $\forall (rs, ls, n) \in SSSoD, \forall l \in ls, \forall t \subseteq rs : |t| \geq n \Rightarrow \cap_{r \in t} auth\_user(r, l) = \emptyset$*;*
- $SDSoD \subseteq 2^{ROLES} \times 2^{LOCS} \times N$ *is a collection of triples* $(rs, ls, n)$ *where each* $rs$ *is a role set,* $ls$ *is normalized location set, and* $n$ *is an integer,* $n \geq 2$*, with the property that no user may activate* $n$ *or more roles from the set* $rs$ *in any normalized location loc from* $ls$*.*
  *Formally:* $\forall (rs, ls, n) \in SDSoD, \forall l \in ls, \forall s \in SESSIONS,$
  $\forall t \subseteq session\_roles(s) \cap rs : |t| \geq n \Rightarrow \cap_{r \in t} auth\_user(r, l) = \emptyset.$

SoD constraints are extended in GSRBAC with respect to locations to provide ability for spatial separation of accesses to services.

## 4 Specification of Spatial Properties

GSRBAC provides resources to express access control policies that take into consideration both user and resource mobilities in the sense that both user

and resource locations may be considered in the time of authorization decision. For the system to be able to make authorization decisions based on user and/or resource locations, a mediator must be able provably verify spatial conditions to acquire permissions enabled for the user based the user's position and resource location.

Several location-sensing techniques which vary in granularity for both indoor and outdoor position estimation of mobile terminals have been reported in the literature. The type of used location estimation technique depends on the requirement of accuracy to the mobile terminal's position which is again determined by the system in the authorization process. For example, for a user requesting access to a secure service limited to a specific room in a building, may require fine granularity in order to ensure that the user does not try to access the service from the room next door. Moreover, due to the diversity in the representation of location information, this information must be represented in a universal and flexible way, such that it can be used efficiently in the access control procedure.

In addition to obtain the location of a user, the system must also be able to perform secure location verification. This is where a user's location is securely verified to meet certain criteria, for example, residing inside a room [16]. Thus, the location information used in the authorization process must be trusted and verifiable. This is particularly important for a service that requires precise accuracy of the mobile terminal in order to prevent disclosure of classified information. Several papers have been presented that propose methods for securing the authenticity of spatial information. In [2] Brands and Chaum used distance bounding techniques (based on RF signals) to verify location claims. Similarly, Sastry et al. [16] and Waters and Felten [18] present methods for secure location verification suited for mobile devices using ultrasound and time-of-flight techniques to verify if a mobile terminal (*prover*) is within a claimed location (or is within an acceptable distance from a *verifier*). This is, however, beyond the scope of this paper, and we assume that the system can identify and verify location of any legitimate user based on a trusted underlying network architecture.

Many different approaches have been proposed to specify spatial domains. Some of them are XML-like descriptions. In this paper we describe spatial domains in more abstract manner that can be easily mapped into XML-like languages. In our access control model, in order to ensure this viability, locations are represented by means of symbolic formalism that defines locations as location expressions which describes location areas on the level of granularity that is identifiable and verifiable by the system.

We assume that areas defined in $LOCS$ cover the whole responsibility domain $D$ of GSRBAC. The domain $D$ is divided on the physical layer into subareas, called primary location cells denoted as $\pi_i$, $i = 1, \ldots, k$, based on the ability of the underlying architecture to uniquely identify and verify user's location within the cells. We assume that underlying infrastructure is unable distinguish between different locations within $\pi_i$ for any $i = 1, \ldots, k$. That is location cells define finest possible granularity of $D$. It depends on underlying location-sensing techniques and determine verifiability of location claims. The primary (physical) location cells may be used in GSRBAC policy definition but it would be not practical in many cases since changing physical locations without changing logical locations would require changes in security policy description. For example, when department offices moves to another building their physical locations are changed but their logical locations are not changed (they are still offices of the same department which means there is no need for changes in the security policy). By using logical locations in policy descriptions we need to modify the mapping function that describes mapping between physical and logical locations. The primary location cells more depend on available location-sensing technology for location verification while logical location domains reflect organizational structure.

