Topology-Aware Access Control of Smart Spaces

Liliana Pasquale, University College Dublin and Lero

Carlo Ghezzi, Edoardo Pasi, and Christos Tsigkanos, Politecnico di Milano

Menouer Boubekeur, Blanca Florentino-Liano, and Tarik Hadzic, United Technologies Research Centre

Bashar Nuseibeh, The Open University and Lero

Smart spaces are becoming increasingly vulnerable from the interplay of cyber and physical entities. A representation of the spaces' topology can reveal security-relevant contextual characteristics, and a visualization tool allows security analysts to edit space topology and verify that access-control policies meet security requirements.

Access control gives organizations the ability to manage which individuals can access what assets, granting individuals the exact access level that befits their role or roles.[1] In large organizations, access control becomes more complex because individuals can have many roles that can change frequently.[2] Despite the substantial research literature and high-profile security products, security analysts still have no way to verify whether existing access-control policies grant the exact access level that employees need. Moreover, many organizations fall short of implementing the correct policies. For example, in large organizations, 50 to 90 percent of employees have over-entitled access, which presents opportunities for insiders to cause harm.[2]

See **www.computer.org/computer-multimedia** for multimedia content related to this article.

A representation of the topology of cyber and physical spaces that accounts for their key structure and relationships can provide security-relevant contextual characteristics, such as where assets are placed and how security controls should be enacted.[3] The topology of a *physical* space can capture the layout of a building including its structural relationships, such as containment and connectivity: a building contains rooms, and rooms are connected through a door. Similarly, the topology of a *cyber*space can capture how a network and digital devices are configured and also include containment and connectivity relationships: a file is stored in a device and devices are connected through a network. A meta-calculus can be used to represent the topology of a cyber-physical space and its dynamics—for example, an agent's access to a physical area allows her to connect her phone to the local network. This representation can be used to reason about the consequences of topology changes on the satisfaction of security requirements.[4]

To support the access control of cyber-physical spaces, such as smart buildings, we developed a tool that security analysts can use to visualize and edit a building's topological characteristics and verify whether access-control policies satisfy the security requirements imposed on

