Topology-Aware Access Control of Smart Spaces

Journal Item

How to cite:

Pasquale, Liliana; Ghezzi, Carlo; Pasi, Edoardo; Tsigkanos, Christos; Boubekeur, Menouer; Florentino-Liano, Blanca; Hadzic, Tarik and Nuseibeh, Bashar (2017). Topology-Aware Access Control of Smart Spaces. IEEE Computer, 50(7) pp. 54–63.

Link(s) to article on publisher's website:
http://dx.doi.org/doi:10.1109/MC.2017.189

Topology-Aware Access Control of Smart Spaces

Topology Aware Access Control of Smart Spaces

Liliana Pasquale[1,2], Carlo Ghezzi[3], Edoardo Pasi[3], Christos Tsigkanos[3], Menouer Boubekeur[4], Blanca Florentino-Liano[4], Tarik Hadzic[4], Bashar Nuseibeh[2,5]

[1]University College Dublin, Ireland.

[2]Lero - The Irish Software Research Centre, Ireland.

[3]Politecnico di Milano, Italy

[4]United Technology Research Center, Ireland

[5]Department of Computing and Communications, The Open University, UK

Abstract: The proliferation of smart spaces, such as smart buildings, is increasing security vulnerabilities arising from the interplay between cyber and physical entities. We proposed that a representation of the topology of cyber and physical spaces may provide security-relevant contextual characteristics and support the verification of security requirements. We also developed a tool that enables editing and visualising of security-relevant topological characteristics of a building, and verifying that access control policies satisfy security requirements. In this article we report on our experience of applying our approach and the tool to solve practical physical access control problems, and provide some lessons learned for researchers and practitioners.

Keywords: access control, security, verification, smart buildings.

Introduction

Access control provides the capability to manage the access of groups of users to particular assets. In practice, access control is difficult to manage within large organisations[1], as each employee must be granted the exact level of access she needs depending on her role. This difficulty may be exacerbated when the roles covered by an employee vary frequently; within large organisations this can happen every three months[2]. Despite the substantial research literature and high-profile security products, security analysts still have no means to verify whether existing access control policies grant the exact access level that employees need. Moreover, many organisations fall short of implementing the correct access control policies. For example, 50 to 90 percent of employees are over-entitled in large organisations[2], increasing opportunities for insiders to cause harm.

In previous work[3] we argued that a representation of the *topology* of cyber and physical spaces, representing their key structure and relationships, can provide security-relevant contextual characteristics, such as where assets are placed and how security controls should be enacted. For example, the topology of a physical space can capture the layout of a building including its structural relationships, such as containment (e.g., a building contains rooms), and connectivity (e.g., two rooms are connected through a door). Similarly, the topology of a cyber space can capture the configuration of the network and the digital devices within the building, also including relationships such as containment (e.g., a file is stored in a device) and connectivity (e.g., two digital devices are connected through the network). We also proposed the use of a meta-calculus[4] to represent the topology of both cyber and physical spaces and its dynamics, and utilised such a composite model to reason about the consequences of the evolution of topological configurations on the satisfaction of security requirements through model checking.

To support access control of smart spaces we apply and extend our work, focusing on the representation of the topology of a smart building and on the verification of access control policies. We developed a tool to enable security analysts to visualise and edit topological characteristics of a building and verify whether access control policies satisfy security requirements expressed on reachability relationships (e.g., whether an agent can reach specific assets or building areas). If the verification fails, the tool provides explanations on how existing credentials should be revised in terms of the current topological configuration of the space. To ensure wider applicability of our approach, our representation of a building topology - hereafter referred to as *BIM-Sec* - complies with an existing industry standard, the Building Information Model (BIM)[5].

In this article we focus on physical access control. We describe our experience of applying our tool to a set of practical physical access control scenarios provided by security analysts. Our contribution shows how a system founded on software engineering principles, such as interactive development, visual abstraction, formal modelling, and requirements specification, can be applied to support security analysts in the design of physical access control policies.

BIM-Sec

BIM and Computer Aided Design (CAD) software for architects enables representing structural and functional characteristics of buildings. Industry Foundation Classes (IFC)[6] has become the de-facto standard format for exchanging BIM models in the construction industry. Despite its widespread adoption, BIM is not expressive enough to represent security-relevant characteristics of a building. For example, BIM models do not include a representation of cyber and physical assets and access control policies. Moreover, the graphical tools adopted to create and modify BIM models, such as Revit[7], do not support security analysis. BIM is also perceived as overly expressive and heavyweight for security analysts: detailed structural properties that might be relevant for architects are often irrelevant for the definition of access control policies.

So, we defined BIM-Sec (Figure 1), a lightweight version of the IFC meta-model that also includes entities that were identified as security-relevant by access control practitioners. Entities supported in IFC are represented in grey. Some intermediate relationships between IFC entities are omitted to simplify the figure.

