Proximity Based Access Control in Smart-Emergency Departments *

S.K.S. Gupta T.Mukherjee K.Venkatasubramanian
Dept. of Computer Science and Engineering
Arizona State University
Tempe, Arizona, 85287
http://impact.asu.edu

T.B.Taylor
MediServe Information Systems
Tempe, Arizona, 85282
http://www.mediserve.com

Abstract

In this paper, we propose a Proximity Based automated Access Control (PBAC) model for smart-ED environments which improves the existing ED work-flow by automating mundane administrative procedure for secure information access, allowing caregivers to focus on the treatment of patients. The proposed access model builds on the traditional role-based access control model and extends it by including multiple authentication levels for preventing unauthorized access. We also provide a semi-formal specification for the PBAC model. We further validate it using ultra-wide-band (UWB) based prototype which was tested in ED.

1 Introduction

Hospital emergency departments (ED) must provide effective and timely treatment to all patients, many times in an unpredictable environment. Mundane activities such as data entry and retrieval often impact ED efficiency by distracting caregivers who must interface with multiple secured hospital information systems to accomplish these tasks. Automating certain tasks, such as authentication login, will reduce these distractions and allow caregivers to concentrate on treating patients [4]. For example, if in a smart-ED, caregivers needing access to a patients medical history can be automatically logged-in, without typing a user name or password, by virtue of their proximity to a computer, they can continue to provide patient care and review clinical data without being distracted.

Proximity-based access, however, has certain pitfalls in that it could potentially allow someone (even an unauthorized person) access, when an authorized user is in proximity but not currently using the resource. For example, a nurse standing by a computer should not be able to gain access to a doctor's log-in when the doctor is merely in proximity of the resource. To handle such conflicts, the system must include authentication mechanisms to prevent users from accessing resources, at a level, they are not actually entitled.

In this paper, we introduce a mechanism for providing automated access to resources in a smart-ED environment called Proximity-Based Access Control (PBAC). This scheme makes access control decisions based on the proximity of the user to a particular resource such that when the user arrives in the proximity of the resource, access with the appropriate privileges is automatically granted. To implement the PBAC model we first defined the notion of *proximity* of a resource by designing a specific area, called *proximity zone*, around the resource. The shape and size of the proximity zone is designed based on the following parameters: the three-dimensional accuracy of the positioning system employed, geometry of the physical workspace in the ED, the electromagnetic environment and the access control requirements for the designated resource.

Appropriate access privileges are determined by using a form of Role-Based Access Control (RBAC)[2], whereby users are assigned different roles, and based on these, are granted predefined access privileges to the resources. Further, the RBAC model is enhanced by introducing multi-level authentication to resolve resource access conflicts arising from the presence of multiple users in the proximity of a resource.

To the best of our knowledge, proximity based automated access has never been integrated in ED system design. In [7], a Spatial Role Based Access Control (SRBAC) model has been used for health-care applications where a medical personnel's role (consequently the associated privileges) is varied based on the current space they inhabit. However they do not focus on providing automated access to resources, an essential necessity for improving the smart-ED work-flow.

Our main *contribution* in this paper is to design, specify and validate a PBAC model for ED environments. The proposed PBAC model *enhances the work-flow* in the ED by providing automated access control to the resources.

*Supported in part by MediServe Information Systems, Consortium for Embedded Systems and National Science Foundation grant ANI-0196156

Further, by incorporating different levels of authentication, the model *prevents the security pitfalls* normally associated with proximity based access control mechanisms.

Our paper is organized as follows, Section 2 presents the motivation for this work, followed by Section 3 which presents the concept of Proximity Based Access Control and its design issues. Section 4 provides details of the access control model, while the access control policies applicable for a PBAC based system are specified in Section 5. In Section 6, we present a prototype for the PBAC scheme using a commercially available UWB-based positioning system and finally conclude in Section 7.

2 Motivation

When patients arrive at an ED, they follow a certain well-defined service paths. The actual path however often depends on their condition. Patients may arrive by public or private vehicles, on foot, or by ambulance. Once identified as requesting emergency evaluation, patients are logged-in, triaged by a nurse (either in a triage area or in a treatment room) and are registered at an appropriate time. Critical patients, who most often arrive by ambulance and require immediate medical attention, usually bypass triage and are taken directly to a treatment room or specialized area such as a trauma or resuscitation room [4].

