2013 Fourth International Conference on Emerging Security Technologies

Spatio-Temporal Role Based Access Control for Physical Access Control Systems

Emsaieb Geepalla
School of Computer Science
University Of Birmingham
Birmingham, UK
Email: E.M.E.Geepalla@cs.bham.ac.uk

Behzad Bordbar
School of Computer Science
University Of Birmingham
Birmingham, UK
Email: B.Bordbar@cs.bham.ac.uk

Xiaofeng Du
BT Technology Service and Operations,
BT Plc, UK
Email: xiaofeng.du@bt.com

***Abstract*—Due to the large size of the global enterprise and the complexity of job's functions within organisations, managing Physical Access Control (PAC) policies has become a challenging problem. It is therefore, very important to develop Access Control mechanisms that can be deployed by organizations to meet their information security needs. In this paper we first demonstrate that current Access Control models such as Spatio-Temporal Role Based Access Control (STRBAC) are not adequate for representing PAC specifications. We then discuss some of the limitations of the current models, which we highlight by conducting a case study involving the modelling of an Access Control mechanism used by a leading telecommunications company. To overcome such limitations, we present an extension of the STRBAC model which considers the physical aspects of Access Control systems. The second contribution in this paper is using our earlier method AC2Alloy to analyse PAC specifications using Alloy analyser to ensure the consistency of the specifications.**

I. Introduction

In the last decades, researchers have proposed several Spatio-Temporal Access Control models [1, 2, 3], such as Spatio-Temporal Role Based Access Control (STRBAC) [1], to support policy designers in designing proper Access Control specifications, especially the Cyber Access Control (CAC) specification. Although these models offer many benefits for implementing CAC systems, they are not adequate enough to represent Physical Access Control (PAC) specifications and still have some limitations that should be overcome prior modelling the physical aspect of Access Control. One of the major drawbacks to these models is the representation of locations, as current models deal with logical location, which may not be suitable for representing the physical aspect of Access Control. This is a critical point, because logical location and physical location are different, especially when dealing with hierarchy. We came across such limitations when trying to model a PAC mechanism used in a leading telecommunications company. Extending the existing models to overcoming such limitations is very important, because such extension will assist systems' designer to create correct PAC specifications.

To overcome such limitations, this paper presents a new Spatio-Temporal Role Based Access Control for Physical Systems (STRBAC-PS). Our model extends the Access Control model that proposed by Ray and Toahchoode [1] in a manner such that it can be used to specify PAC policies. The STRBAC-PS model consists of various rules that can be employed to support various system requirements. These rules may interact with each other in subtle ways and result in inconsistencies, which must be detected before the implementation of the system. Therefore, we make use of our method AC2Alloy [9], to ensure the consistency of the specification. A real world case study is used to demonstrate the feasibility of our approach.

The paper is organized as follows. In Section II, a brief introduction into the STRBAC model and AC2Alloy is provided. Section III describes the PAC system. This is followed by a description of the problem in section IV. Section V presents our efforts to develop the new framework STRBAC-PS. In section VI, AC2Alloy is used to analyse the PAC specification. The paper ends with a conclusion.

II. Preliminary

A. STRBAC Model

The Spatio-Temporal Role Based Access Control (STRBAC) model [1, 4] is an extension of the original RBAC model [7] that supports temporal and location constraints. The STRBAC model is very useful for providing a high level description of Access Control, especially when the time and location information are required to grant or deny access to the resources. For more details about the STRBAC model we refer the reader to [1, 4].

B. AC2Alloy

AC2Alloy [9] is an Eclipse Plug-in application that makes use of the Model Driven Architecture (MDA) [6] technology SiTra (Simple Transformer) [8] to auto-generate Alloy from the Access Control specification in the context of the STRBAC model. AC2Alloy transforms the STRBAC specification into XML representation of the STRBAC specification, and then an Alloy model will be automatically generated from the XML representation. The produced Alloy model can then be automatically analysed using Alloy Analyser [5], which is a SAT-solver based identify an erroneous design. For more details about AC2Alloy we refer the reader to [9].

