



Queensland University of Technology
Brisbane Australia

This is the author's version of a work that was submitted/accepted for publication in the following source:

Skandhakumar, Nimalaprakasan, Salim, Farzad, Reid, Jason F., & Dawson, Edward (2012) Physical access control administration using building information models. *Lecture Notes in Computer Science : Cyberspace Safety and Security, 7672*, pp. 236-250.

This file was downloaded from: <http://eprints.qut.edu.au/53789/>

© Copyright 2012 Springer

This is the author-version of the work.
Conference proceedings published, by Springer Verlag, will be available via SpringerLink. <http://www.springer.de/comp/lncs/>

Notice: *Changes introduced as a result of publishing processes such as copy-editing and formatting may not be reflected in this document. For a definitive version of this work, please refer to the published source:*

http://dx.doi.org/10.1007/978-3-642-35362-8_19

Physical Access Control Administration using Building Information Models

Nimalaprakasan Skandhakumar, Farzad Salim, Jason Reid, and Ed Dawson

Queensland University of Technology, Queensland, Australia
{n.skandhakumar,f.salim,jf.reid,e.dawson}@qut.edu.au

Abstract. Physical access control systems play a central role in the protection of critical infrastructures, where both the provision of timely access and preserving the security of sensitive areas are paramount. In this paper we discuss the shortcomings of existing approaches to the administration of physical access control in complex environments. At the heart of the problem is the current dependency on human administrators to reason about the implications of the provision or the revocation of staff access to an area within these facilities. We demonstrate how utilising Building Information Models (BIMs) and the capabilities they provide, including 3D representation of a facility and path-finding, may reduce the incidents of errors made by security administrators.

1 Introduction

Physical access control is a key element in securing critical infrastructure such as airports, ports, transportation hubs, energy generation plants and military infrastructures [9]. A typical large-scale infrastructure can span across multiple sites with several multi-storey buildings that can host multiple zones with unique security characteristics. Further, there can be several different pathways connecting zones. Of particular interest to physical access control is the fact that there can be normal pathways such as corridors, stairways, and lifts or there can be indirect pathways such as ceiling spaces, partition walls, and ventilation ducts. The scale of the facilities and the spatial relationships and connectivity between the controlled spaces makes the manual administration of access particularly difficult for security administrators [4]. Specifically, it is hard to comprehend the three dimensional nature of the environment through two-dimensional floor plans, which are commonly used by administrators for physical access control configuration and management.

It is not only the scale of these physical facilities that complicates the administration of access control, but the changing culture of these organisations. It is no longer the norm to have all employees at a facility work for the same organisation [21]. Many individual systems and organisational functions are outsourced to external contractors and employees attached to these partner organisations also share the same spaces and resources. This is a dynamic process where the people that require access can change frequently. For example, the heating, ventilation, air conditioning and power management systems can be independently

contracted by different operators, whose staff may need access to various, sometimes highly secure zones in a facility.

There are several shortcomings in the current approaches to physical access control administration tools. The heart of the problem is that they place considerable decision making responsibility on the security administrators. For the purpose of this paper, we conceptually divide administrative requirements that could be facilitated to improve existing physical administrative tools into three categories.

The first requirement is the assignment and revocation of the access to physical spaces. Currently the administrators commonly use two-dimensional floor plans as visual aids to know the spaces, doors, and resources that they need to give access to users. These maps can be digital and part of some of the commercial Physical Access Control Systems (PACS) or simply printed. It is difficult to comprehend the three-dimensional nature of the buildings with multiple floors connected through lifts, stairs and other access paths through two dimensional maps. This is further complicated with the adoption of flexible design practices in many organisations where floor plans change frequently [26]. This can affect the access control process and requires retraining of local knowledge by administrators. The manual process of assignment and revocation of fine-grained access rights in complex environments is therefore challenging in practice. The process of access control administration could be improved with the emergence of 3D modelling tools that can be utilised to improve the user experience of access control tools.

The second key requirement for security operators of critical infrastructures is to comply with least privilege requirements by determining the minimal set of physical resources that staff need in order to perform their tasks. The identification of the minimal set of access permissions demands an analysis of the implications of assignment (or revocation) of permissions to physical resources, e.g., doors, hallways, emergency exits. For example, it is important for security administrators to determine if a user is given access to a resource, what other resources can they access, directly or indirectly? In the case of physical access, if a user is given access to a door, what rooms and spaces can they reach directly through hallways, and indirectly by crawling through air-condition ducts or ceiling spaces?