We introduce logical location domains that reflect organizational spatial structure and organizational security policy. For example, within a University we can define logical location domains representing locations such as departments, laboratories and even individual offices. They can be defined as composition of primary cells $\pi_i$, $i = 1, \ldots, k$.

For example, the allocation of ICT department can be described as a logical location ICTdom $= [\pi_1, \pi_3]$ as an area covered by primary location cells $\pi_1$ and $\pi_3$. Similarly, LIB_dom $= [\pi_2, \pi_4, \pi_5]$ defines the library location area. Assuming that CS_dom, EE_dom and IS_dom are logical location domains for departments of Computer Science, Electrical Engineering and Information Science, respectively, we can define domain for School of Computing CSchool_dom as composition of all its departments in the form of location expression, i.e., CSchool_dom = ICT_dom +CS_dom + EE_dom + IS_dom. The example demonstrates the idea of using location expressions to define new domains.

Since logical location domains can be seen as sets we define new location domains by using domain operations that are similar to operations used in set theory, i.e., union (denoted as '+'), intersection (denoted as '$\times$'), difference (denoted as '–') and complementation (denoted as '$\neg$' or 'outside'), etc.

Generally, the same physical location may be a part of different logical spatial domains. For example, CS_dom, EE_dom may contain the same lab space. In order to simplify definitions and implementations, it is desirable to identify a least required granularity level needed for location expressions to define all meaningful location domains in GSRBAC. As it is defined in [10], a location $l$ from $ULOCS$ is called homogeneous with respect to role $r$ from $ROLES$ if $r$ has the same permission set available in any position inside $l$. Location $l$ from $ULOCS$ is called homogeneous with respect to $ROLES$, if it is homogeneous with respect to all $r$ from $ROLES$. Similarly, a location $l$ from $RLOCS$ is called homogeneous with respect to permission $p$ from $PERMS$ if $p$ is valid in any position inside $l$. Location $l$ from $RLOCS$ is called homogeneous with respect to $PERMS$, if it is homogeneous with respect to all $p$ from $PERMS$.

**Definition 4 (Normalized domains).** *Set of location domains* $L = \{l_1, l_2, \ldots, l_k\}$ *from* $ULOCS$ *are called* normalized *with respect to subset of roles* $R$ *from* $ROLES$ *if it is*

- *a partition of* $L$*, that is,* $L = \cup_{i=1}^{k} l_i$ *and* $l_i \cap l_j = \emptyset$ *for* $i \neq j$*, and*
- *any location* $l_i$ *from* $L$ *is homogeneous with respect to* $R$*.*

Assume that $LOCS$ is a set of normalized domains. Then any meaningful location domain can be presented as a union of sets from $LOCS$. From now we assume that $LOCS$ is a normalized set of locations (with respect to all roles from $ROLES$) that is a partition of the entire domain area $D$ controlled by GSRBAC.

Now we can give formal definition (Definition 5) of spatial expressions as an approach to define location domains in GSRBAC. We assume that GSRBAC model is defined such that primary location cells are normalized domains.

**Definition 5 (Spatial expressions).** *Any primary location cell is a location expression. If* $l_1$ *and* $l_2$ *are two location expressions then*

- *union of domains defined by* $l_1$ *and* $l_2$ *is described by location expression* $l_1 + l_2$*;*
- *intersection of domains defined by* $l_1$ *and* $l_2$ *is described by location expression* $l_1 \times l_2$*;*
- *difference of domains defined by* $l_1$ *and* $l_2$ *is described by location expression* $l_1 - l_2$*;*

- *complementation of a domain defined by $l_1$ with respect to the whole area covered by GSRBAC is described by location expression $outside$ $l_1$.*

The simple logical statements on spatial expression represents spatially-aware logical conditions that are either $true$ or $false$ depending on locations of users and services in the moment of evaluation. Definition 6 introduces the notion of simple logical spatial statement formally.

