BlueSky: Physical Access Control: Characteristics, Challenges, and Research Opportunities

Amirreza Masoumzadeh
University at Albany – SUNY
Albany, New York, USA
amasoumzadeh@albany.edu

Hans van der Laan
Nedap N.V.
Groenlo, Netherlands
hans.vanderlaan@nedap.com

Albert Dercksen
Nedap N.V.
Groenlo, Netherlands
albert.dercksen@nedap.com

ABSTRACT

Physical access control (PAC) is an integral part of the physical security system of any organization. However, despite the size of the PAC industry and its importance in securing our physical environments, public research and development regarding PAC are limited. This paper aims to lower the barriers for the access control research community to explore and engage in the research opportunities regarding PAC systems. We characterize PAC systems and present an access control architecture that captures their central concepts, such as physical space models and different levels of policies, and processes such as policy conversion, enforcement, and analysis. We discuss how PAC can be distinguished from logical access control (LAC), which is applicable to cyber environments. We also present several unique challenges and research opportunities that the PAC domain introduces.

CCS CONCEPTS

• **Security and privacy → Access control**; **Authorization**.

KEYWORDS

physical access control, access control policy, physical security, policy conversion, policy enforcement, policy analysis

ACM Reference Format:
Amirreza Masoumzadeh, Hans van der Laan, and Albert Dercksen. 2022. BlueSky: Physical Access Control: Characteristics, Challenges, and Research Opportunities. In *Proceedings of the 27th ACM Symposium on Access Control Models and Technologies (SACMAT) (SACMAT '22), June 8–10, 2022, New York, NY, USA.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3532105.3535019

1 INTRODUCTION

Physical access control (PAC) is one of the central pillars of an organization's security system. From pharmaceutical employees stealing drugs [9] to a flight management system being stolen from a parked aircraft [14] and heroin disappearing from police evidence lockers before trials [9], small holes in PAC systems can have huge consequences. PAC protects people and physical resources against unauthorized accesses and the disastrous consequences associated. In essence, it is about managing who can access a physical resource/location and when.

PAC is omnipresent, with $8.8 bn worth of PAC products being sold globally in 2021, up from $6.7 bn in 2016, and with $12.0 bn projected sales in 2026 [32]. Despite the size of the PAC industry and its essential role in securing our physical environments, public research and development regarding PAC has been limited. While access to physical resources has been mentioned in some publications, only a few papers actually deal with the distinguishing characteristics of PAC environments such as physical access, topological space models, and physical access/movement barriers.

We distinguish between PAC and its counterpart in cyber systems, logical access control (LAC) [17]. LAC controls the access of computer users to computing resources (devices, applications, data, etc.). Analogously, PAC controls the *physical access* of *physical actors* to *physical resources or spaces*. In other words, PAC is in charge of protecting the physical attack surface compared to LAC which protects the cyber attack surface. The common characteristics of PAC and LAC allow some of the models and techniques developed for LAC to be used in the context of PAC too. For example, many access control policy models that originated in the LAC domain (e.g., role-based access control [27]) are useful in PAC systems as well. However, the physical nature of PAC systems introduces several new challenges and research opportunities. For example, PAC systems need to explicitly take into account the protected physical spaces, their relationships, and how physical barriers (as policy enforcement points) control access to them. The involvement of human actors in PAC systems (as subjects requesting physical access and as physical security personnel) also introduces new complexities in policy enforcement such as handling multiple subjects in a single access request or the possibility of being overridden by physical security personnel.

We further differentiate between PAC and approaches such as location-based access control [10, 1] and access control for IoT/Cyber-Physical Systems (CPS). Location-based access control is a family of LAC policy models that use location information to make access decisions. As mentioned above, such models can be useful in the PAC domain too. However, location-based access control models do not consider the topological connectivity of spaces and do not deal with enforcement points that control the movement of physical subjects within those spaces. Both of those properties are critical in PAC systems. In the context of access control in the IoT/CPS systems, the actors, resources, and (inter)actions under access control can both be physical and digital in nature, while in PAC they are exclusively physical. Due to their broad nature, these IoT/CPS systems can be considered extensions of PAC systems.