A building is represented as a collection of rooms, with each room represented as an *IfcProduct* element labelled with a name and an identifier inherited from *IfcSpace*. A room can also contain other building structural elements (e.g., walls, furniture) as described by the relationship *ContainsElement* brought by *IfcSpace*. Each room can be bounded by walls (*IfcWall*), which in turn can

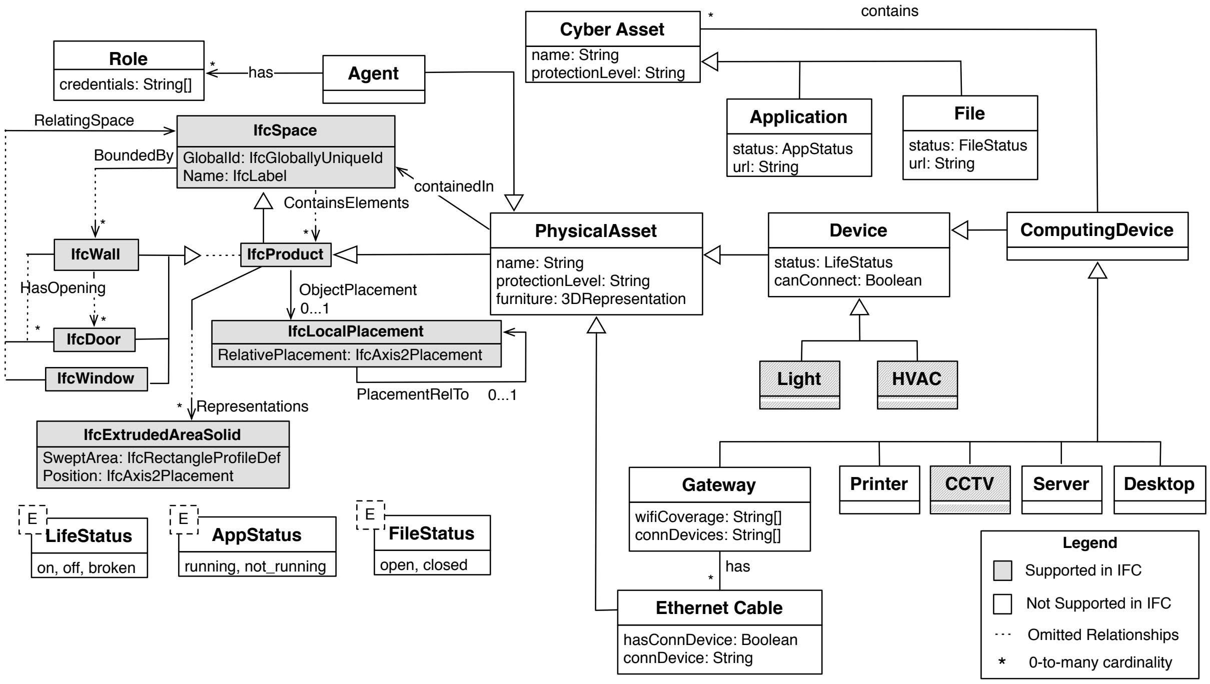


Figure 1. BIM-Sec Meta-Model.

have opening points, each of which indicates the presence of a door (*IfcDoor*) or a window (*IfcWindow*). A door or a window may enable connectivity of a room to another room, as indicated by the *RelatingSpace* relationship. A building structural element (*IfcProduct*) is also characterised by its location (*ObjectPlacement* relationship). In particular, *IfcLocalPlacement* defines the relative placement of an element in relation to the placement of other spaces that may contain it (*PlacementRelTo* relationship). Each building structural element can also be associated with a set of graphical representations. Each room has a shape described by the *SweptArea* property of the *IfcExtrudedAreaSolid* entity.