The process of tracking patients through arrival, triage, treatment and discharge has traditionally been a cumbersome, incomplete and inaccurate manual process. Physicians, nurses, and other caregivers often require access to several data systems, each requiring a unique log-in process. Aside from remembering several passwords, these log-in processes distract staff from their natural work-flow. Session loading and unloading may also detract from patient care. An access control system that automatically logs-in a pre-authenticated user to a resource, will reduce distraction, improve efficiency and improve patient care.

Further, caregivers tend to leave computer resources open without closing their session after each use. Although typically the system automatically closes the session after a preset inactivity interval, patient information is vulnerable to inappropriate access during this time. Using an effective access control model, we can improve the ED work-flow efficiency and eliminate the said vulnerability by automatically closing or suspending a session immediately after a user has left the vicinity of the resource.

In this paper we present a Proximity Based Access Control (PBAC) model for automating access to resources in the ED environment.

3 Proximity Based Access Control

PBAC is a technique for providing automated access to resources based on the proximity of a user to that resource.

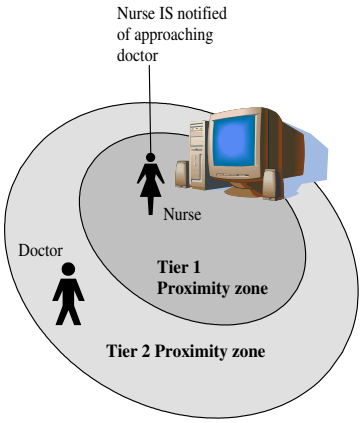

Figure 1. Two-tiered Proximity Zone

Proximity can be defined as a zone around the resource, within which, a user must be located in order to gain access. There are three main aspects of PBAC necessary to determine the accuracy of the access control automation process: 1) The design of the zones which define the proximity of resources; 2) The three-dimensional accuracy of positioning system employed to verify when a user is in the proximity zone; 3) The level of access provided to users within proximity of a resource.

The first two aspects ensure that a user only gains access to a resource when in the correct position respective to that resource, while the last enforces information security and priority of use.

3.1 PBAC Zones and Positioning

The determination of a proximity zone (see Figure 1) around a resource is tied inextricably to the three-dimensional accuracy of the positioning system responsible for determining the location of the user. This accuracy of the positioning systems depend on the electromagnetic characteristics of the environment they are deployed in and may vary dynamically over time. To compensate for errors, techniques like long-term error contour maps could be generated for the positioning systems and used to determine its positioning accuracy. Several positioning systems are commercially available today, they can be roughly classified into three main types: Radio frequency (RF) narrow-band, RF with ultrasound and Ultra-Wide Band (UWB). In indoor environments, UWB typically has better performance because: 1) UWB has short signal pulse making it less vulnerable to multi-path effects; 2) The interference noise is normalized over the wide signal band which has minimal effect on the Signal-to-Noise Ratio (SNR); 3) UWB operates in the 3-10GHz frequency range where few other devices

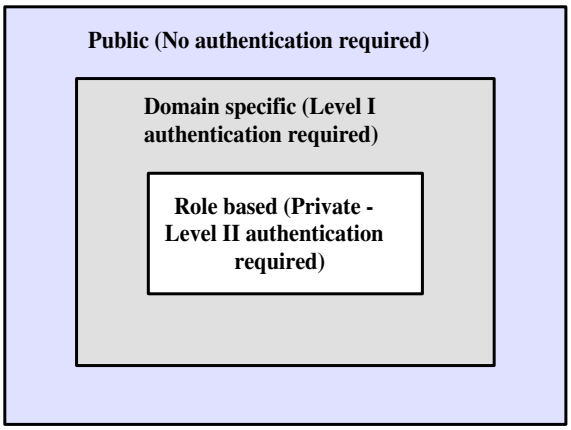

Figure 2. Authentication Levels

would cause interference.