The third administrative requirement is the ability to monitor and audit of staff access to physical resources. Security audits are becoming particularly important due to regulatory compliance requirements. Access control audits can include various data mining operations on past access records or current access control rules. Audit requirements may be post event or more real-time monitoring to efficiently determine who is currently in an affected area under emergency situations. This can help prioritise first responders to plan and evacuate buildings more effectively.

In recent years, there has been significant interest from industry and the research community into the usability of security technologies [2, 6, 14]. However, published research into the usability of physical access control administration

tools is limited. The human factors affecting physical access control and how the functionalities of administration tools hinder or facilitate the process of security policy creation has been overlooked while the need for effective physical access control has increased [4].

In this paper we introduce a novel tool that utilises Building Information Models (BIM) to facilitate the security administration of physical resources. The use of BIMs has gained increasing acceptance around architecture, engineering, and construction industries during the past years [3]. BIMs provide a shared repository of three-dimensional structured data of physical objects, spatial relationships, and dynamic processes within a building. The process of building information modelling begins from the design phase of the building and evolves throughout the lifecycle of the building potentially capturing a vast amount of static and operational information associated with the building. The use of BIMs in an authorisation tool can make the process more intuitive with three-dimensional visualisation of buildings and enables spatial relationship analysis to be part of the access control process.

2 Motivating Scenario

In this section, we present an example scenario that will be used to illustrate the research problems in the later sections. We consider how an administrator would provide physical access in an airport environment, controlled and operated by multiple stakeholders. An airport employee can belong to any of the partner organisations that operate within the airport. However, their access to shared spaces and systems must be controlled under a single access policy.

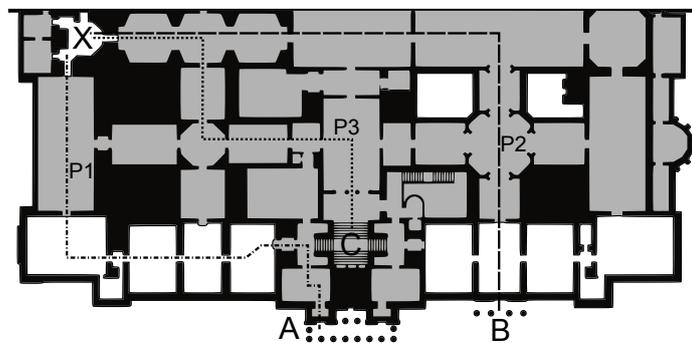


Fig. 1. A two-dimensional floor plan that is typically used to configure physical access control rules

Let us assume there is an emergency repair required in the baggage handling area of the airport, marked by X in Figure 1. In most airports, there will be pre-approved technicians from a contracted company to perform this task.

Ideally, they should be given access only to the space of interest within a limited timeframe and the access rights revoked at the completion of the assigned task. However, in practice these access conditions are not fine grained, enabling most employees to access spaces they need to access even when they are not on duty. The technicians are pre-authorised to access all the areas they need to access to perform their jobs. For example, a lift repair technician will have access to all areas where there are lifts. Furthermore, most of the current access control administration tools rely on 2D maps of the facility to determine the spaces and resources to give access. As shown in the figure, there can be multiple entry points for a facility such as A, B or C (via lift or stairs). For each of these there can be multiple paths passing through different doors that lead to the desired location X. The security administrators must determine the most appropriate path when they are giving access. For a larger facility, the complexity increases with more entry points and path options, and it can become very hard to comprehend with the aid of 2D maps. 2D maps are poor in representing 3D environments with multiple floors connected by stairs, lifts, and ventilation ducts [19]. Furthermore, spatial zones can be dynamic objects in a facility based on the operational conditions. For example, the same set of spaces may be assigned different security levels based on the threat level or in response to an emergency evacuation scenario.

The desirable process for this access control assignment should start from the request to perform a job not as an assignment to individual resources or doors in a physical access control system. The authorisation system should be able to compute the list of resources that should be accessible based on operational needs and the facility's overarching physical security policy. For example, a system policy could say that unaccompanied maintenance contractors should only be given access to doors that have a monitoring CCTV camera fixed. It is also desirable to have pre-defined access patterns for particular resources that comply with system policies. For example, it is possible to pre-define an access path for cleaners to access a particular space within the facility, which can be applied to all users of that class.