0018-9162/17/$33.00 © 2017 IEEE

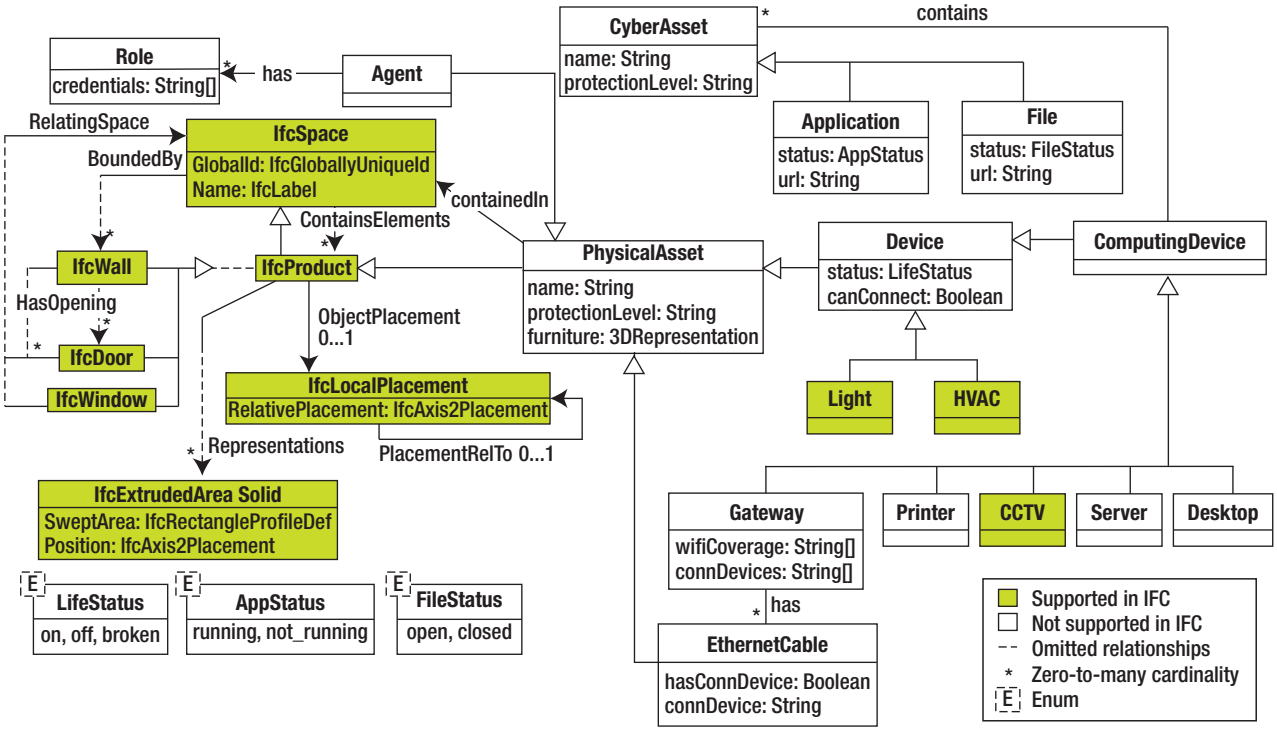

FIGURE 1. The BIM-Sec metamodel (a representation of a building's topological characteristics that is tailored to meet security analysts' needs). BIM-Sec is a lightweight version of the metamodel underlying industry foundation classes (IFCs)—the de facto standard format for exchanging Building Information Modeling (BIM) models. IFC-supported entities are the green boxes. Along with the IFC metamodel, BIM-Sec includes entities that access-control practitioners identified as security-relevant (white boxes).

reachability relationships—for example, to verify whether an individual can reach a specific asset or building area. If verification fails, the tool provides guidance on how to revise access-control policies for the current topological configuration. The representation of a building's topological characteristics—referred to as BIM-Sec—is tailored to meet security analysts' needs and is compliant with the Building Information Modeling (BIM) standard to ensure wider applicability of our approach.[5] BIM-Sec augments the BIM model with a representation of a building cyberspace, omitting those details of the physical building that are likely to be irrelevant for security analysts.

To evaluate our tool, we applied it in scenarios from security analysts that reflect practical problems in the access control of smart buildings. Our emphasis was on demonstrating how a system founded on software engineering principles, such as interactive development, visual abstraction, formal modeling, and requirements specification, can be applied to support security analysts in the design of access-control policies for cyber-physical spaces.

REPRESENTING CYBER-PHYSICAL SPACES

The BIM model, which is produced from the CAD software, makes it possible to represent a building's structural and functional characteristics. Industry foundation classes (IFCs) have become the de facto standard format for exchanging BIM models in the construction industry.[6] As the sidebar "Analyzing Access-Control Security" describes, despite its widespread adoption to support security analysis, the BIM model alone is not expressive enough to represent security-relevant characteristics. For example, it does not include a representation of cyber assets; certain physical assets, such as agents; or access control policies. Moreover, the graphical tools adopted to create and modify BIM models, such as Autodesk's Revit (autodesk.com/products/revit-family/overview), do not support security analysis. In addition, security analysts perceive the BIM model as overly expressive and heavy on detailed structural properties that might be irrelevant in defining access-control policies.

Figure 1 shows the BIM-Sec metamodel with some intermediate relationships between IFC entities omitted for simplification. The model represents a building as a collection of rooms, with each room represented as an `IfcProduct` element labeled with a name and an identifier inherited from `IfcSpace`. A room can also contain other building structural elements, such as walls and furniture, as described by the relationship `ContainsElement` brought by `IfcSpace`. Each room can be bounded by walls (`IfcWall`), which in turn can have opening points, each of which indicates the presence of a door (`IfcDoor`) or window (`IfcWindow`).

ANALYZING ACCESS-CONTROL SECURITY

Construction-automation research has used the Building Information Modeling (BIM) standard as the basis for exploring access security. Efforts have been focused on physical security, but recent work is adding a cyber dimension to the BIM-based studies.

PHYSICAL SECURITY

One research group proposed 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.[1] Another approach detects intrusions of malicious agents in a physical area by identifying mismatches between the information provided by ultra-wideband real-time location systems and the video recordings from CCTV cameras.[2] BIM-XACML[3] is a policy extension to eXtensible Access Control Markup Language (XACML)[4] that allows the expression of access-control conditions involving reachability relationships that can be inferred from the building model, including normal pathways (for example, corridors, stairways, and lifts) and indirect pathways (for example, ceiling spaces, partition walls, and ventilation ducts). One proposed approach measures how long it will take an agent to reach a specific area, basing that value on building structure and the time it can take to break barriers of different materials, such as doors, windows, and walls.[5]

CYBER-PHYSICAL SECURITY

Although physical security is a critical part of access control, cyber-physical threats must also be considered, as an agent can exploit aspects such as network connectivity among devices to access sensitive data stored in a device within the building that cannot be physically reached. Recent work has enriched BIM models with the semantics of cyber-physical space descriptions, with an emphasis on verifying the reliability properties of a space's evolution (for example, the time required to reach one room from another).[6]

Verification of access-control policies has centered on XACML and role-based access control (RBAC)—a popular method for restricting system access. One group proposed analyzing XACML policy properties by encoding them into a Boolean satisfiability problem.[7] Anomaly discovery has also gained attention. Efforts include the use of a technique based on a binary decision diagram that checks for any policy redundancies[8] and a topology for formally defining and detecting an extended set of anomalies for physical access control.[9] These include building topology anomalies, such as building areas that are not reachable from the outside, and conflicting policies.