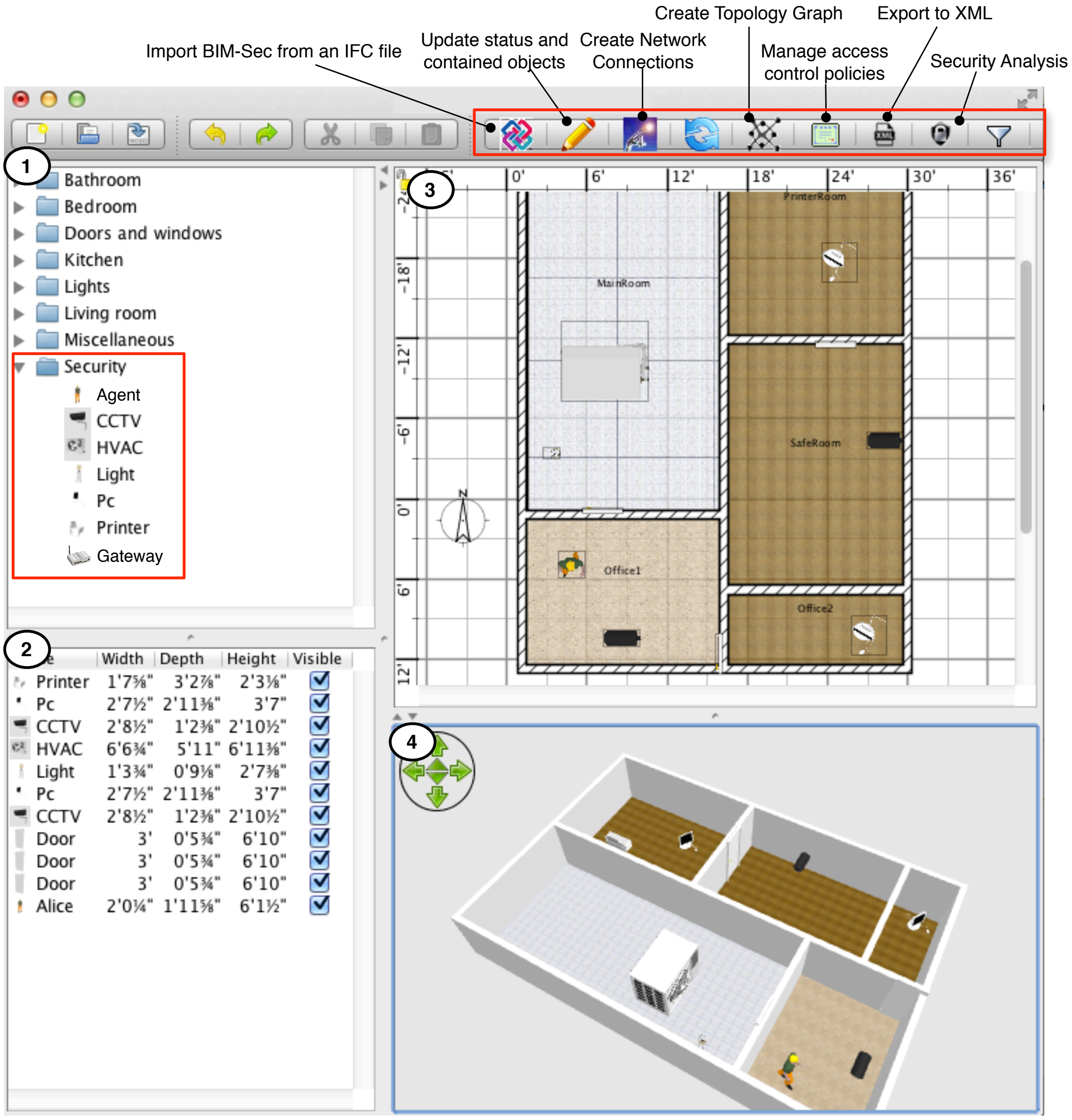
BIM-Sec includes additional physical and cyber entities that are not fully supported in IFC. In particular, we extend *IfcProduct* to also represent a *PhysicalAsset*. *Agents* are a particular kind of physical assets that can traverse the building depending on its structural properties. Note that agents differ from the *IfcActor* element supported by the IFC standard, as the latter is intended to represent different stakeholders involved in the construction project of a building. Access control policies are expressed according to the Role-Based Access Control[8] (RBAC) model by associating each agent with a set of *Role*s. A role is in turn associated with a set of *credentials*, i.e. a list of physical areas and assets that role grants access to. An alternative model is Attribute-Based Access Control (ABAC)[9] model, according to which authorisation to perform a set of operations is determined by evaluating attributes associated with the subject, object, and requested operations. Although ABAC would allow defining more dynamic access control policies (e.g., blocking access temporarily), we used RBAC since it is the most widely used access control model in practice.

Both agents and physical assets can be contained in a physical space; this can be indicated by the *containedIn* relationship, which is explicitly defined for the physical assets that were not originally included in the IFC meta-model.

A physical asset can also represent a *Device*, such as a *Light* or an *HVAC* (a *Heating, Ventilation, Air Conditioning* unit). Devices can connect to other ones and are characterised by a *status* (*on*, *off*, *broken*). Lights are security-relevant because, for example, their malfunctioning may allow an offender to access a valuable asset unnoticed. HVACs are security-relevant because their malfunctioning may compromise the integrity of data centres and other critical equipment co-located in the same area and requiring a specific target temperature to function properly. Note that although the IFC standard supports the representation of an HVAC (*IfcHvacDomain* element), it does not allow the representation of its current status and network connectivity.

We also specify *ComputingDevices* that can contain *CyberAssets*, such as *Files* or *Application*s. A computing device is security-relevant since confidential files or critical applications they contain can be accessed directly or from other devices connected to it. Moreover, representing the *status* of files (open or not) allows the detection of whether agents - who are co-located in the physical space with the device in which the file is stored - can see it breaching its confidentiality.

Gateways and *Ethernet Cables* enable network connectivity and allow accessibility to the devices connected. Representing network connectivity is particularly relevant in building



e	Width	Depth	Height	Visible
Printer	1'7⅝"	3'2⅞"	2'3⅛"	☑
Pc	2'7½"	2'11⅜"	3'7"	☑
CCTV	2'8½"	1'2⅜"	2'10½"	☑
HVAC	6'6¾"	5'11"	6'11⅜"	☑
Light	1'3¾"	0'9⅛"	2'7⅜"	☑
Pc	2'7½"	2'11⅜"	3'7"	☑
CCTV	2'8½"	1'2⅜"	2'10½"	☑
Door	3'	0'5¾"	6'10"	☑
Door	3'	0'5¾"	6'10"	☑
Door	3'	0'5¾"	6'10"	☑
Alice	2'0¼"	1'11⅝"	6'1½"	☑

Figure 2. Graphical interface of our tool; extended functionalities are indicated in red.

automation systems, for which network protocols, such as KNX[10], do not include security features. For example, passwords employed to authenticate valid commands may be sent in clear text on the network, thus allowing key sniffing. For the gateway, we also represent the network cables connected to its ports and the rooms covered by the WiFi signal. For each network cable we identify the devices connected to it. For the sake of this running example, we assume wireless connectivity covers the whole floor.