3 Related Work

Human-computer interaction is often seen as the weakest link of security in many systems [23]. In practice, many security practitioners consider access control as a task that they perform irregularly and many of them do not have the necessary training [6]. The major motivation behind the current access control tools and systems has been regulatory requirements for accountability and preventive measures [5]. Even widely researched and adopted access control concepts such as Role Based Access Control (RBAC) are in practice hard to grasp for many non-specialist users who are most of the time the end users of these administration tools [7]. It has been widely argued [6, 7] that access control systems and associated administration tools must consider usability as a basic requirement at their design time. In recent years, research into human computer interaction

in security, also known as HCI-SEC [14], has gained much attention. The main motivation behind HCI-SEC is that security and usability must complement each other [2]. It is widely accepted that human errors can be prevented or minimised with changes to the user-interfaces to a system [20]. A better approach to handling human error is to address them at a system level, rather than blaming them on individuals [24]. In general, resource owners are the people with the best knowledge about their access control requirements [11]. However, it is often difficult for these resource owners to express their security needs in computer terms correctly. A formal approach for analysing the correctness of physical access control rules is presented by Fitzgerald et al. [10]. In access control, administrators are expected to express the functional goals as user roles or permissions. It is desirable to express these rules in an intuitive way [16]. This has been the main motivation behind the work being discussed in this paper.

User interfaces that interact with three-dimensional object displays can benefit users of an access control administration tool, which needs to convey the details of the building with multiple dimensions to its users. Such interfaces with three-dimensional displays are suitable for systems that need to identify information with depth [30]. There have been attempts in commercial software products for using building models in policy administration tools for physical security. Some of the recent versions of industry standard physical access control systems provide support for importing CAD files of building and using them as visual interfaces for administration. Our analysis into current commercial tools and associated research show that the available user interfaces are not adequate in addressing these usability requirements behind policy authoring. The SiPass solution from Siemens supports 2D maps that can be imported as AutoCAD files [27]. Gallagher Command Centre (i.e. formally known as Cardax FT Command Interface) includes a comparable visual interface feature with floor maps [13]. The Omnipresence 3D Security Platform [12] provides interface connecting to other systems, including access control systems. However, the functionalities provided by these applications are limited to 2D maps and annotation of spaces. They do not use the spatial information present in building information models to infer spatial relationships which can be used in access control policy creation and management.

Building Information Models (BIM) can be seen as centralised repositories of objects and processes within a building. BIMs are designed from the initial design process of the building, and they evolve throughout the lifecycle of the building. The overall goal of building information modelling is to provide a common repository of semantically rich three-dimensional information that can be used seamlessly and sequentially by all members of the design and construction team, and ultimately by the owner/operator of a facility throughout the facility's life cycle [18]. BIM technology extends into fully integrated 3D and 4D modelling adding the time dimension for scheduling or sequencing for the building design. This process produces the building information model, which incorporates spatial relationships, geographic information, building geometry, and quantities and properties of building components, including the life-cycle

processes of construction and facility operation. The use of building information modelling in this context has gained increasing acceptance around different industries during the past years [29]. Even though other types of data models such as CityGML [15] exist that can be used for buildings, the wider architecture, engineering, construction (AEC) research community, private sector, and governments have adopted building information modelling as the way forward for buildings [3]. BIMs support computational geometry that enables spatial analysis functionalities such as path finding. There are tools to formally analyse BIMs in the Industry Foundation Classes (IFC) format for integrity, quality and physical safety [8], thus ensuring desirable outcomes for spatial analysis functions. BIMs are used in emergency response, evacuation, and recovery scenarios to support indoor navigation with path finding capabilities and to provide important building information with spatial context to emergency responders and rescuers [25]. Some of these existing functionalities also have security and access control implications. For example, in the event of an emergency evacuation security privileges and physical access policies can change based on the affected areas. This requires an authorisation framework that can support creating pre-meditated access policy.

4 Using BIMs for Access Administration

In this section, we present an access control administration tool that we have developed as part of our research into utilising BIMs for access management in large scale facilities. This prototype implementation addresses the three main physical access control administration problems we have identified earlier: intuitively creating physical access control policies, conveniently managing physical access control systems, and effectively auditing physical access control logs.

The core of this administration tool is based on the concepts of our authorisation framework using building information model that we previously presented in [28]. The authorisation framework utilises BIMs in three key stages of access control: policy design, policy management and decision making. As shown in Figure 2 each of these processes are captured by a unique component in the authorisation framework. We provide a brief overview of this framework in the following paragraph.