Apart from the positioning system, the proximity zones around resources are dependent on the access control policies for the resource. For example, suppose the access control policy of a resource mandates that a nurse yield the resource to a doctor and that the system display an on-line notification when the doctor is approaching the resource. In this scenario the system must be able to predict the movement of the doctor and notify the nurse well in advance to allow completion of work. A potential solution to this requirement would be to define a two-tier proximity zone around the resource. A small inner zone enveloping the resource would determine the resource access while a larger outer zone (e.g. the room where the resource is located) would detect anyone (i.e. the doctor) approaching the resource. Access to a vacant resource is only granted when the user enters the inner zone. However, once logged-in, the system could be configured to log-off the user only after they leave the outer zone. Establishing two-tiered proximity zones for each resource provides for the most flexibility when writing and revising access control policies. Figure 1 shows examples of the two-tier resource proximity zones.

It should be noted that access control policies and positioning accuracy only provide general guidelines for the design of the smart space, while their actual shapes and sizes are defined by the accuracy of the positioning system. Geometry of the space is a third factor affecting proximity zone design and supersedes these other requirements due to its immutable characteristics.

3.2 Information Access Granularity

Simply defining PBAC zones as noted above is not sufficient to manage multiple users with varying degrees of security access. A doctor passing through the proximity of a resource (without any intension of using it) may get automatically logged in, allowing a malicious entity access the resource with her (doctor's) privileges. We address this issue using a multi-level authentication approach by defining three authentication levels (Figure 2) of information access:
1. *No-Authentication*: User access is restricted to publicly available data. For example, bulletin announcements, Internet access etc.
2. *Authentication Level-I*: Is applicable to individual domains (like ED, ICU). Caregivers on entering a domain, perform a simple challenge/response (using an RFID badge, for example) and are authenticated at this level. Once authenticated, the caregivers get a common set of privileges for the domain. For example, if the domain in an ED, all the doctors and nurses in it will be able obtain a common set of privileges specific to the ED and its patients.
3. *Authentication Level-II*: Used by caregivers who want to access sensitive patient information not freely available at Level-I. They have to perform an additional more rigorous authentication steps (like using a PKI authenticator [6]) to be authenticated at this level.

This authentication scheme, thus, complements the access control model while facilitating appropriate level of access privileges to end users.

4 Role Management in PBAC

Authentication restricts the access to resources to prevent malicious acts. We however still need to decide the granularity of access that users get once they are authenticated. We use a variant of the Role Based Access Control model specified in [3] for addressing this issue. In our approach to PBAC, we define two main types of roles - **organizational** and **group**. The organizational role is assigned to a user when they join the system and usually corresponds to the actual position held by the user within the organization, for example a person joining a hospital as a doctor gets an organizational role of a *doctor*. Group roles assigned to users are more specialized in nature and are based on a specific area or domain where the user works. For example, users working in the trauma resuscitation area of the ED form a group and get assigned to a specific group role. Each user has one organizational role, but may have multiple group roles.

Each resource is assigned an access control list (ACL) which is a table of possible roles (called resource-roles) and corresponding privileges. Each user's group role and current contextual information is mapped on to a particular resource-role (by a resource) whose corresponding privileges are assigned to the user. This is particularly true when users authentication themselves at Authentication Level-II. However at Authentication Level-I, the privileges provides to a user is a function (union, intersection) of privileges associated with individual resource-roles of all the users in the domain. Figure 3 shows the ACL maintained by a resource

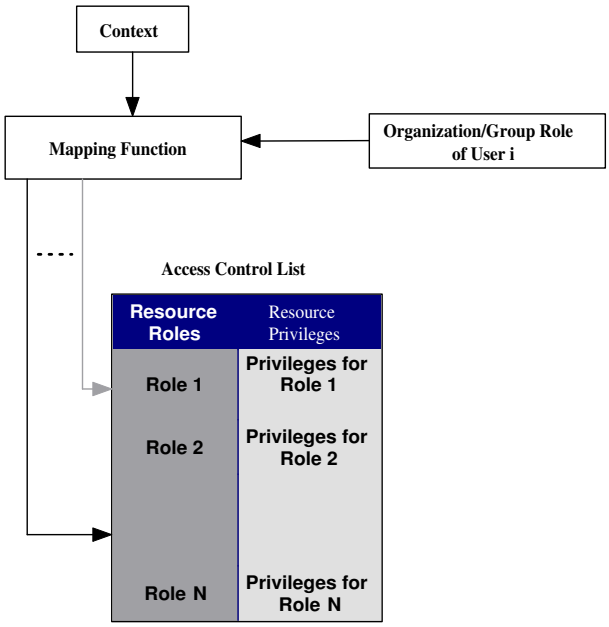

Figure 3. Mapping of Group Role to Resource Role

and the mapping of a user's group role to a particular resource role.