Topology Aware Access Control

Our topology aware access control tool (https://www.youtube.com/watch?v=zuLumnbv5w0) provides security analysts with a graphical user interface to import, modify and analyse smart buildings. It extends SweetHome3D (http://www.sweethome3d.com), an open source software application for drawing the plan of a house, arrange furniture and visualise the results in 3D.

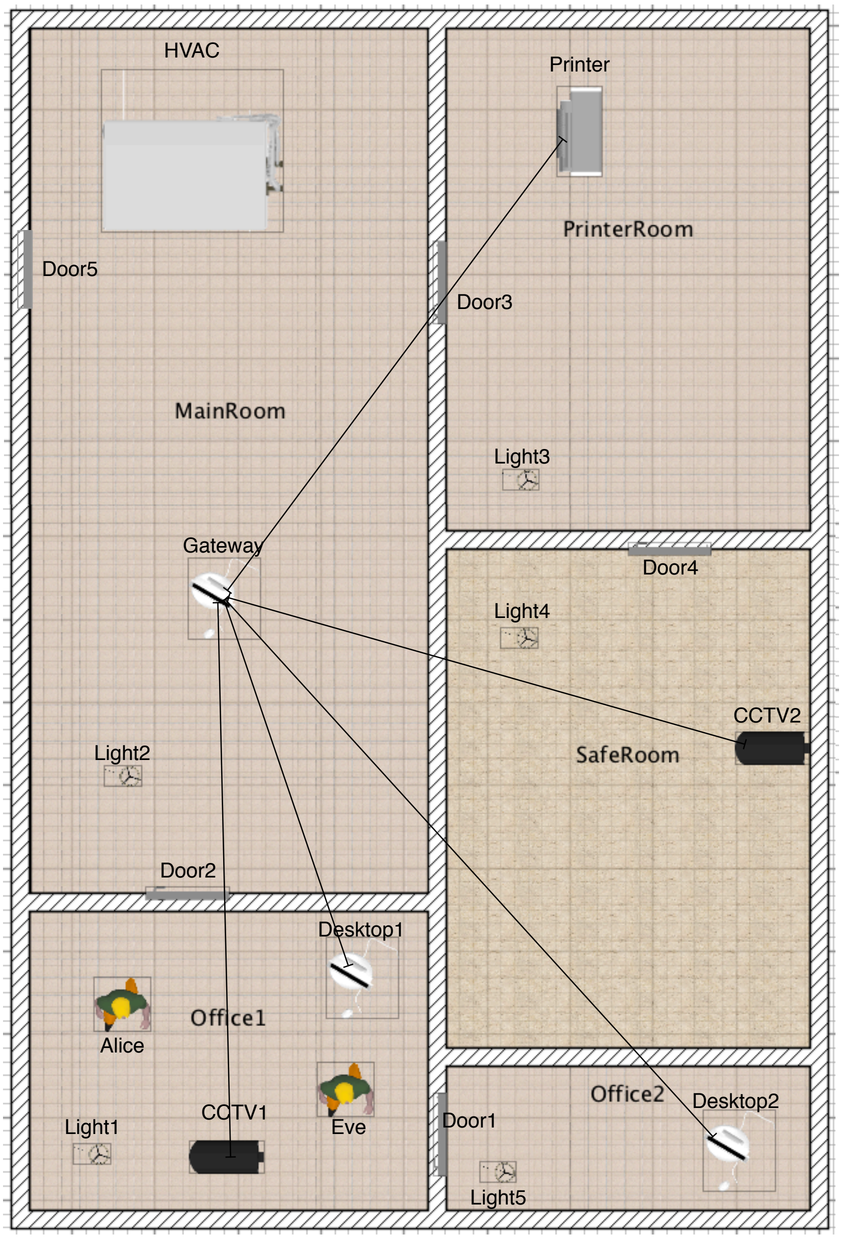


Figure 3. Floor map of our usage scenario.

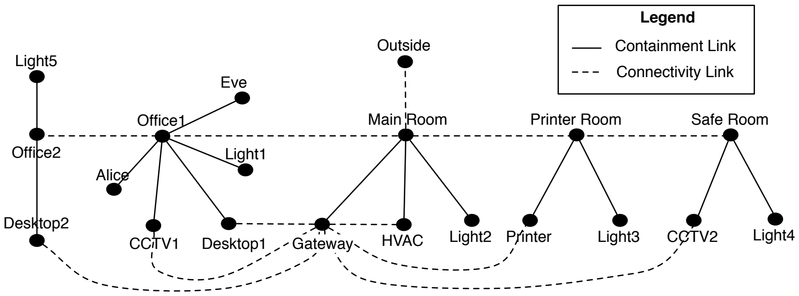


Figure 4. Graph associated with the building topology of our example.