The BIM layer consists of BIMs that are loaded into a model server. These BIM files originate from multiple stakeholders of the facility that are converged into one BIM in the model server. The spatial reasoning module provides the spatial reasoning functions required for the authorisation framework. This includes different spatial functions such as locating access doors to a space, reachability analysis based a specified starting and ending points, or obtaining the list of resources contained within a given space. The visualisation engine will generate 3D and 2D representations of BIM data to be used by different processes of the authorisation framework such as spatial reasoning and policy transformation. The authorisation layer of this framework adopts the formalised XACML architecture [22]. It adds spatial capabilities through the extension points sup-

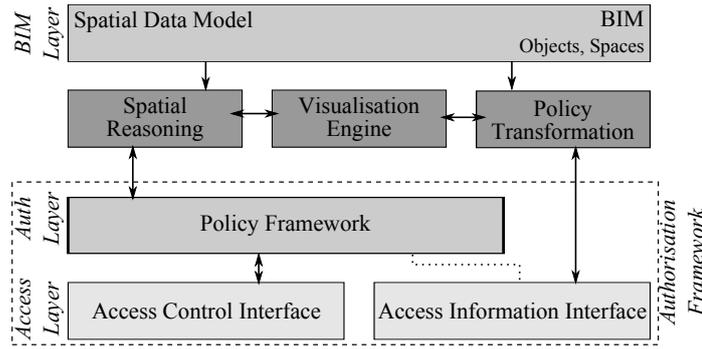


Fig. 2. Architecture of an authorisation framework using building information models

ported by the XACML standard. The access layer of this framework provides access control decision-making capabilities to external systems via the Access Control Interface. It also enables external systems that have their own authorisation decision-making capabilities to utilise the framework functionalities via the Access Information Interface.

The authorisation model is designed to support a converged approach towards physical and logical access control. In this paper we will only focus on our proposed tool for administering physical access control. The BIM layer provides the base for the implementation by providing the spatial data model for representing resources and computing spatial functions. We have also implemented the visualisation, spatial reasoning, and policy transformation components as part of this prototype. These components can be interfaced to an external physical access control system through the access information interface; however it is not part of the current version of the tool.

This prototype is developed as a client-server application that can be accessed through any modern web browser that supports OpenGL. The authorisation framework is modelled into an Eclipse Modelling Framework, in conjunction with a BIM engine that is based on the same technology. The meta-model shown in Figure 3 is the foundation for our prototype implementation. We take an approach similar to [17], by combining attribute and role based access control. The user model represents the generic role based policy specification. It is connected to the more descriptive policy model through the assignment class. Resources are objects contained in the building information model. A specific instance of an object can be accessed via its globally unique identifier (GUID). In this implementation, we are only using the object types of Zones, Spaces, and Doors. Conditions include any relationships or constraints, including time or binary exclusions. For example, binary exclusion would allow a user access to only one of the two specified spaces to satisfy separation of duty constraints. We use the XACML data model [22] at policy level. The meta-model policies are transformed and mapped into the basic XACML policy elements such as subject, resource, action, and condition.

The main user interface for the prototype loads within a browser window with multiple tab panels (see Figure 4). The search and results panels are shared to

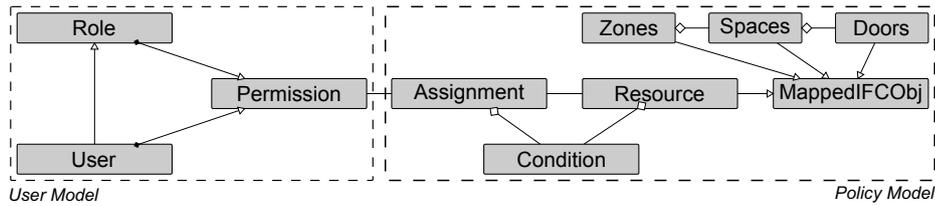


Fig. 3. Simplified meta-model diagram for the implementation of the physical access control administration tool

enable a consistent experience across different modes of operation. The visualisation panel loads BIM objects and other conditions are superimposed on the same rendered model. This also has the option to switch between 2D and 3D representations of the visualisation. In the following sections we discuss the functionalities of our prototype. We also discuss how they address each of the three main physical access control administration problems identified earlier.