SACMAT '22, June 8–10, 2022, New York, NY, USA

ACM ISBN 978-1-4503-9357-7/22/06…$15.00
https://doi.org/10.1145/3532105.3535019

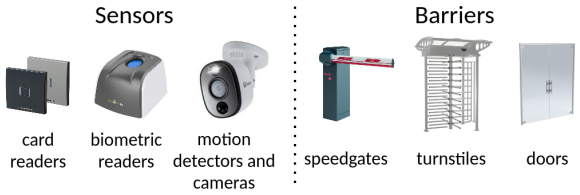

Figure 1: Example Sensors & Barriers

However, in practice and in the literature, the focus is often on digital access to cyber-physical resources, with physical actions and the complexity that the physical domain introduces only being sparsely explored. The latter aspects are the core of PAC, which we will highlight in this paper.

We believe that the barriers to entry for the access control research community into PAC systems are much higher than in cyber environments, and consequently, many unique challenges that this domain introduces are not well known. For researchers, it is easier to access, gain insight about, and develop for LAC systems than PAC systems, apart from maybe the PAC system of their respective organizations. The goal of this paper is to lower the barriers for the access control research community to explore and engage in the research opportunities in PAC systems. This paper is the result of a collaboration between academia and industry (Nedap has a track record of 40+ years producing PAC hardware and software). Informed by our joint perspectives, we present an access control architecture that captures the central concepts and processes in PAC and use that to identify the unique challenges and research opportunities in this domain. The following summarizes our specific contributions (and their organization) in this paper:

- We provide a concise background on the physical access control domain (Section 2).
- We present an architectural overview of the PAC access management and enforcement (Section 3) that identifies its key concepts and processes.
- We characterize PAC, review the related work, and identify research challenges in terms of high-level policies (Section 4), their conversion into enforcement-level policies (Section 5), policy enforcement (Section 6), and policy analysis (Section 7). Throughout these sections, research challenges and opportunities have been highlighted using *italicized* paragraph headings.

2 BACKGROUND

The concept of access control was invented soon after humanity introduced the concept of property. To protect one's property, some mechanism was needed to ensure the property could only be accessed by trustworthy subjects. Historically, these mechanisms or *barriers* varied from guards, moats, and drawbridges with secret passphrases to mechanical locks and keys. As humanity evolved through different eras, properties could belong to individuals, tribes, kingdoms, and countries. In addition to physical assets, people were also protected by building walls around castles, cities, and even countries. As a result of this wide range of applications, the field of physical access control developed a rich set of solutions in the analog domain.

2.1 History and Evolution of PAC

Evolution from a technology perspective. In the industrial age, the focus on automation and efficiency also impacted the solutions for physical protection. Mechanical devices were first replaced by electronic devices, roughly divided into *sensors* (card readers and infrared motion detectors) and *actuators* (electronic door locks and turnstiles controls). Some example sensors and barriers are shown in Figure 1. Sensors trigger actuators, which can render barriers traversable. Whereas in a mechanical lock, the keyhole (sensor) and lock (actuator) are combined into a single device, electronic solutions introduced decoupling the sensing and locking parts. This separation of the actuator (e.g., lock) from the sensor (e.g., card reader) implied the possibility of directional access control as different sensors could be placed on either side (in/out or ingress/egress) of a barrier. The evolution of electronic devices resulted in programmable electronic locks and keys, e.g., mag-stripe or contactless keycards. Once devices were connected using networks, they replaced more and more mechanical locks to reduce the burden of key management. With the advent of networked access control devices, using fine-grained temporal and spatial access rights became feasible. This led to a better balance between protection and accessibility of assets.

Evolution from a functional perspective. From a functional perspective, physical access control evolved out of the need to manage and log physical access. It started with keeping track of who was aware of the secret passphrase, then who handed a copy of mechanical keys, and finally managing who had access to what, where, when, and how. With the advent of globalization and networked systems, PAC has evolved from a local issue of protecting a single building into a global concern of governing access to international locations of organizations.