A screenshot of the graphical interface of our tool is shown in Figure 2. From the first area of the GUI it is possible to import 3D representations of entities and edit their attributes as shown in the second area. In the third area it is possible to visualise the 2D plan of the building, while the fourth area provides a 3D rendering of the defined building.

As shown at the top of Figure 2, security analysts can import an IFC file and edit its corresponding BIM-Sec representation, which is maintained and modified locally. In particular, our tool extracts only those entities and properties that are security-relevant and ignores objects characterising complex architectural properties or other furniture elements. Security analysts can enrich a BIM-Sec model by updating assets' status and contained cyber assets, identifying network connectivity between two devices, and specifying access control policies. Security analysts can also export the modified BIM-Sec model into a textual format (e.g., XML) to support portability to existing access control systems, as well as external applications which might leverage the building model to verify other non-security requirements, such as energy efficiency, and safety.

To support security analysis our tool generates a graph representing the topology of the cyber and physical space from a BIM-sec model. Each node of the graph can represent a room (i.e. instance of the *IfcProduct* class representing a building area), or an asset. The links of the graph are annotated with their type expressing the nature of the relation. A *connectivity* link between two rooms indicates physical connectivity; it is created if the rooms are connected through a door or a window. A *connectivity* link between two devices indicates network connectivity. A *containment* link indicates a containment relationship; it is created between a room and the physical assets it contains or between a digital device and the cyber assets it contains. We assume the graph generated is always connected.

Security requirements to be analysed are expressed as reachability properties (e.g., all employees having a specific role cannot reach an asset or a room). These requirements are verified by traversing the graph. We apply the breadth-first search algorithm, whose complexity is linear; this ensures scalability in practical settings.

Note that our tool presents some limitations related to the parsing of IFC files. We only support rooms defined as rectangular shapes in the IFC standard. Finally, our IFC parser was tested for simple building plans having just one floor; in future work we will consider buildings having many floors connected through stairs and elevators.

Usage Scenarios

In this section we demonstrate the broader applicability of our approach by describing a set of possible usage scenarios, as indicated by practical needs of access control practitioners. Although scenarios presented here are rather simple, the sheer size of the underlying models in practical settings can make manual evaluation unfeasible even for simple requirements.

A map of the building that was imported from an existing IFC file and further edited for our scenarios is shown in Figure 3. The building includes five rooms: *Office1*, *Office2*, *MainRoom*, *SafeRoom*, and *PrinterRoom*. Each room can contain security relevant entities; for example the *PrinterRoom* contains a *Printer*, while the *MainRoom* contains an *HVAC* and a *Gateway*, whose wireless signal covers all rooms in the building. *Office1* and *Office2* contain *Desktop1* and *Desktop2*, respectively. Agents *Alice* and *Eve* are in *Office1*. Existing network connections are also shown as continuous lines connecting different devices in Figure 3. The graph representing the building topology is shown in Figure 4.

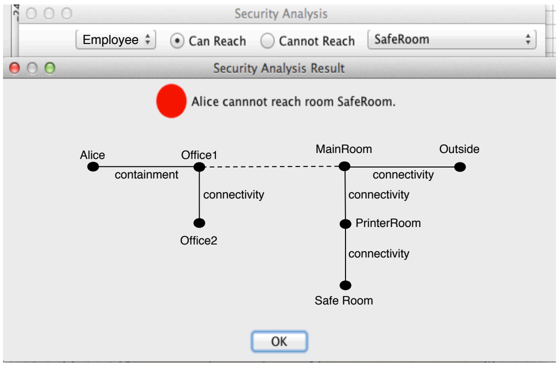
We created RBAC policies by associating Alice and Eve with roles *Employee* and *Visitor*, respectively, and by assigning to each role the following credentials (i.e. list of rooms and assets each role grants access to).

- Employee: PrinterRoom, Office1, Office2, SafeRoom, Desktop2;
- Visitor: PrinterRoom, Office1, Office2, MainRoom, Desktop1.

The usage scenarios are described as follows.

For the first scenario we verify requirement **R1**: "*Every Employee in the building should reach the SafeRoom*". This requirement is not satisfied since the credentials associated with the Employee role only take into account accessibility to the SafeRoom without considering other rooms that might need to be traversed to access the SafeRoom. When a security analysis provides a negative outcome our tool presents a counterexample graph showing containment and connectivity relationships between assets and rooms in the cyber and/or physical space determining the violation of the security requirement. We use a dashed line to indicate those relationships that made the security analysis fail either because they are missing (e.g., two rooms are not connected through a door/window) or because an agent does not have the access rights to exploit that relationship. For example, the graph associated with the outcome of our previous analysis is shown in Figure 5; the line connecting Office1 and the MainRoom is dashed because Alice does not have access rights to enter the MainRoom, although Office1 and the MainRoom are connected.

For the second scenario we verify requirement **R2**: "Every *Visitor should not reach CCTV2"*. This requirement is also violated because -- although Eve does not have access to the SafeRoom -- she can connect to CCTV2, which shares the same network connection as Desktop1. The graph associated with the outcome of this analysis is shown in Figure 6. Eve is co-located with Desktop1 and has the right to access it; the links between Desktop1, the Gateway and CCTV2 identify existing network connectivity that can be exploited by Eve to access CCTV2 from Desktop1.