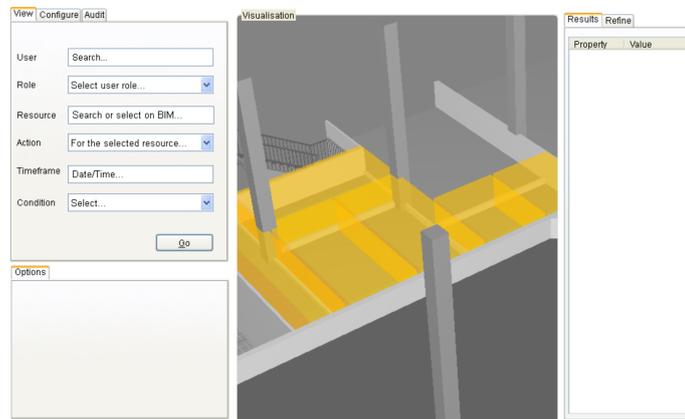


Fig. 4. Browser based user interface for access control administration with 3D visualisation window

4.1 Create Access Control Rules from BIM Visualisation

The configuration mode of the prototype can be used in creating access control policies that would be used in the authorisation framework. Administrators can visually select a target resource from BIM that the users need to be given access. This three-dimensional interface can be more intuitive for administrators as the required prior knowledge is minimised. For example, an administrator can select a particular space from the BIM visualisation and assign it to users or roles. The configuration mode of the prototype utilises the following functionalities of the tool:

Manage Users: Users can be assigned to one or more roles. Both users and roles can have resource assignments and conditions.

Manage Resources: Rooms and hallways in a building are mapped as individual spaces. These spaces can be grouped into the logical relationship of zones. Each of the individual spaces can have multiple accessible door objects. Access assignments can happen at all three of these object levels.

Identify Paths: An important spatial functionality of this tool is the ability to determine all potential paths to a destination. It maps physical spaces from the BIM into a graph with doors as weighted nodes connecting them based on the security criteria. The administrator can specify the conditions that must be satisfied. Some of these conditions include, shortest path, the path that goes through CCTV camera monitoring, the paths that are currently least crowded, or those that require the minimum security clearances. These additional conditions are also attached to the graph links. The path finding functionality uses graph traversal to identify optimal paths for a given criteria.

Define Conditions: This tool supports the definition of different types of conditions that can govern the access policies. Logical inclusions and exclusions of resources from assignments are allowed with different Boolean operators. For example, a particular space can be excluded from an assignment when a corresponding user or role has access to another specific space. This can be a powerful feature in applying separation of duty constraints. Each of these conditions can be time limited based on fixed times or relative times.

Assign Access Rules: Those access conditions with corresponding resources can be assigned for users or roles as access permissions. This permission-assignment relationship provides the connectivity between the user model and the policy model in the meta-model shown in Figure 3.

Alert on Inconsistencies: The tool has the feature of checking across existing policy rules when creating a new rule. This alerts the administrators of any potential inconsistencies across existing rules and new rules. For example, when a new resource assignment violates an exclusion condition this can alert the administrator to change policy rules or to remove the assignment.

Propagate Access Rights: Once access policy rules are defined they can be propagated to enforcement-level objects. For example, in physical access control systems, a policy rule for accessing a space can be transformed into multiple door access rules that can be uploaded to door lock controllers.

Figure 5 shows how administrators can use the tool to automatically calculate all the spaces that they need to give access in order to reach a given space from a starting point. They can additionally refine these with actions and conditions associated with the resource. There can also be other separation of duty and least privilege constraints applied to these conditions. The tool would then generate the access control policy rules comprising the Subject, Object, Action and Condition elements that can be mapped into an XACML policy. These rules can again be transformed into low-level enforcement policies for a PACS that controls individual doors based on the GUID properties of the doors computed through space containment relationships. We note that some rules with complex

conditions may not be supported depending on the capabilities of the PACS. The same policy can be transformed into the proprietary formats supported by different PACSs from different vendors. The reverse of the same transformations can be used to manage policies from different systems in a single tool.