The main drawback of current work to verify access-control policies is that it omits policies based on cyber-physical topological properties, such as containment (a room contains devices, and a device runs applications and stores files) and connectivity (rooms are connected through a door, and devices are connected through the network). Moreover, these approaches lack justifications to support analytical results, which are needed to guide policy revisions 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 Eng.*, 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 Univ., 2014.
3. N. Skandhakumar, "Integrated Access Control for Smart Buildings Using Building Information Models," PhD dissertation, Queensland Univ. of Technology, 2014.
4. *OASIS Std. eXtensible Access Control Markup Language (XACML) Version 3.0*, 2013; oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.
5. S. Porter et al., "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 et al., "Adding Static and Dynamic Semantics to Building Information Models," *Proc. 2nd Int'l Workshop Software Eng. 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. 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'l J. Software Tools for Technology Transfer*, vol. 10, no. 6, 2008, pp. 503–520.
9. W.M. Fitzgerald et al., "Anomaly Analysis for Physical Access Control Security Configuration," *Proc. 7th IEEE Int'l Conf. Risk and Security of Internet and Systems* (CRiSIS 12), 2012, pp. 1–8.

A door or a window can enable rooms to connect, as indicated by the `RelatingSpace` relationship. A building's structural element (`IfcProduct`) is also characterized by its location (`ObjectPlacement` relationship). In particular, `IfcLocalPlacement` defines the relative placement of an element in relation to other spaces that might contain it (`PlacementRelTo` relationship). Each building structural element can also be associated with a set of graphical representations. A room's shape is described by the `SweptArea` property of the `IfcExtrudedAreaSolid` entity.

Extensions to the IFC metamodel

BIM-Sec extends `IfcProduct` to represent a physical asset as `PhysicalAsset`. Agents are a specific physical asset that can traverse the building in accordance with its structural properties. Agents are not considered part of the `IfcActor` elements in the IFC metamodel, which represent the various stakeholders involved in building construction. BIM-Sec expresses access-control policies according to the role-based access control (RBAC) model[7] by associating each agent with a set of roles. A role is in turn associated with a set of credentials—a list of physical areas and assets to which the role is granted access. An alternative model is attribute-based access control (ABAC),[8] which grants authorization to perform operations on the basis of evaluating the attributes associated with the subject, object, and requested operations. Although ABAC enables access-control policies to be more dynamic, for example, to block access temporarily, we chose to use RBAC in BIM-Sec because it is more widely used in practice.

Physical assets, including agents, can be contained in a physical space, as indicated by the `containedIn` relationship. This relationship is explicitly defined for the physical assets that are not included in the IFC metamodel.

A physical asset can also be a device (`Device`), such as a light or a heating, ventilation, air conditioning (HVAC) unit. Devices can connect to other devices, and are characterized by a status (on, off, or broken). Lights are security relevant because, for example, their malfunctioning might hinder surveillance, allowing an intruder to access a valuable asset unnoticed. Likewise, malfunctioning HVAC units might compromise the integrity of datacenters or of critical equipment collocated in the area for which the HVAC unit must maintain a specific temperature and humidity. The IFC metamodel includes an element to represent an HVAC unit (`IfcHvacDomain`), but has no representation for capturing the unit's current status and network connectivity.

Computing devices

BIM-Sec also represents computing devices (`ComputingDevices`) that can contain assets (`CyberAssets`) such as files or applications. A computing device is security relevant, not only because its contents can be accessed directly or by connected devices but also because the status of files on a device (open or not) reveals whether the agents in the same physical space can see that content and possibly breach its confidentiality.

Gateways and Ethernet cables enable network connectivity and allow accessibility to connected devices. Representing network connectivity is particularly relevant for a building's automation systems because network protocols, such as KNX,[9] do not include security features. For example, passwords employed to authenticate valid commands could 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.

IMPORTING MODELS AND EDITING POLICIES

Our tool for topology-aware access control provides security analysts with a GUI to facilitate importing 3D representations of building entities for use in modifying and analyzing the security of smart buildings. Figure 2 shows a screenshot. Our tool extends Sweet Home 3D (sweethome3d.com), an open source software application for drawing a house plan, arranging furniture, and visualizing results in 3D.