2.2 PAC Installation and Upgrade

The installation of electronic physical access control systems in buildings is quite intrusive and costly. The economics of initial investment and installation costs lead to a typical lifespan of at least 10 to 15 years. On system replacement, parts of the installation are reused whenever possible. The main drivers for mid-term system changes are stricter regulations or legislation which could lead to, for example, stricter security requirements. A key factor in the design and planning of physical access control systems is the trade-off between the use of electronic vs. mechanical locks, the latter being significantly cheaper to install but offering a lower level of convenience and flexibility. Based on our experience in the PAC industry, we estimate the ratio of mechanical to electronic locks in modern PAC installations to be approximately 4 to 1. This is especially the case in highly dynamic contexts with regular changes in key-holders.

3 OVERVIEW OF PAC ACCESS MANAGEMENT AND ENFORCEMENT

We propose the architecture in Figure 2 to capture the overall process of access management and enforcement in a PAC environment, and use it to to organize our discussions in the rest of the paper. The components that are marked with a star are distinguishing

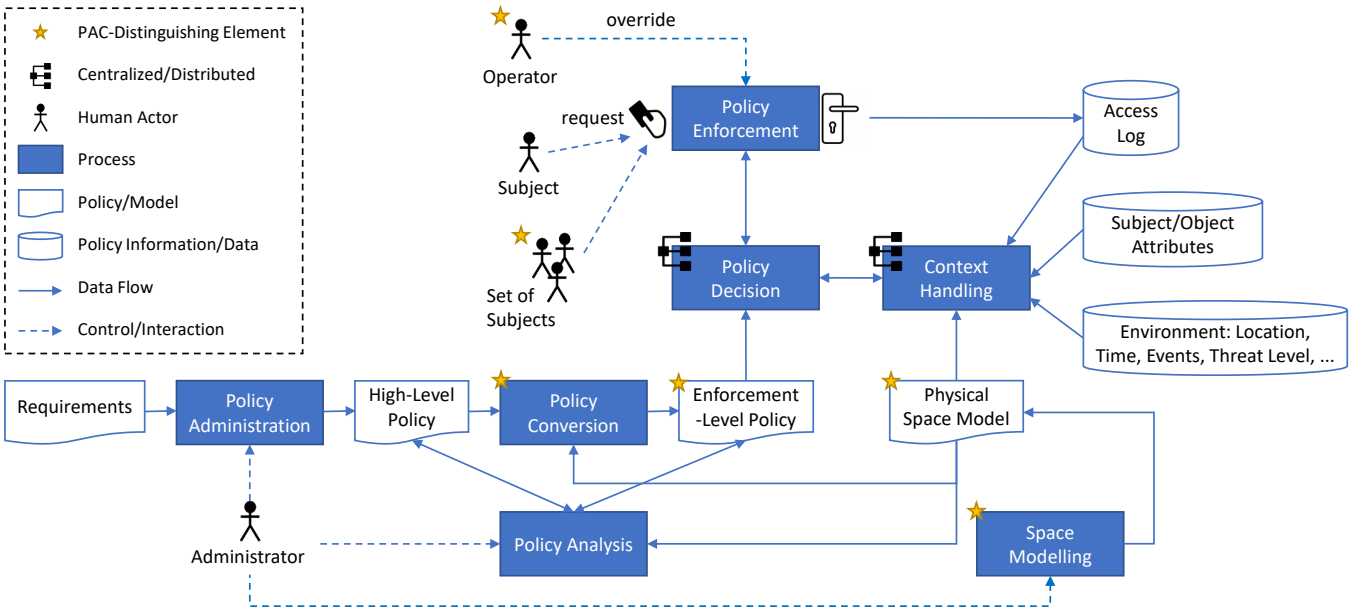

Figure 2: PAC Access Management and Enforcement

elements of a PAC architecture compared to those that are also common in a LAC architecture (e.g., see XACML [12, Section 3]).