**Definition 6 (Simple logical spatial statement).** *Let $l$ be a location expression identifying a locations domain. Assume $a_1, a_2$ are users from USERS or a resources/services from SERVICES.*

- *condition $a_i$ inside $l$ is true when $a_i$ is inside the domain identified by $l$ at the time of validation;*
- *condition $a_i$ outside $l$ is true when $a_i$ is outside the domain identified by $l$;*
- *condition anywhere is true for any location;*
- *condition $a_1$ close-to $a_2$ is true when $a_1$ is physically close to $a_2$.*

Simple logical spatial statements can be used to construct compound logical statements using traditional logical connectives like conjunction, disjunction, etc. The compound logical spatial statements are spatial conditions defined on $ULOCS$ and $RLOCS$ that serve as guards for permissions and must be satisfied for permission to be granted.

## 5 Emergency Aware Role-Based Access Control: A Spatial Case

In this section we consider a case when GSRBAC should be preferred comparing to previously proposed approaches. Consider, for example, use of RBAC system to handle access control in the case of medical emergency. Handling emergency situations means that someone without having assigned a role with actual permissions should be able to perform some actions (for example, life saving actions). In this section we consider a spatial solution to handle such emergency situations.

An approach to handle emergencies in medical setting has been proposed recently [7,8]. The proposed approach is based on enforcement of "breaking-the-glass" principle. It means that someone who is a user of an RBAC-based system but without actual permission can "break the glass" and get needed permissions in the case of emergency. The approach was extended to mobile

setting in [14] to handle life-critical situations when users who are not a part of $USERS$ (and cannot be authenticated by the system) must access resources. To permit such access of unauthenticated users or in other words permit "breaking the glass", SRBAC [14] requires users to be in pre-specified locations. However in GSRBAC we can express a "proximity" requirements (which is a more general case) that would require to be close to for example ambulance car or life-saving equipment.

Let us illustrate how GSRBAC can be used to provide access of unauthenticated user in the case of emergency in the proximity of life-saving equipment.

We propose to define a special emergency role $r_E \in ROLES$ that may be activated by users only from specific locations: for example, close to life-saving equipment $X$ or in the hospital $Y$ (assuming that underlying system is able to verify such spatial properties). We also define an emergency handler user $u_E \in USERS$ that can be available in the system and does not require authentication (kind of "guest" user). Assume that permissions $p_1, \ldots, p_k$ are needed to provide necessary emergency care to the patient. These necessary permissions will comprise role $r_E$ with added spatial constraint $t$ on the activating user location: $r_E = \{t : [p_1, \ldots, p_k]\}$ where $t$ is a logical spatial statement $t = (close\_to(X)) \vee (inside(Y))$. The only role assigned to user $u_E$ is the emergency role $r_E$, that is $(u_E, r_E) \in UA$ and $assigned\_roles(u_E) = \{r_E\}$ but $assigned\_users(r_E) = USERS'$ where $USERS' \subseteq USERS$ and $USERS'$ is a set of those legitimate users in the system that may "break the glass" [7, 8] (that is, activate $r_E$).

## 6 Conclusions

In this paper we present Generalized Spatial RBAC (GSRBAC), a model that extends RBAC and SRBAC to incorporate location information associated with roles and services in order to permit location-based definition of security and energy related policies. In the GSRBAC model, permissions are dynamically assigned to the role depending on location of a user and may be granted if in addition location of the requested service satisfies specified spatial constraints. Incorporating spatial information in RBAC as proposed in GSRBAC would enable RBAC to define more elaborated and fine-grained security policies with requirements to implement both more secure and green (energy-efficient) future mobile applications.

## References


[1] S. Aich, S. Sural, and A. Majumdar. Starbac: Spatiotemporal role based access control. In R. Meersman and Z. Tari (Eds.), *On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS*, Lecture Notes in Computer Science, Vol. 4804, pp. 1567–1582. Springer, Berlin/Heidelberg, 2007.

[2] S. Brands and D. Chaum. Distance-bounding protocols (extended abstract). In *Theory and Application of Cryptographic Techniques*, pp. 344–359, 1993.

[3] S. Chandran and J. Joshi. Lot-RBAC: A location and time-based RBAC model. In A. Ngu, M. Kitsuregawa, E. Neuhold, J.-Y. Chung, and Q. Sheng (Eds.), *Web Information Systems Engineering WISE 2005*, Lecture Notes in Computer Science, Vol. 3806, pp. 361–375. Springer, Berlin/Heidelberg, 2005.