Entity importing and editing

In areas 1 and 2 of the screenshot in Figure 2, security analysts can import an IFC file and edit its corresponding BIM-Sec representation, which is maintained and modified locally. Our tool extracts only entities and properties that are security relevant, ignoring those that characterize complex architectural properties or other furniture elements. Security analysts can enrich a BIM-Sec model by updating an asset's status, revising contained cyber assets, identifying network connectivity between two devices,

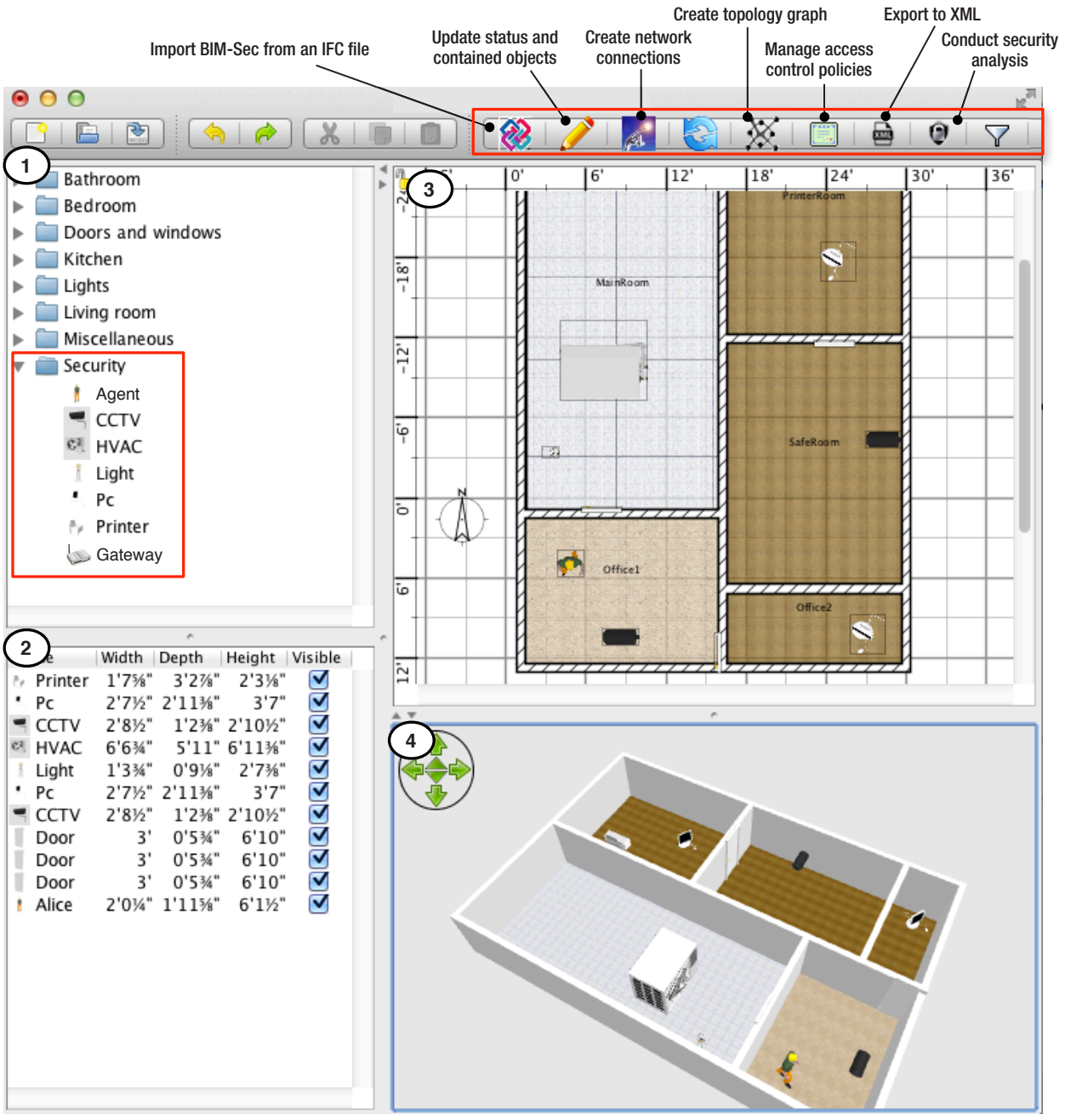

FIGURE 2. Screenshot from our tool's GUI, which extends Sweet Home 3D. In area 1, analysts can import an IFC file, which is a 3D representation of entities. In area 2, they can edit the corresponding BIM-Sec representation. In areas 3 and 4, they can visualize the building in 2D and 3D. The red box around entities in area 1 and toolbar icons denote functions beyond those provided in Sweet Home 3D.

and specifying access-control policies. They can also export the modified BIM-Sec model into a text format, such as XML, for porting to existing access-control systems or to applications that might use the BIM model to verify requirements unrelated to security, such as energy, efficiency, and safety.

Topology graph

From the BIM-Sec model, our tool generates a graph that captures the building's cyber-physical topology. Each node represents a room (an instance of the `IfcProduct` class) or an asset, and links are annotated with a type that expresses the nodes' relationship. A connectivity link, for example, can indicate that two rooms are connected through a door or a window, or that two devices are linked through a network. A containment link can be between a room and the physical assets it contains or between a digital device and the cyber assets it contains. We assume that a path exists between every node pair.