III. Physical Access Control (PAC) System

In a large organisation such as a leading telecommunications company which deals with physical and cyber infrastructure, managing PAC policies is a complex task. The complexities arise mainly from the following four aspects:

978-0-7695-5077-0/13 $26.00 © 2013 IEEE
DOI 10.1109/EST.2013.13

- A large number of building/zones with distributed geo-locations
- Buildings with different risk levels, which required different levels of Access Control.
- A variety of users who have access to buildings based on a mixture of roles such as permanent employees and an outsourcing workforce.
- Time constraints for accessing the building/zones. For example, certain zones can be accessed during the day but during the night they are locked.
- Physical access can invalidate cyber access. For example, if a machine is protected by a firewall but people can physically access to it, then they can access the hard disk and copy it.

An example of Physical Access Control (PAC) is as follow:

- A user swipes ID card to submit his or her user profile to the system to verify the user information.
- The card reader reveals which building or zone the user is accessing and therefore, submits the user profile and building profile to the system.
- Both profiles (user profile and building profile) are processed by the Physical Access Control (PAC) system. The process involves a rule engine that has full knowledge of the physical access policies. It compares the two profiles and makes an access decision.
- Two possible results (access granted or access denied) can be returned by the Access Control process.

During the access granted process, time and location are also important factors. For example, if a user tries to access a building/zone outside of his/her working hours or, in a different geographical location from his/her normal working region, then access may not be granted.

A. Running Example: Physical System

1) Security Policies:

a) Entity: In organisations such as telecommunications company users are mainly categorised based on their job type. Examples of these categories may consist of company employees, technical employees, clerical employees, and cabling engineers. The organisations are based on several regions (for example, Birmingham region, Manchester Region). Every region consists of several buildings such as `x, y, z`, which contain several zones or rooms such as server room and common room. Each Physical Access Control point (a card reader, for example), can be considered as a zone or room entrance. In this paper, we assume that the organisation is based on one region (*Birmingham Region*) and it only consists one building `(x)`, which contains three zones: Low Risk Zone, Medium Risk Zone and High Risk Zone as depicted in Figure 1. The organisation also employs thousands of users. `Dave, Mark, Tom, Sarah, Amy` and `Hannah` are a small list of the users within the organisation that has been chosen to illustrate our approach. Examples of the different permissions that users can have are listed in Table I.

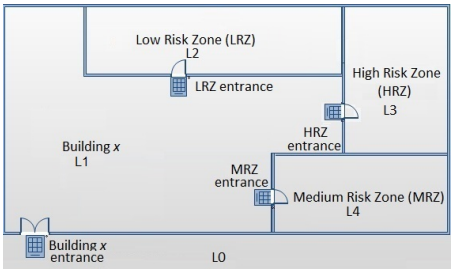

Fig. 1. Location

TABLE I. LOST OF PERMISSIONS

	Permission
P1	Access Building *x*
P2	Access Low level zone (i.e. common room)
P3	Access medium level zone (i.e. data center)
P4	Access High level zone (i.e. server room)
P5	Access street cabinets

Users are assigned to roles based on the timed and location constrains as illustrated in Table II. Moreover, the roles are assigned to the permissions based on the time and location constrains as summarised in Table III.

TABLE II. USERS TO ROLES ASSIGNMENT CONSTRAINTS

Users	**Roles**	**Times**	**Locations**
Dave	cabling engineer	DayTime	L5: street cabinets Birmingham Region L2: Low Risk Zone Birmingham Region
Sarah	cabling engineer	DayTime	L5: street cabinets Birmingham Region L2: Low Risk Zone Birmingham Region
Tom	cabling engineer	DayTime	L5: street cabinets Birmingham Region L2: Low Risk Zone Birmingham Region
Amy	technical engineer	DayTime	L3: High Risk Zone Birmingham Region
Mark	clerical employee	DayTime	L4: Medium Risk Zone Birmingham Region
Hannah	company employee	DayTime	L2: Low Risk Zone Birmingham Region