When a user comes within the proximity zone of a resource, the resource determines the role of this user and maps it on to a resource-role. Users can thus access resources based on the privileges associated with the resource-role. To provide access, the PBAC adheres to certain policies which enforce the correct working of the system. In the next section we present PBAC policy overview.

5 Access Control Policy Specifications

There are two types of policies for the PBAC system: 1) **Administrative Policies** - Rules for defining system administration functions, such as adding users, assigning roles, privileges, etc; 2) **Access Control Policies** - Rules to control access to resources within the system (i.e. the decisions to account for the various roles, associated privileges and contextual information of the system at the time of the access).

The administrative policies ensure that medical personnel have been properly assigned the roles in the system (hospital), whereas the access control policies take these user roles and assist in providing automated access to resources in specific hospital domains (like ED).

5.1 Administrative Policies

We have two pairs of administration policies, one for adding and removing organizational roles and other for adding and removing group roles. Administrative policies are crucial and can be enforced by the system administrator only. For any user to obtain a group role, she needs to have an organizational role first. Organizational roles are assigned to users based on their work in the system

5.2 Access Control Policies

When a user is in the proximity of a resource, they are given access to it based on the the access control policies described next. When a user comes within the proximity zone of a resource they are granted access to the resource. A function named $checkRole$ is used to determine the appropriate role for the user and performs the following functions: 1) Maps the user's group role to the appropriate resource-role; 2) Generates the resource role for all the users in the group using a function f (to provide privileges corresponding to the Authentication Level-I). Another function called AR then maps the returned resource role to appropriate privileges. The function $Enters(u, Z)$ returns true when a user u enters the zone Z of a resource, while the function $PBAC(u)$ stores the current privileges of the user u. When the user leaves the zone Z (function $Exits(u, Z)$ returns true) of a resource PBAC of the user becomes empty (ϕ).

Algorithm 1: Single User in Proximity to Unoccupied Resource
1. User enters the proximity of a resource;
2. if $(Enters(u, Z))$
3. $\quad PBAC(u) = AR(checkRole(u))$
4. endif
5. if $(Exits(u, Z))$
6. $\quad PBAC(u) = \phi$
7. endif

Algorithm 2: Single User in Proximity to Occupied Resource
1. User enters the proximity of a resource;
2. if $(Enters(u2, Z) \wedge Contains(u1, Z) \wedge logout\_init(u1))$
3. $\quad PBAC(u1) = \phi$
4. $\quad PBAC(u2) = AR(checkRole(u2))$
5. endif

Algorithm 3: Multiple Users in Proximity to Unoccupied Resource
1. User enters the proximity of a resource;
2. if $(Enters(u*, Z))$
3. $\quad chosen\_user = Rand(u*) \vee Closest(u*) \vee Earliest(login\_init(u*)$
4. $\quad PBAC(chosen\_user) = AR(checkRole(chosen\_user))$
5. endif

Algorithm 1 defines the function of automatic user login and logout on a unused resource. If another user ($u2$) enters in the zone Z (see Algorithm 2) of a resource when

another user $u1$ is accessing it($Contains(u1, Z)$), then $u1$ has to explicitly logout ($logout\_init(u1)$) before $u2$ can login. Algorithm 3 presents the scenario where multiple users enter the zone Z at the same time ($Enters(u*, Z)$), then the policy dictates giving access in one of the three ways: randomly, to the user who is closest to the resource, or whoever requests of the resource first. When a user leaves a resource, the system checks to see how many other users are in the proximity and uses one of the three aforementioned techniques to give system access to the user.