Given the high-level business and security requirements, administrators craft a high-level physical access control policy. A key distinction of PAC policies is that they involve physical resources, spaces, and physical enforcement points. We propose a *physical space model* that is responsible for formally and comprehensively identifying those elements and their physical relationships such as placement, containment, and connectivity (reachability). This model is a key component of the architecture that is referenced and used in many other models and processes. Managing the space model is also a responsibility of administrators.

The enforcement of the high-level PAC policy in a physical environment is highly dependent on the capabilities and placements of the enforcement points. The individual *enforcement-level policy* executed by each enforcement point is based on the high-level policy, but more limited in its scope and expressiveness. We consider a *policy conversion* process that translates (preferably, in an automated fashion) the high-level policy into enforcement-level policies based on the physical space model. The access control specification and management also need to support analysis capabilities that are used to assess and improve both types of policies.

The access decisions should be made according to the applicable enforcement-level policies determined using the access request contexts. An access request context includes information such as subject/object attributes (role, clearance, etc.), environment (location, time, events, etc.), and previous access decisions. We discuss those policy information types in Section 4. Both policy decision-making and context handling could be performed centrally or in a distributed fashion. In a distributed policy decision-making approach, the enforcement-level policy needs to be distributed to the enforcement devices. Similarly, in a distributed context handling approach, data sources can be replicated locally (cached) on enforcement devices in contrast to a centralized format that depends on querying data from remote servers upon each policy decision instance. A discussion of the trade-offs of those approaches is provided in Section 6.

A notable distinction of PAC systems is that in addition to an individual subject, a set of actors could be considered as subjects in a single access request. Another interesting distinction is that the policy enforcement may be routinely overridden by operators (e.g., physical security personnel) to meet operational needs, such as temporarily allowing a guest to enter a space that is meant for personnel only or helping someone who lost/forgot their badge.

The subsequent sections will highlight the unique challenges and research opportunities from the perspective of policies and processes. Specifically, we will focus where PAC and LAC diverge the most; the high-level/enforcement-level policies, policy conversion, policy enforcement, and policy analysis.

4 HIGH-LEVEL POLICIES

PAC policies, similar to LAC policies, can rely on checking a variety of information types as part of the access request context. However, they differ in the specifics of what they take into account. Based on our industrial experience, we present the types of policy information which cover most policy information requirements for realistic PAC use-cases. Subsequently, we present research challenges and opportunities related to high-level PAC policies.

We broadly categorize the essential types of policy information into subject/object attributes, environment, and access log.

Subject/Object Attributes Examples of subject attributes include role, clearance, and organizational unit. Objects, typically protected spaces, may also have attributes such as space function and designation (e.g., office, workshop, etc.)

Environment PAC policies are often composed considering enforcement environment contexts:

Space/Location Of particular interest in a PAC system is modeling protected spaces and considering them in the context of evaluating access requests. Access control policies may use either logical locations (e.g., meeting room, lobby), or geographic locations (e.g., within a meter from a certain geo-coordinates). We emphasize that using logical locations as references to physical spaces is a better fit for PAC systems. The modeling of protected spaces in PAC often involves determining how spaces are connected and accessible from each other (topology) and how enforcement points control such accesses (e.g., physical barriers between spaces). The space model and policies may also rely on relationships between spaces, such as containment (i.e., being part of or inside) and hierarchies. For example, when a room is (contained) in a presidential suite, policies applicable to the suite may be applicable to the room as well. Hierarchies can represent an even wider range of relationships and be used to propagate policies between spaces. For example, a hierarchy can represent type-of relationships (e.g., a conference room is a meeting room), or the grouping of functional zones (e.g., by department or business unit) or physical security zones.

Time PAC authorizations are usually time-dependent. For instance, many authorizations may be valid only on workdays and during working hours. Therefore, notions such as time intervals, relative time, days of the week, repetition, and dates must be considered.

Events Additionally, scheduled events (e.g., in-house conferences or visits by VIPs) and non-scheduled events (e.g., emergency evacuations) may be taken into account by policies in a PAC system.