TABLE III. PERMISSIONS TO ROLES ASSIGNMENT CONSTRAINTS

Role	**Permission**	**Time**	**Location**
company employee	P2	DayTime	L2
cabling engineer	P5 P2	DayTime	L5 L2
technical engineer	P4	DayTime	L3
clerical employee	P3	DayTime	L4

b) Role Hierarchy: The hierarchy of roles in the telecommunications company is depicted in Figure 2.

c) Separation of Duty between Roles: The telecommunications company requires that the same user should not be *Clerical Employee* and *Cable Engineer* at the same time and the same location.

d) Cardinality Constrain over Roles: For health and safety the telecommunications company requires that no more than two users should have the role *Cable Engineer* at the location `L5` *(street cabinet)* and during the same time.

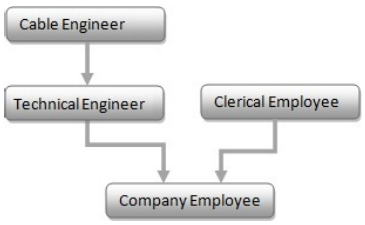

Fig. 2. Role Hierarchy

IV. Description of the Problem

Representation of locations is one of the major limitations of the current STRBAC model that needs to be overcome in order to be able to specify all of the security requirements for the Physical Access Control systems. This is because the STRBAC model deals with logical locations which may not be suitable for PAC specifications. Next we shall explore the differences between logical and physical locations.

A. Logical Location v.s Physical Location

Locations in Cyber Access Control (CAC) systems specify a set of logical entities. This model is not sufficient for capture access to resources. For example, due to the presence of doors and locks we need to create a model which shows how access to locations require credentials to access other locations.

B. Differences Between Hierarchy of Location in the Cyber and Physical Systems

In general, Location Hierarchy is a partial order on the set of Locations, that specifies which location is inside another location (i.e. l_i is inside l_j). In the cyber systems this means that if a user u is assigned a role r and its permission p at a time t and at the outer location l_j, then the same user u can have the role r and the permission p at the inner location l_i. This is may not be true in the Physical Access Control, where having a permission to access to the outer location does not necessary mean the same user will be granted access to the inner locations. For example, in Figure 1, if a user u has permission to access the location `L1`, this does not necessary mean the same user u will have permission to access the any of the inner locations `L2`, `L3` and `L4`. As a result, hierarchy of location in the Physical Access Control is not the same as the hierarchy in Cyber Access Control.

V. The Proposed Model: STRBAC-PS Model

Spatio-Temporal Role Based Access Control for Physical Systems (STRBAC-PS) is a model that extends the STRBAC model to be capable to describe the specification of Physical Access Control. in such a way that it becomes capable of describing the specifications of Physical Access Control. It is similar to the STRBAC model in that the STRBAC-PS has the basic sets of entities: Users (U), Roles (R), Permissions (P), Times (T). However, we have introduced an additional set; Location Graph (LG) to replace the set of Locations. Next we shall briefly describe these entities, but before that we present the location model for Physical Access Control (PAC) systems.

A. Extend Location Models for Physical Access Control

In order to formalise the Physical location we introduce the concept Location Graph `(LG)`, which is a graphical model that emphasises both the locality and the connectivity of Physical Access Control (PAC) systems.

Definition 1: Location Graph `LG`=(l_0, L, E), where L is a finite set of nodes and $E \subseteq L \times L$ is a set of directed edges connecting the nodes of L. Nodes in L, which are sometimes called *locations* consist of (possibly) multiple rooms, corridors, ... etc, so that if a person can access one of them, then he/she can access all of them. L has a unique node called *outside* location represented as $l_0 \in L$, which represents the entire world outside the premises. Edges E represent links which are marked by permissions. We define the allocated permissions function as $m : E \rightarrow P \cup \{\epsilon\}$, where $m(e)$ is the permission marking the edge e. $e = (l, l')$ showing the permissions required to go from l to l'. If $m(e) = \epsilon$, then a person does not need any permission for going from l to l'. Sometimes we simply write the permissions on the edge to represent the allocated permission. In this case we can write $l \xrightarrow{p} l'$ to say that, for going from l to l' the permission p is required. For example, the physical location depicted in Figure 1 can be represented using Location Graph as illustrated in Figure 3. Figure 3 shows that a user requires a set of permissions in order to be able to move from one node to another. For instance, it shows that a user needs to have the permission (p_1) in order to move from the node l_0, which represents the *outside* to the node `L1`, which represents (Building x).