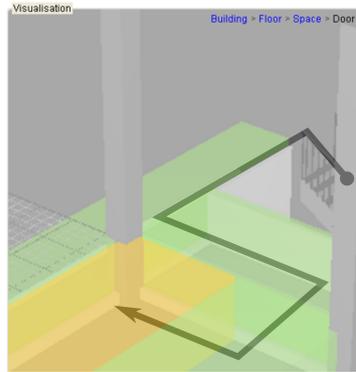


Fig. 5. Path calculated from external starting point to the selected space

Let us see how this can be applied in the example scenario presented earlier. The end point can be selected as the room shown in yellow on Figure 5 where the maintenance task needs to be carried out. The starting point could be any of the external gates through which the technician can enter the airport. There can be multiple paths to this particular room passing through different spaces. In the current access control systems, this access knowledge will depend on the expertise of the security administrator. Using this tool, the administrator can calculate different path options with different criteria such as lowest security clearance or shortest distance, and the system can identify the best path option. This path option can then be translated into a list of spaces or portals that need to be given access. The tool can also automatically alert the administrator if the only available path requires a higher clearance level than a maintenance technician can have, for which alternative arrangements, such as an escort, can be made.

4.2 Visualise and Analyse Access Control Rules using BIMs

One of the prominent problems in current access control administration tools is the difficulty in reporting the current access privileges for a user or a role. Even though they provide textual lists of user/role privileges, these lists can be long, making it difficult for administrators to relate the privileges to the spaces they make accessible within a large facility. To address this requirement, the prototype enables administrators to visualise, as accessible spaces, the privileges possessed by a user or role (Figure 6).

Search Access Control Policy: Administrators can perform various search queries on a policy and refine the search results by users, roles, conditions, etc. The refined policy rules can also be edited within the tool.

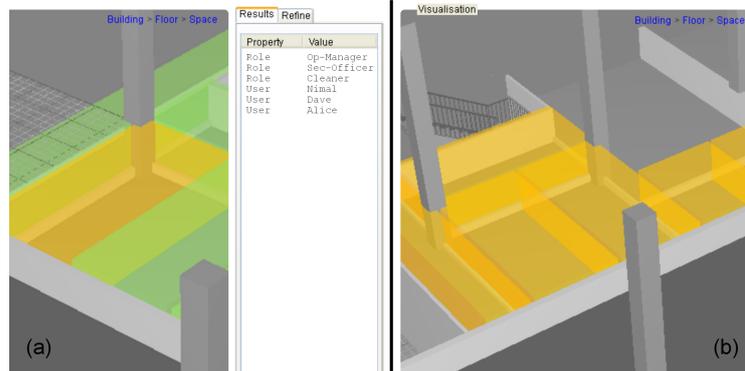


Fig. 6. Managing physical access through visualisation: (a) List users that can access the selected space, (b) Show spaces the selected user can access.

Visualise Access Control Policy: Selected policy set can be visually overlaid on BIM visualisation. For example, all policy sets corresponding to a role can be visually overlaid to show users/roles that have access to a selected space (shown in yellow on Figure 6a) or to show the spaces and zones the role can access (shown in yellow on Figure 6b). This also allows one to edit the specific policy sets from the visualisation.

Analyse Access Control Policy: The tool can analyse the loaded access policy against existing conditions to find inconsistencies and violations. This can be useful when auditing sets of existing rules from an external physical access control system that are loaded into the authorisation framework. For example, administrators can view all the spaces that are accessible by a user at normal times or under emergency conditions. These spaces can be highlighted on a visualisation of the building.

Security administrators can load existing access control policies for particular users or roles and visualise the spaces they can access. This search functionality can be further narrowed down with additional conditions and timeframes, which can be used for scenario planning and analysis. The use of BIMs to represent the relationships between objects presents another interesting functionality where analysis can be performed on given access rights and inconsistencies can be identified at a policy level.

4.3 Access Control Audit and Analysis using BIMs

The audit mode of this tool can be used on physical access control logs in conjunction with BIMs. In this mode of operation administrators can visualise past access logs superimposed as access paths (Figure 5) or aggregated spaces (Figure 6b) on a BIM visualisation. The following functionalities of the prototype implementation are utilised in this mode of operation.

Access Log: The access log is a simple implementation of past access records. The log entries are assumed to be imported from an external physical access control system. The minimal entities for each access log are a timestamp, a user ID and a resource ID. The resource ID corresponds to the GUID of a door in the meta-model.

Generate Access Path: This tool can generate access paths for each user based on the log entries by connecting the relevant doors. This connected path can be visually overlaid on a BIM along with the policy rules for the corresponding user.

Analyse Access Log: The analysis functionality takes access log entries and compares it with existing policy rules. This can be useful in identifying any short-coming in the enforcement arrangement such as tailgating or reversed doors.