Security requirements are expressed as reachability properties; for example, employees with a certain role can or cannot reach an asset or a room. Our tool applies a breadth-first search algorithm with linear complexity to traverse the graph and verify reachability properties. The nature of our algorithm ensures that our tool will scale in practical settings.

In parsing IFC files, our tool has some limitations; for example, it supports only rooms that the IFC metamodel defines as rectangular. Our tool is also limited to use with building plans involving a single floor; we aim to extend our tool for building plans involving multiple floors connected through stairs and elevators.

APPLICATION SCENARIOS

Three use scenarios provided by professional access-control analysts give a flavor of our approach's broader applicability. These scenarios are simple because the sheer size of the underlying models in practical settings makes manual evaluation infeasible even for simple requirements. We also created a YouTube video of our tool in action with other simple scenarios (youtube.com/watch?v=zuLumnbv5w0).

Building plan

Figure 3 shows a map of the building we imported from an IFC file and further edited for our scenarios. Figure 4 shows the graph of the building topology.

We created RBAC policies by associating `Alice` with the `Employee` role and `Eve` with the `Visitor` role and assigned each role credentials as follows:

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

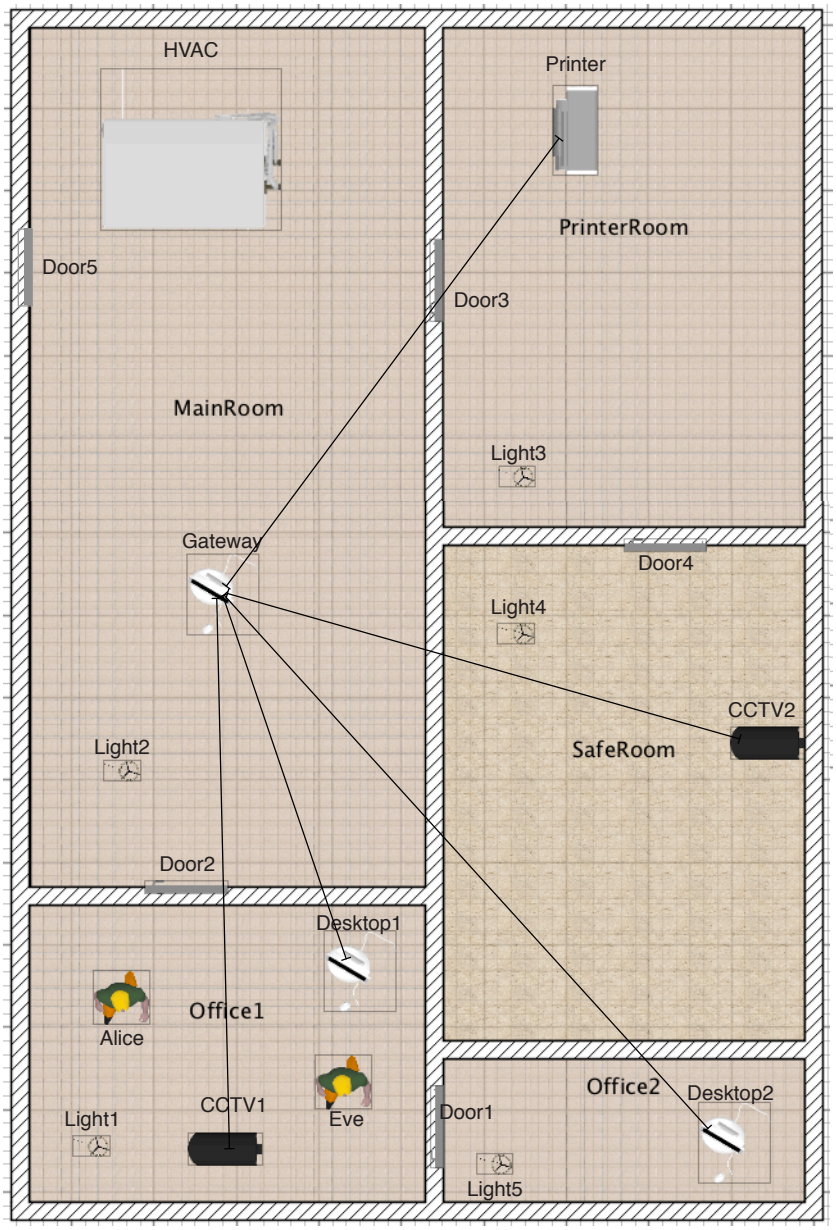

FIGURE 3. Building map for the application scenarios. The building includes five rooms represented as `Office1`, `Office2`, `MainRoom`, `SafeRoom`, and `PrinterRoom`. Each room can contain security-relevant entities; for example, `PrinterRoom` contains a `Printer` entity, while `MainRoom` contains `HVAC` and `Gateway` entities. The gateway's wireless signal covers all five rooms. `Office1` and `Office2` contain `Desktop1` and `Desktop2`, and `Office1` contains agents `Alice` and `Eve`. Existing network connections are shown as continuous lines connecting different devices.