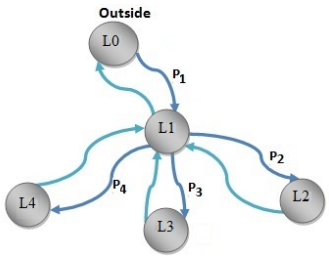

Fig. 3. Location Graph

This location model has sufficient information to deal with the two problems addressed in Secton IV of this paper.

Notation 1: Assume that $LG = (l_0, L, E)$ is the Location Graph as defined in *Definition 1*, we write $\delta = l_1 \xrightarrow{p_1} l_2 \xrightarrow{p_2} l_3 .....l_{k-1} \xrightarrow{p_{k-1}} l_k$ for a path of edges connecting locations, in which p_i represents permissions required to go from the location l_i to l_{i+1}, where $i = 1, 2, 3, ..., k-1$.

B. STRBAC-PS Entities

In this section, we describe the entities of the STRBAC-PS model. Table IV provide a short description of all the entities of the STRBAC-PS model.

1) Impact of Location Graph on Permission Role Acquire `(PRA)`: In order to have physical access to an inner location in a building, for example a room, a person needs to have access into a set of doors and corridors which allows him/her to go through them and ends up in the inner location. There

TABLE IV. STRBAC-PS ENTITIES

STRBAC-PS Entities	Description
Users (U)	a finite set of users, U=$\{u_1, u_2, ..., u_m\}$
Roles (R)	a finite set of roles, R=$\{r_1, r_2, ..., r_k\}$
Permissions (P)	a finite set of permissions, P=$\{p_1, p_2, ..., p_o\}$
Times (T)	a finite set of times, T=$\{t_1, t_2, ..., t_n\}$
User Role Assignment (URA)	a relation that associates users to roles based on the time and location constraints, URA $\subseteq$ U $\times$ R $\times$ T $\times$ L
Permission Role Acquire (PRA)	a relation that associates permissions to roles based on the time and location conditions, PRA $\subseteq$ R $\times$ P $\times$ T $\times$ L
Role Hierarchy (RH)	a transitive partial order on the set of roles, RH $\subseteq$ R $\times$ R $\times$ T $\times$ L
Separation of Duty between Roles (SoDR)	a constraint over roles, which specifies that users should not assign to exclusive roles
Cardinality constraints over Roles (CCR)	a constraint over roles, which specifies the restriction on certain roles which can be assigned to a limited number of users

might be multiple paths to the inner location, but he/she requires to be able to go through at least one of them to reach to the inner location. To formalise this, consider a Location Graph $LG = (l_0, L, E)$ as defined in *Definition 1*. Assume that a role r has the permissions p to access a location l at time t. Then there exists at least one path of the form $l_0 \xrightarrow{p_0} l_1 \xrightarrow{p_1} l_2.....l_k \xrightarrow{p_k} l$, such that the role r has all permissions $p_0, p_1, p_2, ...p_k$. In other words, $\forall i$ $pra(r, p_i, t, l_i)$, where $0 \leq i \leq k-1$.

VI. ANALYSING OF THE RUNNING EXAMPLE USING AC2ALLOY

The most frequent question during modelling of Access Control systems is whether the specification is consistent with functional requirements and compliant with security requirements or not. In order to answer this question, this paper makes use of AC2Alloy [9] to generate an Alloy model from the STRBAC-PS specification and then uses Alloy Analyser to verify the generated Alloy model.

A. Transformation of the Running example into Alloy

The AC2Alloy tool is used to create an Alloy model from the STRBAC-PS specification. When we apply AC2Alloy to the Physical Access Control specification in the context of STRBAC-PS, the specification will be transformed to the XML representation and then the XML representation will be transformed automatically into Alloy code as described in Section II. For sake of conciseness, specifications are omitted. They are available in [10].