[4] M.L. Damiani, E. Bertino, B. Catania, and P. Perlasca. Geo-RBAC: A spatially aware RBAC. *ACM Trans. Inf. Syst. Secur.*, 10:1–42.

[5] D.F. Ferraiolo, D.R. Kuhn, and R. Chandramouli. *Role-Based Access Control*. Artech House, 2003.

[6] D.F. Ferraiolo, R. Sandhu, S. Gavrila, D.R. Kuhn, and R. Chandramouli. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, 4(3):224–274, 2001.

[7] A. Ferreira, D. Chadwick, P. Farinha, R. Correia, G. Zao, R. Chilro, and L. Antunes. How to securely break into RBAC: The BTG-RBAC model. In *Proceedings of Annual Computer Security Applications Conference (ACSAC'09)*, pp. 23–31, December 2009.

[8] A. Ferreira, R. Cruz-Correia, L. Antunes, P. Farinha, E. Oliveira-Palhares, D. Chadwick, and A. Costa-Pereira. How to break access control in a controlled manner. In *Proceedings of 19th IEEE International Symposium on Computer-Based Medical Systems (CBMS2006)*, pp. 847–854, 2006.

[9] S.M. Futaci, K. Jaffres-Runser, and C. Comaniciu. On modeling energy-security tradeoffs for distributed monitoring in wireless ad hoc networks. In *Proceedings of Military Communications Conference (MILCOM2008)*, 16–19 November, pp. 1–7, IEEE, 2008.

[10] F. Hansen and V. Oleshchuk. Spatial role-based access control model for wireless networks. In *Proceedings of IEEE Vehicular Technology Conference (VTC2003)*, Vol. 3, pp. 2093–2097, 2003.

[11] F. Hansen and V. Oleshchuk. SRBAC: A spatial role-based access control model for mobile systems. In *Proceedings of the Seventh Nordic Workshop on Secure IT Systems (Nordsec 2003)*, 15–17 October, pp. 129–141, 2003.

[12] F. Hansen and V. Oleshchuk. Location-based security framework for use of handheld devices in medical information systems. In *Proceedings of Fourth Annual IEEE International Conference on Pervasive Computing and Communications, PerCom Workshops 2006*, 13–17 March, pp. 564–569, 2006.

[13] M. Migliardi and A. Merlo. Modeling the energy consumption of distributed IDS: A step towards Green security. In *MIPRO, 2011 Proceedings of the 34th International Convention*, 23–27 May, pp. 1452–1457, 2011.

[14] V. Oleshchuk and R. Fensli. Remote patient monitoring within a future 5G infrastructure. *Wireless Personal Communications*, 57: 431–439.

[15] I. Ray, M. Kumar, and L.Yu. Lrbac: A location-aware role-based access control model. In A. Bagchi and V. Atluri (Eds.), *Information Systems Security*, Lecture Notes in Computer Science, Vol. 4332, pp. 147–161. Springer, Berlin/Heidelberg, 2006.

[16] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *WiSe'03: Proceedings of the 2003 ACM workshop on Wireless Security*, pp. 1–10, ACM Press, 2003.

[17] K.K. Venkatasubramanian, A. Banerjee, and S.K.S. Gupta. Green and sustainable cyber-physical security solutions for body area networks. In *BSN2009, Sixth International Workshop on Wearable and Implantable Body Sensor Networks*, 3–5 June, pp. 240–245, 2009.

[18] B.R. Waters and E.W. Felten. Secure, private proofs of location. Technical Report TR-667-03, Princeton University, January 2003.

## Biography

**Vladimir Oleshchuk** is Professor of Computer Science at University of Agder, Norway. He received his MSc in Applied Mathematics (1981) and PhD in Computer Science (1988) from the Kiev State University, Ukraine, and his MSc in Innovations and Entrepreneurship (2007) from the Norwegian University of Science and Technology (NTNU). He has been working at University of Agder since 1992. He is a member of IEEE and a senior member of ACM. His current research interests include formal methods and information security, privacy and trust with special focus on mobile and healthcare applications.