Scenario 1

The goal in the first scenario was to verify the requirement "Every employee in the building should be able to reach the safe room." This requirement is not satisfied since the credentials associated with the `Employee` role take into account accessibility only to the safe room; they do not consider the room that the employee might need to traverse to get to the safe room.

When a security analysis yields a negative outcome, our tool provides a

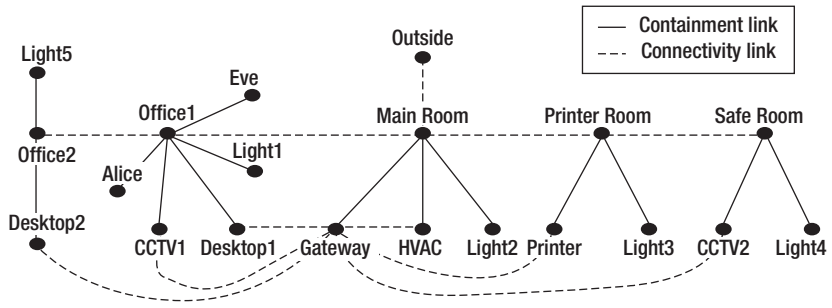

FIGURE 4. Graph associated with the building map in Figure 3.

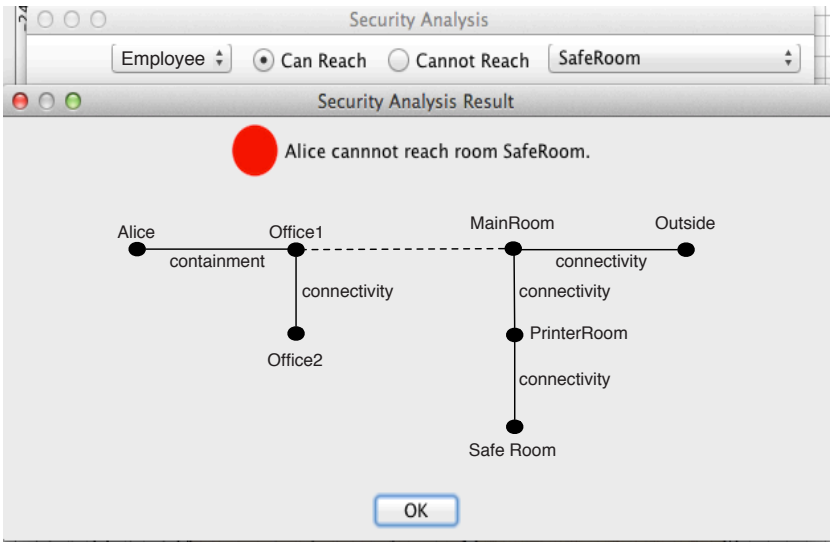

FIGURE 5. Outcome of the security analysis in the first application scenario. The outcome is negative (red dot), so the tool provides a counterexample graph showing the connectivity needed for a positive outcome (dashed line). In this case, Alice requires credentials to go through the main room to reach the safe room.

counterexample graph, as in Figure 5, which shows existing containment and connectivity relationships between assets and rooms and a dashed line to denote why the outcome was negative. In Figure 5, the dashed line connects the rooms that Alice (in the `Employee` role) must cross to reach the safe room. Missing relationships can make the security analysis fail because the agent does not have access rights. In scenario 1, Alice does not have access rights to the main room and so cannot go there even though Office1 and the main room are connected.

Scenario 2

The second scenario's objective was to verify the requirement, "Every visitor should not reach CCTV2." As Figure 6 shows (and Figure 4, although less obviously), this requirement is also violated because Eve can connect to the desktop in the office she is visiting (Office1), and through the gateway, she can connect to CCTV2. The graph in Figure 6 clearly shows that Eve is collocated with the desktop and has the right to access it, but it also shows how she can connect to CCTV2 through links between `Desktop1`, `Gateway`, and `CCTV2`.

Scenario 3

In the third scenario, the aim is to verify the requirement "No employee should ever be able to reach doc.pdf." We assumed that doc.pdf is a confidential document being printed: it is contained in `Printer` and its status is `open`), and that all employees have access to the main room. According to Figure 4, the requirement is violated because, although Alice (assigned the `Employee` role) cannot access the digital version of the document because she cannot access the printer, she *can* cross the printer room while the doc.pdf is being printed. Alice's ability to be in the printer room at that time violates the reachability property in the requirement and by extension violates the required security.

INSIGHTS INTO SECURE ACCESS CONTROL

Our experiments in applying our tool to support access control gave us considerable insight into security-related access-control issues and helped us arrive at some foundational principles.