B. Model Analysis

To ensure that the Physical Access Control (PAC) system is consistent, several Alloy `checks` will be produced via AC2Alloy. For example, an Alloy `check` will be generated for the cardinality constraint over the role *Cable Engineer* as depicted in Figure 4.

```
check{((L5 in CableEng.node)&&(DayTime
 in CableEng.time)=>(#CableEng.user <3))}
```

Fig. 4. Example of the Transformation of Cardinality Constraints

The execution of the Alloy `check` shows that Alloy Analyser picked up a counterexample as depicted in Figure 5. This means tthat he policy is inconsistent because there are more than two user (Tome, Dave and Sarah) assigned to the role *Cabling Engineer* at the node `L5`, which represents *(street cabinet)* during the *DayTime*, which is not permissible according to the Cardinality constraint.

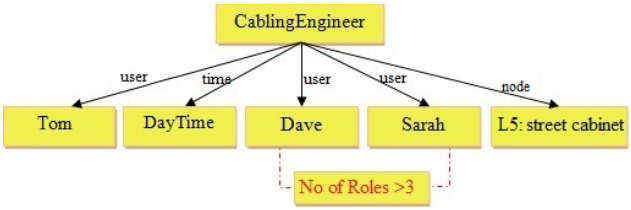

Fig. 5. Counterexample for the Cardinality `check CC1`

VII. CONCLUSION

In this paper, we extend the existing STRBAC model so that it can be used to specify Physical Access Control (PAC) policies. To achieve this, we have introduced the concept of Location Graph to formalise the physical location. The paper also provided a real world example to show the shortcomings of the existing access control models and to highlight the benefits of our new framework. To ensure the consistency of the Physical Access Control (PAC) specification the paper makes use of our previous method, AC2Alloy, to transform the specification into alloy. Finally, it uses an Alloy Analyser to identify any errors in the design.

REFERENCES

[1] Indrakshi Ray and Manachai Toahchoodee. A Spatio-temporal Role-Based Access Control Model. In Proceedings of the 21st Annual IFIPWG11.3Working Conference on Data and Applications Security, pages 211.226, Redondo Beach, CA, July 2007.

[2] Hsing-Chung Chen, Shiuh-Jeng Wang, Jyh-Horng Wen, Yung-Fa Huang, Chung-Wei Chen: A Generalized Temporal and Spatial Role-Based Access Control Model. JNW 5(8): 912-920 (2010).

[3] Arjmand Samuel, Arif Ghafoor, and Elisa Bertino. A Framework for Specification and Verification of Generalized Spatio-Temporal Role Based Access Control Model. Technical report, Purdue University. CERIAS TR 2007-08.

[4] Ray, I., Toahchoodee, M.: A Spatio-Temporal Access Control model supporting delegation for pervasive computing applications. In Proceedings of the 5th International Conference on Trust, Privacy and Security in Digital Business (TrustBus'08). LNCS Springer, Turin (2008).

[5] Jackson.Daniel (2006), Software Abstractions Logic, Language, and Analysis, Cambridge: The MIT Press.

[6] MDA: Model Driven Architecture, Object Management Group (2005), www.omg.org/mda/.

[7] David F. Ferraiolo, D. Richard Kuhn and Ramaswamy Chandramouli. Role Based Access Control. 2nd Edition.2007.

[8] D. H. Akehurst, B. Bordbar, M. J. Evans, W. G. J. Howells, and K. D. McDonald-Maier, "SiTra: Simple Transformations in Java," in ACM/IEEE 9TH International Conference on Model Driven Engineering Languages and Systems, 2006, pp. 351-364.

[9] E. Geepalla, B. Bordbar, and J. Last. Transformation of spatio-temporal role based access control specification to alloy. In Model and Data Engineering (pp. 67-78). Springer Berlin Heidelberg, 2012.

[10] E. Geepalla. "Model-Driven Approaches to Analysing Time- and Location-Dependent Access Control Specifications." PhD Thesis, University of Birmingham, 2013.