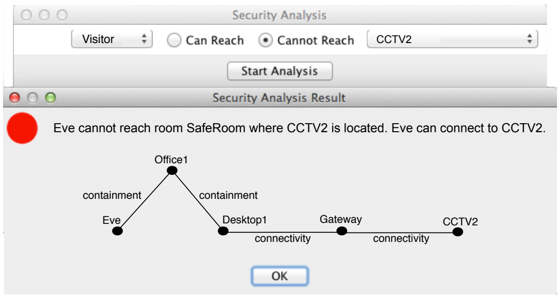

Security Analysis

Employee ● Can Reach ○ Cannot Reach SafeRoom

Security Analysis Result

Alice cannnot reach room SafeRoom.

Figure 5. Outcome of the first security analysis.



Security Analysis

Visitor ○ Can Reach ● Cannot Reach CCTV2

Security Analysis Result

Eve cannot reach room SafeRoom where CCTV2 is located. Eve can connect to CCTV2.

Figure 6. Outcome of the second security analysis.

For the third scenario we assume that a confidential document (*Doc.pdf*) is being printed (i.e. it is contained in the Printer and its status is *open*), and all Employees now are also entitled to access the MainRoom. We verify requirement **R3**: "*No Employee should reach Doc.pdf*". This requirement is not satisfied, because although Alice does not have direct access to the Printer, she might traverse the PrinterRoom while the document is being printed (status open). This is equivalent to having Alice co-located with the document and violating the required security property.

Lessons Learned

The experience of applying our approach to the physical access control problem domain provided us with some key insights and lessons learned summarised below.

Topology is worth it. Explicitly modelling topology ensures a focus on what needs protection, rather than on other secondary concerns. Considering the topology of the cyber and physical space provided an enriched view of the attack surface that could be exploited to achieve potential threats, and led to the definition of more robust access control policies depending on containment and connectivity relationships.

More automation is needed. There is a need to support the systematic derivation of credentials satisfying specific security requirements expressed in terms of accessibility of agents to assets or areas. This would allow security administrators to manage the complexity associated with maintaining the access control system by avoiding manual definition of policies.

We (still) need accurate role models. It is necessary to maintain a mapping between changes in roles that happen, for example, due to changes of work projects, and the resources to which the new roles require to access. This would allow the access control system to change automatically the access control policies affected by such changes.

Complex requirements are still useful. More complex requirements should constrain the paths that agents can traverse to reach certain states. Moreover, specific sequences of interactions of agents in a smart space might lead to violations of access control policies. Such is the case when, for example, a confidential document is printed and access to the printer room must be revoked until the owner collects the document. Inherent to this scenario is that access rights to the printer room must be temporarily revoked, even if other agents are entitled to them according to prevailing policies. Dealing with such scenarios requires verifying access control policies on different evolutions of the topology of the smart space. This would allow the enforcement of finer grained behaviour, such as conditional access depending on the state of the configuration of the space. This is also useful for authentication purposes, where complex protocols involving a specific sequence of actions should be enacted.

Planning to adapt. There is a need of dynamic access control systems, capable of adapting at runtime, to react to changes in topology. Changes in the topology triggered by movements of assets in the physical or cyber space can change the attack surface dynamically. Roles and context changes should also be taken into account as possible adaptation triggers. Indeed changes in roles might require reducing or escalating the current access control policies. However, in large organisations[2] access control policies are escalated when employees change their roles, without revising the credentials that have been granted previously. Moreover, in emergency situations, access levels may need to be temporarily downgraded or reconfigured to facilitate accessibility to safe passages in emergency situations.

However, adaptation does not come for free - it requires specifying triggers of change and monitoring for such changes continuously in order to update the current representation of the topology of a smart space. Those changes cannot always be monitored automatically (e.g., agents movements). To make adaptive approaches accessible assurances are needed that reconfigurations of access control policies satisfy certain security requirements and do not over-entitle agents.

Logging for topology awareness. Digital devices can log security-relevant information. For example, surveillance cameras and card readers can record who has traversed a building area or has accessed a room. Information from logs may be used for different purposes. First, it can help build a more accurate map of the building, complementing the information (e.g., location of computing devices, gateways, network connections) that is originally extracted from the BIM model, if available. Second, logs can provide hints about the building paths that are traversed frequently in order to apply more or less restrictive access control policies to protect those passages and place surveillance cameras or other logging facilities that might be useful for future forensic investigations. Finally, mismatches in logs can be used to identify anomalies. For example, recording of subsequent accesses by an agent to rooms that are distant from each may need to be flagged. Access of an agent to a room and usage by the same agent of a device that is not placed in that room can also indicate security problems.

Open Research Issues

Our experience has identified some further research directions that will extend the applicability of our approach to more complex scenarios. We are planning to include in our model a richer set of security controls, such as authentication mechanisms, can ensure finer grained protection of cyber assets, as well as physical assets that might be cyber controlled.