These functionalities are used to implement the access control audit requirements. The access logs can be searched to narrow down accesses by a particular user or to a given space within a given timeframe. BIMs can be used as both visualisation front ends and to provide the base for spatial analysis for access audits. In case of physical access logs, they can be used to generate the access path for a given user within a given time, using the list of doors accessed. This can be visually overlaid on a BIM visualisation as a tentative path connecting these doors. This capability can be used by administrators as a post event analysis tool and can be extended to provide monitoring for path deviations and access errors. For example, we can show access errors for a selected user and which doors they have tried to access for which they do not hold access privilege. The user logs can also be aggregated and visualised as set of spaces and zones instead of individual paths. For example, administrators can select a user or a role and visually compare the spaces they can access from the policy and the spaces they have used in the past from the logs. This can be useful in identifying redundant access privileges that accumulate over time. The same access audits can also be used in other operational analysis such as time spent by a user in a given space. For example, assuming egress is also controlled, it is possible to extract the length of time a maintenance technician spends in a given space and compare it with their job assignments.

5 Future Work

Our current work opens up multiple avenues for future research. This paper was based on an assumption that it is easier for security administrators to work with 3D representation of facilities, than to use the existing two-dimensional floor plans. However, the validity of this assumption as well as the usability of the proposed tool are yet to be evaluated. We would also like to investigate how to extend the proposed tool such that it supports converged access control, to enable the control of access to information systems as well as physical resources. Finally, we would like to investigate how to interface the proposed tool with open standard communication protocols for building automation and control networks such as BACNet [1].

6 Conclusion

Physical access control administration in large-scale facilities is a difficult task. Administrators should be able to easily comprehend the complex nature of their environments in order to make informed access control policy decisions. However currently available physical access control administration tools do not consider usability as a key requirement. We proposed a physical access control mechanism that facilitates visual access control administration using building information models. We based our access control framework on the basic concepts of role-based access control and other well-defined security constructs to ensure a solid formal grounding for the concepts presented in this paper. The main advantage of the proposed approach is that it can reduce dependency on expert knowledge and provide decision-making capabilities in performing security administrative tasks. This is primarily achieved through providing a 3D visualisation of a facility, path finding functionality and identification of potential inconsistencies within a policy rule set.

Acknowledgements: This research forms part of the work undertaken by the project *Airports of the Future* (LP0990135) which is funded by the Australian Research Council Linkage Project scheme. The authors acknowledge the contributions made by the many aviation industry stakeholders involved in this project. We would also like to thank Mr. Joerg Kirgeland for his work on implementing the prototype discussed in this paper. Professor Robin Drogemuller deserves special mention for his valuable comments and for providing the building information models. More details on *Airports of the Future* project and its participants is available at <http://www.airportsofthefuture.qut.edu.au>.

References

1. ASHRAE SSPC 135: BACnet - a data communication protocol for building automation and control networks (2012) Online, Available from: <http://www.bacnet.org/>.
2. Balfanz, D., Durfee, G., Grinter, R.E., Smetters, D.K.: In search of usable security: Five lessons from the field. *IEEE Security and Privacy* **2**(5) (September 2004) 19–24
3. Baty, J.: The rise of BIM. *Concrete Contractor* **12**(1) (2012) 34–37
4. Bauer, L., Cranor, L.F., Reeder, R.W., Reiter, M.K., Vania, K.: Real life challenges in access-control management. In: Proceedings of the 27th international conference on Human factors in computing systems. CHI '09, New York, NY, USA, ACM (2009) 899–908
5. Beal, B.: IT security: the product vendor landscape. *Network Security* **2005**(5) (2005) 9–10
6. Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson, L., Fels, S., Fisher, B.: Towards understanding it security professionals and their tools. In: Proceedings of the 3rd symposium on Usable privacy and security. SOUPS '07, New York, NY, USA, ACM (2007) 100–111