Topology is worth it. Explicitly modeling topology ensures that analysts can focus on what needs protection, rather than on secondary concerns. Considering a building's cyber-physical topology enriches the view of the attack surface that adversaries could exploit and leads to the definition of more robust access-control policies that reflect containment and connectivity relationships.

More automation is required. Researchers should address ways to systematically derive credentials that satisfy specific security requirements expressed in terms of agents' accessibility to assets or areas. Automated derivation would free security administrators to manage the complexity associated with maintaining the access-control system rather than manually defining policies.

Role mapping is critical. Mapping roles makes it easier to track how they

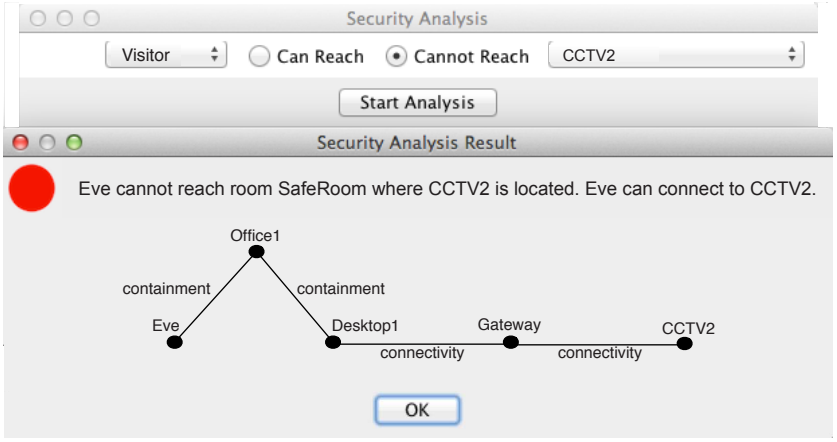

FIGURE 6. Outcome of the second security analysis. Again, the requirement is violated because Eve can connect to the CCTV2 even though she cannot physically reach it. Although the graph is not a counterexample, it isolates and clarifies the path that Eve can take to access CCTV2, which is less intuitive in the graph in Figure 4.

change related to work projects and resource access. The access-control system could then accommodate new or altered roles simply by changing relevant access policies.

Complex requirements can be useful. Specific agent-interaction sequences in a smart space might lead to violations of access-control policies; for example, when a confidential document is printed, access to the printer room must be revoked until the owner collects the document. Thus, access rights to the printer room must be temporarily revoked, even if access-control policy dictates that other agents are entitled to that access. Complex requirements, such as conditional access, can constrain the paths that agents traverse to reach certain assets or areas. Such requirements would allow the enforcement of policy even when the topology changes (the printer room "evolves" from being a universally accessible space to a restricted one until a document finishes printing). Such complex requirements would account for the state of the space's configuration and would also be useful for authentication, which requires enacting complex protocols that involve completing a specific action sequence.

Adaptability is key. Dynamic access-control systems could adapt at runtime in response to topology changes triggered by asset movement in either physical space or cyberspace or by role or context changes. Such changes might require reducing or escalating an employee's access credentials. In large organizations, the latter case is frequent, as employees change their roles but often without revising any previously granted credentials. In emergency situations, access levels might need to be temporarily downgraded or reconfigured to facilitate accessibility to safe passages.

Adaptability comes at a cost, however. Change triggers must be specified, and identifying them requires continuous monitoring to keep the topology's representation current. Moreover, changes such as agent movement cannot always be monitored automatically. 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 is important for topology awareness. Logging is an excellent way to keep a building's cyber-physical topology in the forefront. Surveillance cameras and card readers can record who has traversed a building area or accessed a room. Information from logs can be used to create a more accurate building map to complement information extracted from the BIM model by identifying the location of computing devices, gateways, and network connections. Logs can also be used to pinpoint building paths that are most often used, which is valuable information for adjusting access-control policies. Analysts can make access more or less restrictive and place cameras or other logging facilities in frequently traversed passages to protect them or provide information for future forensic investigations. Finally, mismatches in logs can highlight anomalies—for example, an agent accesses two distant rooms in a very short time or uses a device that is not physically in the same room.

Additional research will extend the applicability of our BIM-Sec model and visualization tool to more complex scenarios. We are already updating the model to include a richer set of security controls, such as authentication mechanisms, which can ensure finer-grained protection of cyber assets and cyber-controlled physical assets, such as increasing a desktop screen's opacity to temporarily protect the confidentiality of digital documents currently in use or applying two-factor authentication to secure access to the process that controls the building's HVAC systems.

We also plan to address ways to automate assigning credentials to roles according to specific security requirements. An open challenge is how to support dynamic credential adaptation when topology, roles

ABOUT THE AUTHORS

LILIANA PASQUALE is a lecturer in the Computer Science Department at University College Dublin and associated researcher at Lero—the Irish Software Research Centre. Her research interests include requirements engineering and adaptive systems, with a focus on security, privacy, and digital forensics. Pasquale received a PhD in information and communication technologies from Politecnico di Milano. She is member of IEEE and is on the editorial board of the *IET Journal*. Contact her at liliana.pasquale@ucd.ie.