Other Environment Contexts PAC policies may also involve other environment contexts such as *threat level* or the *presence of operators*. In high-security facilities, such as those of banking institutions and organizations responsible for critical infrastructure, access to spaces may become more restrictive at an escalated threat level. It is also common in PAC systems to require fewer or different authorizations in the presence of operators. For example, a building lobby may become publicly accessible only when receptionists are at their posts. Such contexts and their impact on access control policies are under-explored in the literature to the best of our knowledge.

Access Log PAC may rely on previous access decisions in its evaluation of a given access request, for instance, for enforcing *anti-passback* and *anti-loitering* policies (discussed below).

We note that the enforcement-level policies as well as the policy conversion and policy analysis processes would also utilize the abovementioned policy information types. The existing access control models for LAC systems capture the abovementioned information to varying degrees by formalizing concepts such as groups, roles [27], parameterized/contextual roles [16], attributes [18, 29], location [10], time [3], contexts [4], and access history [31]. However, it is essential to develop specification models that comprehensively consider these information types. Furthermore, more comprehensive formal modeling is needed to capture and reason about information such as physical spaces that are central in PAC policies.

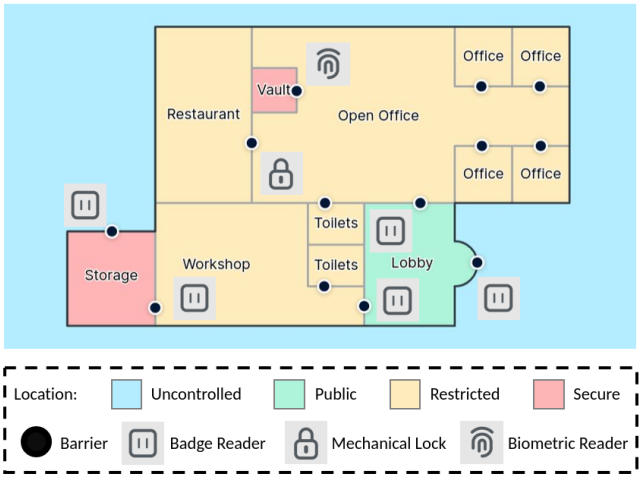

Figure 3: Example PAC Environment to Capture in Physical Space Model

Comprehensive Physical Space Models. Geographic locations, logical locations, and relationships among locations such as containment and hierarchies have been extensively explored in the RBAC literature [10, 8]. Specific to PAC systems, a research opportunity is to develop comprehensive space models that capture the topology of logical spaces and the movement of subjects and resources between them. These models should also consider physical barriers that may restrict access to the spaces and their properties such as directionality. Figure 3 illustrates the need for a physical space model in a PAC system highlighting locations, their connectivity, a grouping into security zones, barriers, and enforcement devices.

PAC-Specific Policies. We have identified a number of policies in PAC systems that are less commonly used in LAC systems and have received little attention in the literature. It is essential to develop formal specification models that are capable of incorporating these policies:

Chief-First / Visitor & Escort where authorization of an individual requires prior authorization by a higher-authority subject.

Four-Eyes where performing an action requires the authorization of two individuals for that action.

Anti-Passback where the goal is to prevent a person from improperly sharing their credentials with other parties after using them themselves. For example, an *anti-passback* policy can prevent a subject from passing a barrier that they just did.

Anti-Loitering where the goal is to put constraints on the progress of a person through a secured area such that, for example, the person may only stay for a specified amount of time in any location.

Metapolicies Handling Multi-Subject Requests. In LAC systems, high-level policies often only deal with access control requests involving a single subject. In contrast, PAC systems commonly need to authorize multiple subjects in one request either implicitly or explicitly. This is due to the practical problem that when a group of

subjects is in the proximity of a barrier, opening the barrier might allow multiple subjects to pass it. Therefore, all subjects capable of passing the barrier at the time may need to be considered in authorizing a request to open the barrier. A potential approach could be to combine policies applicable to the individual subjects involved using combining strategies such as those supported by XACML [12]. However, depending on the situation, different combining strategies might be considered. For example, a system may need to prevent opening a barrier if two subjects, one authorized and another unauthorized to open the barrier, happen to arrive at the same time at its opposite sides (i.e., using a deny-overrides strategy). In contrast, in a very similar situation, the authorized subject may need to intentionally allow an otherwise-unauthorized subject to pass the barrier, for instance, when a security guard directs a guest to a meeting space (i.e., using a permit-overrides strategy). Therefore, an interesting research direction is developing models to support context-dependent/situation-aware metapolicies for handling multiple-subject requests correctly.