7. Brostoff, S., Sasse, M.A., Chadwick, D., Cunningham, J., Mbanaso, U., Otenko, S.: 'R-What?' Development of a role-based access control policy-writing tool for e-Scientists: Research Articles. *Software: Practice and Experience* **35**(9) (July 2005) 835–856
8. Eastman, C., min Lee, J., suk Jeong, Y., kook Lee, J.: Automatic rule-based checking of building designs. *Automation in Construction* **18**(8) (2009) 1011 – 1033
9. Fernandez, E.B., Ballesteros, J., Desouza-Doucet, A.C., Larrondo-Petrie, M.M.: Security patterns for physical access control systems. In: *Proceedings of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, Berlin, Heidelberg, Germany, Springer-Verlag (2007) 259–274
10. Fitzgerald, W.M., Turkmen, F., Foley, S.N., O'Sullivan, B.: Anomaly analysis for physical access control security configuration. In: *Proceedings of the 7th International Conference on Risks and Security of Internet and Systems*. (2012)
11. Flechais, I., Mascolo, C., Sasse, M.A.: Integrating security and usability into the requirements and design process. *International Journal of Electronic Security and Digital Forensics* **1**(1) (May 2007) 12–26
12. Fortem Inc.: Omnipresence 3D Central Command (2012) Online, Available from: <http://www.fortem.com/index.php?page=central-command>.
13. Gallagher Group Ltd.: Gallagher Command Centre (2012) Online, Available from: <http://security.gallagher.co/products/gallagher-products/command-centre-core-features/>.
14. Garfinkel, S.L.: Design principles and patterns for computer systems that are simultaneously secure and usable. PhD thesis (2005)
15. Grger, G., H. Kolbe, T., Nagel, C., Hfele, K.H.: OGC City Geography Markup Language (CityGML) Encoding Standard. Technical Report OGC 12-019, Open Geospatial Consortium Inc (2012)
16. Inglesant, P., Sasse, M.A., Chadwick, D., Shi, L.L.: Expressions of expertness: the virtuous circle of natural language for access control policy specification. In: *Proceedings of the 4th symposium on Usable privacy and security*. SOUPS '08, New York, NY, USA, ACM (2008) 77–88
17. Kuhn, D.R., Coyne, E.J., Weil, T.R.: Adding attributes to role-based access control. *Computer* **43**(6) (June 2010) 79–81
18. Liebich, T., Adachi, Y., Forester, J., Hyvarinen, J., Karstila, K., Reed, K., Richter, S., Wix, J.: buildingSMART: Industry Foundation Classes, IFC2x Edition 4 Release Candidate 2 (August 2010) Online, Available from: <http://buildingSMART-tech.org/>.
19. Mandloi, D., Thill, J.C.: Object-oriented data modeling of an indoor/outdoor urban transportation network and route planning analysis. In Jiang, B., Yao, X., eds.: *Geospatial Analysis and Modelling of Urban Structure and Dynamics*. Volume 99 of GeoJournal Library. Springer Netherlands (2010) 197–220
20. Maxon, R.A., Reeder, R.W.: Improving user-interface dependability through mitigation of human error. *International Journal of Human-Computer Studies* **63**(1-2) (July 2005) 25–50
21. Minnick, D., Ireland, R.: Inside the new organization: a blueprint for surviving restructuring, downsizing, acquisitions and outsourcing. *Journal of Business Strategy* **26**(1) (2005) 18–25
22. Moses, T.: eXtensible Access Control Markup Language (XACML) Version 2.0. OASIS Standard. Technical report, OASIS Open (February 2005)

23. Patrick, A.S., Long, A.C., Flinn, S.: HCI and security systems. In: CHI '03 extended abstracts on Human factors in computing systems. CHI EA '03, New York, NY, USA, ACM (2003) 1056–1057
24. Reason, J.: Human error: models and management. *BMJ* **320**(7237) (March 2000) 768–770
25. Rueppel, U., Stuebbe, K.M.: BIM-based indoor-emergency-navigation-system for complex buildings. *Tsinghua Science & Technology* **13**(1) (2008) 362–367
26. Shuchi, S., Drogemuller, R., Kleinschmidt, T.: Flexible airport terminal design : towards a framework. In TANG, L.C., Watson, G.H., eds.: Proceedings of the IIE Asian Conference 2012, Singapore, Department of Industrial & Systems Engineering, NUS (June 2012) 348–356
27. Siemens Building Technologies Group: SiPass Integrated (2012) Online, Available from: <http://www.siemens.com.au/security-access-manage>.
28. Skandhakumar, N., Reid, J., Dawson, E., Drogemuller, R., Salim, F.: An authorization framework using building information models. *The Computer Journal* **55**(10) (2012) 1244–1264
29. Succar, B.: Building information modelling framework: A research and delivery foundation for industry stakeholders. *Automation in Construction* **18**(3) (2009) 357 – 375
30. Tavanti, M., Lind, M.: 2D vs 3D, implications on spatial memory. In: Proceedings of the 2001 IEEE Symposium on Information Visualization. INFOVIS '01, Washington, DC, USA, IEEE Computer Society (2001) 139–145