CARLO GHEZZI is a full professor in the Department of Electronics, Information, and Bioengineering at Politecnico di Milano. His research interests include software engineering with a focus on software evolution, self-adaption, and formal assurances. Ghezzi is a Fellow of IEEE and ACM, and a member of the European Academy of Sciences and of the Italian Academy of Sciences. He is an associate editor of *Communications of the ACM* and *Science of Computer Programming*. He received an ERC Advanced Grant on Self-Managing Situational Computing. Contact him at carlo.ghezzi@polimi.it.

EDOARDO PASI is a web developer at Skillbill. While conducting the research reported in this article he was a graduate student in computer engineering at Politecnico di Milano. His research interests include access control of smart buildings, software development, and functional programming. Pasi received an MSc in computer engineering from Politecnico di Milano. Contact him at edoardo.gacc@gmail.com.

CHRISTOS TSIGKANOS is a postdoctoral researcher at Politecnico di Milano. His research interests include requirements engineering, cyber-physical systems, and formal verification. Tsigkanos received a PhD in information and communication technologies from Politecnico di Milano. He is a member of IEEE. Contact him at christos.tsigkanos@polimi.it.

MENOUER BOUBEKEUR is a manager in the Strategic Business Development group at the United Technologies Research Centre. His research interests include complex, embedded, and real-time systems; cyber-physical systems; and cyber security. Boubekeur received a PhD in computer science from the University of Joseph Fourier. Contact him at boubeKM@utrc.utc.com.

BLANCA FLORENTINO-LIANO is a senior research scientist in the Decision Support group at the United Technologies Research Centre. Her research interests include machine learning and data mining for security and energy applications, signal processing, and pattern recognition. Florentino-Liano received an MSc in multimedia and communication from the University Carlos III of Madrid (UC3M). She is a member of the Society of Women Engineers (SWE). Contact her at florenb@utrc.utc.com.

TARIK HADZIC is a staff research scientist in the System Modeling and Optimization group at the United Technologies Research Centre. His research interests include the design, development, and application of intelligent reasoning techniques in product configuration and access control–policy management. Hadzic received a PhD in IT and computer science from the IT University of Copenaghen. Contact him at hadzict@utrc.utc.com.

BASHAR NUSEIBEH is a professor of computing at The Open University, a professor of software engineering at Lero—the Irish Software Research Centre, and a visiting professor at University College London (UCL) and the National Institute of Informatics (NII), Japan. His research interests include requirements engineering, adaptive systems, security, and privacy. Nuseibeh received a PhD in software engineering from Imperial College London. He is a Fellow of the British Computer Society and the Institution of Engineering & Technology and holds a Royal Society–Wolfson Merit Award and an ERC Advanced Grant on Adaptive Security and Privacy. Contact him at b.nuseibeh@open.ac.uk.

and other contextual factors change. We also encourage organizations to mine logged information, which analysts can then use to refine the building topology's representation and make it easier to update in response to change. Logs are also useful for targeted surveillance and forensic investigation. Equipped with such information, analysts can ensure that access control is consistently in line with security requirements.

ACKNOWLEDGMENTS

This work was partially supported by a Science Foundation Ireland grant 13/RC/2094, and ERC Advanced Grants 291652 (Adaptive Security and Privacy [ASAP]) and 227977 (Self-Managing Situated Computing [SMScom]).

REFERENCES

1. B. Schneier, "Is Perfect Access Control Possible?," Sept. 2009; 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. Systems Science* (HICSS-43), 2010, pp. 1–3.
3. L. Pasquale et al., "Topology Aware Adaptive Security," *Proc. 9th ACM Int'l Symp. Software Eng. for Adaptive and Self-Managing Systems* (SEAMS 14), 2014, pp. 43–48.
4. C. Tsigkanos et al., "On the Interplay between Cyber and Physical Spaces for Adaptive Security," *IEEE Trans. Dependable and Secure Computing*, 2016; ieeexplore.ieee.org/document/7542583.
5. C. Eastman et al., *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 (IFCs) for Data Sharing in the Construction and Facility Management Industries*, 2013.
7. R.S. Sandhu et al., "Role-Based Access Control Models," *Computer*, vol. 29, no. 2, 1996, pp. 38–47.
8. V.C. Hu et al., *Guide to Attribute-Based Access Control (ABAC) Definition and Considerations*, NIST Special Pub. 800, no. 162, 2014.
9. H. Merz, T. Hansemann, and C. Hübner, *Building Automation: Communication Systems with EIB/KNX, LON and BACnet*, Springer Science & Business Media, 2009.