5 ENFORCEMENT-LEVEL POLICIES & POLICY CONVERSION

A distinguishing characteristic of PAC environments from LAC environments is that the high-level policies in PAC need to be enforced though enforcement points which can only enforce a subset of the whole policy. This leads to two types of policies living side-by-side: high-level policies and enforcement-level policies. While the administrators capture the high-level security requirements using high-level policies, their correct system-wide enforcement relies on the enforcement-level policies which are intended for the enforcement points. Due to the different intentions of these two types of policies, they are often based on different abstractions and models. High-level policies are usually applicable system-wide (e.g., linking subjects to the physical spaces they are allowed to access because of their organizational roles). To enforce the high-level policies, they need to be converted into one or more enforcement-level policies which control individual or sets of barriers (e.g., an access list for each specific barrier). In this section, we will present open research challenges and opportunities regarding enforcement-level policies and policy conversion.

Automated Conversion from High-Level to Enforcement-Level Policies. Based on our experience, it is preferable to perform policy conversion in an automated fashion. A manual process could be highly tedious and error-prone. Tsankov et al. have proposed a *policy synthesis* framework to automatically convert a set of high-level requirements for physical spaces to enforcement-level policies [33]. In terms of high-level requirements, in addition to permission and prohibition to access a space, their framework supports expressing *blocking* (subjects cannot access space X after accessing space Y) and *waypointing* (subjects must access space X before accessing space Y) as high-level requirements. An open research opportunity is to support a richer and more diverse set of high-level policies in such a conversion framework. Starting points could be policies incorporating a more variety of information such as times constraints and events, and PAC-specific policies, as discussed in Section 4.

Modeling and Placement of Enforcement Points. To configure the policy enforcement devices, the policy conversion process needs to know how those devices work, e.g., what policy model they support, or what physical blocking mechanism they can enforce. The existing related work considers only relatively simple policy enforcement points. For instance, Tsankov et al. [33] consider door-like enforcement points capable of handling attribute-based policies. While doors are relatively simple mechanisms (letting subjects through or not), other types of barrier devices may have more complex behavior. As an example, a turnstile barrier can additionally ensure that only a single subject can pass through at a time and only in a certain direction. Elevators are another interesting category of enforcement points that may connect multiple spaces without necessarily being capable of distinguishing different flows (discussed in more detail in Section 6.3). One open research problem is formally capturing such enforcement capabilities to be considered in the conversion process. Moreover, the placement of the enforcement points in the physical space model is critical. A given high-level policy may not be enforceable based on the types and placement of the existing enforcement points. In that case, a research challenge is how to optimize updating and/or installing additional enforcement points to enforce the given high-level policies. We also envision a tradeoff research problem of suggesting to the administrators a similar-enough high-level policy to the given policy when constrained by using the existing enforcement points.

Interoperation with Proprietary Enforcement Devices. A practical challenge in the policy conversion process is the requirement to work with enforcement-level devices with varied support for policy models. Most industrial PAC hardware vendors have their own proprietary (and sometimes restrictive) policy models. Furthermore, a PAC system may contain devices from different vendors (see also the discussion on hybrid systems in Section 6.2). Attempts have been made to establish industry standards for interoperability. Most noteworthy, ONVIF, a leading standardization body for IP-based physical security products, has introduced a policy model based upon RBAC with schedules [23]. However, such standards are yet to make a significant impact in practice [32]. In the absence of a widely-supported standard policy model, an open research problem is converting high-level policies to device-specific policies while ensuring a consistent system-wide enforced policy across devices made by various vendors.

6 POLICY ENFORCEMENT

In this section, we elaborate on some of the intricacies of PAC policy enforcement in the physical domain, and introduce research challenges and opportunities that follow from this.