Automating the assignment of credentials to roles, given a specific set of requirements specified by security analysts will also be addressed in future work. Supporting adaptation of credentials when changes in topology, roles and other contextual factors take place is also an open challenge. Finally, information mined from logs can be used to improve the accuracy of the representation of the building topology that could be updated when changes are detected. Logs can also be used to learn the behavioural patterns of the agents within the building to support targeted surveillance and, more generally, to support forensic readiness.

Acknowledgements

This work was partially supported by the Science Foundation Ireland grant 13/RC/2094, and the ERC Advanced Grant no. 291652.

References

1. B. Schneier, “Is Perfect Access Control Possible?” Sept. 2009; https://www.schneier.com/essays/archives/2009/09/is_perfect_access_co.html.
2. X. Zhao and M. E. Johnson. “Access Governance: Flexibility with Escalation and Audit,” *Proc. 43rd Hawaii Int. Conf. on Systems Science*, 2010, pp. 1-3.
3. L. Pasquale, C. Ghezzi, C. Menghi, C. Tsigkanos, and B. Nuseibeh, “Topology Aware Adaptive Security,” *Proc. of the 9th ACM Int. Symposium On Software Engineering for Adaptive and Self-Managing Systems*, 2014, pp. 43-48.
4. C. Tsigkanos, L. Pasquale, C. Ghezzi, and B. Nuseibeh, “On the Interplay Between Cyber and Physical Spaces for Adaptive Security,” IEEE *Trans. on Dependable and Secure Computing*, 2016, to appear.
5. C. Eastman, C. M. Eastman, P. Teicholz, and R. Sacks, *BIM Handbook: A Guide to Building Information Modeling for Owners, Managers, Designers, Engineers and Contractors*, John Wiley & Sons, 2011.
6. *ISO 16739:2013. Industry Foundation Classes (IFC) for Data Sharing in the Construction and Facility Management Industries*, 2013.
7. AutoDesk, “Revit,” www.autodesk.com/products/revit-family/overview.
8. R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, “Role-Based Access Control Models,” *IEEE Computer*, vol. 29, no. 2, 1996, pp. 38–47.
9. V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone. "Guide to attribute based access control (ABAC) definition and considerations." *NIST Special Publication 800*, no. 162, 2014.
10. H. Merz, T. Hansemann, and C. Hübner: *Building Automation: Communication Systems with EIB/KNX, LON and BACnet*, Springer Science & Business Media, 2009.

Related Work: Access Control Security Analysis

Research in construction automation has leveraged the BIM standard to perform security analysis. For example, Chen et al.[1] propose a simulation technique to identify what parts of a physical space are covered when CCTV cameras are placed at predefined locations and have a specific focal length. Rafiee[2] detects intrusions of malicious agents in a physical area by identifying mismatches between the information provided by Ultra Wide Band Real-time Location Systems and the video recordings from CCTV cameras. BIM-XACML[3] is a policy extension to eXtensible Access Control Markup Language (XACML[4]) that allows expressing access control conditions that involve reachability relationships that can be inferred from the model of the building, including normal pathways, such as corridors, stairways and lifts, as well as indirect pathways such as ceiling spaces, partition walls, and ventilation ducts. Porter et al.[5] provide an approach for measuring the time that can be taken by an agent to reach a specific area by considering the structure of a building and the time that can be taken to break barriers (e.g., doors, windows, walls) made of different materials.

However, existing work in construction automation has focused exclusively on physical security without considering cyber-physical threats exploiting, for example, network connectivity between computing devices. Recently, existing work[6] has enriched BIM models with semantics of cyber-physical space descriptions, focusing however on verification of reliability properties regarding evolution of the space.

Verification of access control policies has been mainly centered on XACML and RBAC. For example, Hu et al.[7] propose a SAT encoding for analysing properties of XACML policies. Anomaly discovery has also gained attention recently. For example, Hughes et al.[8] use a binary decision diagram based technique to check whether policy redundancies exist. Fitzgerald et al.[9] further explore the notion of topology to formally define and detect a larger set of anomalies for physical access control, such as building topology anomalies (e.g., one or more areas of the building are not reachable from the outside), and conflicting policies. However, these approaches do not allow verifying access control policies depending on topological properties, such as containment and connectivity, expressed on both the cyber and physical space that a building inhabits. Moreover, they do not provide justifications to support the result of the analysis, which could provide guidance on how the policies should be revised if verification fails.

References

1. H.-T. Chen, S.-W. Wu, and S.-H. Hsieh, “Visualization of CCTV Coverage in Public Building Space using BIM Technology,” *Visualization in Engineering*, vol. 1, no. 1, 2013, pp. 1-17.
2. M. Rafiee, “Improving Indoor Security Surveillance by Fusing Data from BIM, UWB and Video,” master’s thesis, Concordia University, 2014.
3. N. Skandhakumar, “Integrated Access Control for Smart Buildings using Building Information Models,” PhD dissertation, Queensland University of Technology, 2014.
4. *OASIS Std. eXtensible Access Control Markup Language (XACML) Version 3.0*, 2013.
5. S. Porter, T. Tan, T. Tan, and G. West, “Breaking into BIM: Performing Static and Dynamic Security Analysis with the Aid of BIM,” *Automation in Construction*, vol. 40, 2014, pp. 84-95.
6. C. Tsigkanos, T. Kehrer, C. Ghezzi, L. Pasquale and B. Nuseibeh, “Adding Static and Dynamic Semantics to Building Information Models,” *Proc. 2nd Int. Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS 16)*, 2016, pp. 1-7.
7. H. Hu, G.-J. Ahn, and K. Kulkarni, “Anomaly Discovery and Resolution in Web Access Control Policies,” *Proc. 16th ACM Symp. On Access Control Models and Technologies* (SACMAT 11), 2011, pp. 165-174.