6 Prototype Development

In order to verify our ideas, we performed certain preliminary experiments and built a system prototype for the PBAC using a commercially available UWB-based positioning system developed by Ubisense Inc [5]. We tested the system in a functioning Level-One Trauma Center ED of a major hospital in the Phoenix area. In separate experiments, we used 4 sensors to create a tracking cell in two structurally different treatment areas within the ED. In each case we found that the UWB system provided a localization accuracy of about *2-8 inches*.

One of the important aspects of our proposed PBAC scheme is the design of the proximity zone around resources. The design of proximity zone has two aspects: 1) the shape of the proximity zone mandated by the application and its environment (policies, geometry of the area), and 2) the accuracy of the positioning system under the ED's radio environment. If S_{app} denotes the shape of a proximity zone and R_{app} is the set of distances from the resource to its boundary (mandated by the application), then we design the proximity zone as follows: 1) The shape of the proximity zone (S) is left unchanged, i.e. $S = S_{app}$; 2) The set of distances from the resource to the boundary of the proximity zone (R) is given by $R_i = i + \delta$ for all $i \in R_{app}$, where δ is the error imposed by the positioning system accuracy in ED. For example, if the application mandated proximity zone as a circle with a radius of 5 feet around the resource, and δ is calculated as the maximum error in the positioning system (according to our experiments $\delta = 8$ inches), then we can compute the actual proximity zone as a circle with a radius of 5 feet and 8 inches.

We have also developed a prototype for the proposed PBAC scheme which relies on the aforementioned positioning system for detecting proximity. The prototype was tested on the Ubisense tracking simulator and involved 2 doctors and 1 nurse. We tested this prototype for the following four scenarios:
1) *Single user (medical personnel) trying to access an unoccupied resource* - In this case, when medical professional is detected within the proximity of an unoccupied resource (by the positioning system), she is immediately granted access to it as per Steps 2 and 3 of Algorithm 1.
2) *Multiple users trying to access an unoccupied resource* - Here, the idea is to resolve the conflict between the multiple users. Therefore, when multiple users are detected within a (unoccupied) resource proximity the system logs-in the user as per the assertions in Step 1-5 of Algorithm 3.
3) *User in proximity without requiring access* - We address this issue at the policy level itself by specifying a function $Enters(u, Z)$ whose implementation ensures that only users present within the proximity zone for a certain amount of time are provided access.
4) *Temporary absence of a logged in user from resource proximity* - The $Exits(u, Z)$ function abstract this idea and ensures that users' session is closed only after substantial absence from the resource proximity.

Both $Enters(u, Z)$ and $Exits(u, Z)$ mentioned above have been implemented using the APIs provided by Ubisense.

7 Conclusions

In this paper we designed and formulated an access control model (PBAC) for improving emergency department work-flow. The scheme provided access to resources based on medical professionnel's: 1) proximity to a resource, and 2) role in the system. We further enhanced this model by including a multi-factor authentication scheme which prevented unauthorized resource access. This model was prototyped using UWB-based positioning system and found to be a viable technology in real ED environments.

Acknowledgments

We gratefully acknowledge the intellectual contributions of Valliappan Annamalai, Vikram Shankar of the IMPACT Lab at Arizona State University and the support of Bruce and Zach Mortensen of MediServe Information Systems.

References

[1] F.Adelstein, S.K.S.Gupta, G.G.Richard and L.Schwiebert "Fundamentals of Mobile and Pervasive Computing". *McGraw Hill*, 2005

[2] R. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman "Role Based Access Control Models". *In IEEE Computer*, Feb, 1996.pp 38-47

[3] G. Sampemane, P. Naldurg and R. H. Campbell. "Access control for Active Spaces". *In Proc. of ACSAC*, 2002

[4] T. B. Taylor "A View of the Emergency Department of the Future.". *ACEP Section for Emergency Medical Informatics* 2000, Dallas, TX

[5] Ubisense. *http://www.ubisense.net/*

[6] Unified Authentication Tokens. *http://www.verisign.com/products-services/security-services/unified-authentication/index.html/*

[7] F Hansen, V Oleshchuk "Application of role based access control in wireless healthcare information systems.". *Proc. For Scandinavian Conference in Health Informatics* 2003