6.1 Psychological Acceptability

PAC systems need to enforce access control policies in the physical world, using barriers that usually, by default, block the movements of human subjects. Thus, they need to be designed according to an acceptable trade-off between security and convenience. Inconvenience and insufficient system acceptance will inevitably lead to working around or abusing the system. Examples of this are *tailgating* (multiple subjects following a leader without actually requesting access and thus not being logged), use of emergency

exits to shortcut routes, and collaboration with insiders to bypass being logged by the system.

Security and Convenience. In practice, the trade-offs between security and convenience are strongly influenced by usability and psychological acceptability. An interesting research direction is to develop frameworks for systematic consideration of usability factors and their impact on policy enforcement with the goal of reducing friction between security objectives and convenience.

6.2 Hybrid PAC Systems

Despite the many benefits that electronic access control systems have over mechanical "lock and key" systems, in practice, most organizations maintain a combination of electronic and mechanical locks, i.e., a hybrid PAC system. Technical and financial constraints in combination with expected usage and availability will determine the mix of different locks. Flexibility, logging, and turnaround time for policy updates are better in the case of an electronic lock. For example, a lost badge can be blocked instantly and remotely, whilst losing a mechanical key will require the replacement of all keys and the corresponding lock cylinder. Similarly, an access control policy can be updated in an electronic locking device instantaneously, provided the network is operational, while issuing or withdrawing a physical key will require the physical transfer of the key. The main benefit of mechanical locks is that they are much cheaper. To bridge the gap between online and offline (mechanical) access control systems, manufacturers have come up with creative mixes:

Network on Card which involves re-writable access cards, used to transport access policies, blacklists, and access logs between the locks and the management system [24]. Subjects need to update their cards daily at an updating device that reads the access log and battery states of the locks the subject has visited the previous day. In the same session, the actual access control policy and blacklist are written to the card. The locks are configured at installation with a lock policy and a unique ID which is referenced in the policies. Due to limitations of both lock and card storage memory, power consumption, and the card read/write times, the access control policies in these systems are very basic.

Key Cabinets which are access-controlled cabinets in which tagged physical keys are stored. A subject can open the cabinet and release the key(s) assigned to her. Removing and returning the keys is recorded in the access log, and access to the cabinet is managed from the PAC system. Advanced setups in which the return of the key is a prerequisite to leaving a site are used to relieve the problem of missing keys. This type of setup is typically used for service engineers who need to do their maintenance jobs in technical areas in buildings outside of office hours, i.e., without the presence of a receptionist or guard.

Policies for Hybrid Systems. To the best of our knowledge, formal high- and enforcement-level policy models capable of supporting hybrid PAC systems have not been developed and studied in the literature. This prevents holistic policy design and analysis of the mechanical and electronic subsystems. As a follow-up research opportunity it is interesting to explore using high-level policies for automated generation of configuration instructions for manually-managed components of hybrid PAC systems.

6.3 Elevators

Modern multi-floor buildings have elevators in addition to stairs. In confined contexts such as multi-tenant office buildings or high-security sites with many security zones, a rich set of elevator access control policies may be implemented. Most suppliers of high-end elevators provide an API to their elevator controller through which the following components can be controlled from a PAC system:

Floor Topology which defines and names the different destination floors which can be reached by a specific elevator carriage.

User-Interface Elements such as devices for calling the elevator, choosing the destination, or selecting the fastest elevator.

Carriage Control which designates the specific use of the carriage, e.g., transport of goods, emergency use, or VIPs. Depending on the building setup, the carriage may have a front and rear entry or be part of a so-called double-deck setup in which the lower carriage handles only the bottom half of a high-rise building.

From a policy administration perspective, the definition of elevator access control policies is a tedious task. But, from an enforcement perspective, the situation is more complicated. Since an elevator carriage is typically used by multiple subjects in a single ride, tailgaters and free riders are hard to prevent. As a result, subjects can easily end up in destinations to which they should have been denied access. This poses security risks but also risks of subjects getting trapped. To overcome this, additional enforcement on critical destinations could be added, with a penalty of increased complexity and cost.