8. G. Hughes and T. Bultan, “Automated Verification of Access Control Policies Using a SAT Solver,” *Int. J. on Software Tools for Technology Transfer*, vol. 10, no. 6, 2008, pp. 503-520.
9. W. M. Fitzgerald, F. Turkmen, S. N. Foley, and B. O'Sullivan, “Anomaly Analysis for Physical Access Control Security Configuration,” *Proc. 7th IEEE Int. Conf. on Risk and Security of Internet and Systems* (CRiSIS 12), 2012, pp. 1-8.

Author Biographies

Liliana Pasquale is a lecturer at University College Dublin (Ireland) since June 2016. She received her PhD from Politecnico di Milano in 2011. Her research interests are in requirements engineering and adaptive systems, with particular focus on security, privacy and digital forensics. She received an IBM PhD Fellowship, a Windows Azure for Research Award and a Best Paper Award at ICWS and SEAMS.

Carlo Ghezzi is a full professor at the Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Italy. He is an ACM Fellow, an IEEE Fellow, a member of the European Academy of Sciences and of the Italian Academy of Sciences. He received the ACM SIGSOFT Outstanding Research Award (2015) and the Distinguished Service Award (2006). He is past President of Informatics Europe. He has been the Editor in Chief of the ACM Trans. On Software Engineering and Methodology and Associate Editor of IEEE Trans. on Software Engineering. He is currently an Associate Editor of the Communications of the ACM and Science of Computer Programming. His research has been mostly focusing on different aspects of software engineering. He co-authored over 200 papers and 8 books. He coordinated several national and international research projects and has been a recipient of an ERC Advanced Grant.

Edoardo Pasi is a web developer at Skillbill srl (Italy). He received his Master from Politecnico di Milano in 2015. His research interests are in access control of smart buildings.

Christos Tsigkanos is a PhD candidate at Politecnico di Milano under the supervision of prof. Carlo Ghezzi. He received his received a BSc degree in computer science from University of Athens and a MSc degree in software engineering from University of Amsterdam. His research interests lie in the intersection of software engineering and security, and include self-adaptive systems, cyber-physical systems, requirements engineering and formal verification.

Menouer Boubekeur leads the External Research Development activities at the European Research Center for United Technologies (UTC) in Cork (Ireland). He holds a Ph.D. from the University of Joseph Fourier for research into formal verification of asynchronous circuits in late 2004. His main research interests are in the areas of complex systems, embedded and real-time systems, Cyber physical systems and cyber security.

Blanca Florentino-Liano holds a Master degree in Multimedia and Communication from University Carlos III of Madrid (UC3M, Spain). She joined the European Research Centre for United Technologies in Cork (Ireland) in 2012 where she is working in the decision support group as a senior research scientist conducting research in the area of machine learning and data mining for security and energy applications. Her main research interests are signal processing, data mining and pattern recognition. She is a member of the Society of Women Engineers (SWE).

Tarik Hadzic is a staff research scientist at the European Research Center for United Technologies in Cork (Ireland) since 2011. He received his Ph.D. in Information Technology and Computer Science from the IT University of Copenaghen in 2007. His research interests focus on design, development and application of intelligent reasoning techniques such as constraint programming, decision diagrams, and discrete optimization to a number of application domains, such as of product configuration and access control policy management.

Bashar Nuseibeh is Professor of Computing at The Open University (Director of Research 2001-2008) and Professor of Software Engineering at Lero - the Irish Software Research Centre (Chief Scientist 2009-2012). He is a Visiting Professor at University College London (UCL) and the National Institute of Informatics (NII), Japan. His research interests lie at the intersection of requirements engineering, adaptive systems, and security and privacy. He served as Editor-in- Chief of IEEE Trans. on Software Engineering and the Automated Software Engineering Journal. He received an ICSE Most Influential Paper Award, a Philip Leverhulme Prize, an Automated Software Engineering Fellowship, a Senior Research Fellowship of the Royal Academy of Engineering, and an ACM SIGSOFT Distinguished Service Award. He currently holds a Royal Society-Wolfson Merit Award and an ERC Advanced Grant on Adaptive Security and Privacy.

Email Addresses

Dr. Liliana Pasquale
liliana.pasquale@ucd.ie

Prof. Carlo Ghezzi
carlo.ghezzi@polimi.it

Mr. Edoardo Pasi
edoardo.gacc@gmail.com

Mr. Christos Tsigkanos
christos.tsigkanos@polimi.it

Ms. Blanca Florentino-Liano
florenb@utrc.utc.com

Dr. Tarik Hadzic
HadzicT@utrc.utc.com

Dr. Menouer Boubekeur
boubeKM@utrc.utc.com

Prof. Bashar Nuseibeh
b.nuseibeh@open.ac.uk