Elevators as Moving Spaces. Research is needed to formulate a comprehensive model of elevators from a PAC perspective. Elevator carriages can be modeled as moving access-controlled spaces which are connected to fixed spaces on floors or as transportation mechanisms that are not access-controlled. Such a model is currently missing but required for proper policy design and policy analysis for PAC systems with elevators.

6.4 Authentication Factors

From a security perspective, anonymous users should be prevented whenever possible [26]. In the context of PAC, this implies that subjects should be uniquely identifiable. Although this raises a serious privacy concern, in industrial PAC, more so than LAC, the legal traceability requirement of individual subjects overrides privacy considerations. This poses the practical problem of proving that a subject actually "has used" her access for herself, for someone else, or maybe not at all. Additionally, subjects could tailgate other subjects if no anti-tailgaiting protection is in place. As an example, a basic authentication policy on what the subject "has", e.g., some token such as a keycard, does not enforce that the subject's identity matches that of the token owner because it could be a borrowed or stolen keycard. This renders the access log less reliable for *forensic research*, i.e., legal investigations into a subject's movements. A multi-factor authentication policy using biometric attributes in the enforcement point is the most reliable solution in this respect.

Forensic Readiness. The reliability of access logs for use in forensic research offers an interesting challenge for further research. Analyzing PAC access control policies prior to their deployment in

terms of completeness and correctness of logging and distinguishing accesses can offer great benefits to forensic researchers because they can rely on a known quality of service.

6.5 Transactional Physical Access

Elaborating further on the accurate logging of accesses in PAC systems, it is important to distinguish between *access granted* and *access used*. While this distinction is often not made in LAC systems, it is quite relevant in PAC systems to know if a granted access decision actually results in a physical movement. Consider a subject entering a building using a turnstile at the entrance. After authentication, access is granted. But, only if the subject actually enters the turnstile and exits after a 180-degree rotation of the turning mechanism, access is used. The steps from authenticating, entering the turnstile, rotating, and leaving the turnstile can be seen as *transactional physical access*. If the rotation is not completed, the transaction is aborted and should not be logged in as completed access. In this example, the physical enforcement device setup has the capability of ensuring the validity of the transaction. In a more common situation in which a speed-gate, a sliding door, or a regular door is used with single-factor authentication, we can only assume that the physical access transaction took place unless we have other evidence for corroboration, e.g., footage from a video camera with face recognition. These examples show the intricacies of physical access and the impact of human behavior on the quality of the access log.

Formalizing Transactional Physical Access. Further research is needed to formalize the concept of transactional physical access and study its impact on PAC. A possible outcome is a probabilistic model for describing the quality and reliability of access logs. Use-cases for such a formal model are forensics, access decisions based on prior accesses, and anomaly detection.

6.6 Centralized vs. Distributed Decision-Making

Without generalizing, our experience leads us to the insight that LAC tends towards a more centralized decision-making approach whereas PAC tends towards a decentralized architecture. Good industry practice in physical access is to allow a maximum response time of three seconds between requesting access and activating the lock. If this delay is exceeded, experience shows that subjects get irritated, which potentially leads to damage to equipment, productivity loss, reduced user acceptance, and subsequently a system defect. Therefore, the access decision needs to be made instantly and near real-time as the access request is made. This poses a trade-off between a centralized versus a distributed (local to the enforcement point) decision point. To guarantee correct system behavior, in which the decision points evaluate policies according to the latest policy information, consistency must be guaranteed on all distributed devices. This concerns the ordering of messages, time synchronization of all involved devices, and storing irrefutable evidence of changes and access requests. In high-impact situations, PAC is mission critical and a distributed architecture with redundant information for the evaluation of the access decision must be designed. An example showing the consequence of not taking into account this redundancy is the total office lockout of Facebook's personnel as the result of their network failure [22]. Depending on the complexity of the policy specification model and non-functional requirements such as encryption, the computing power at the end-points needs to be scaled accordingly. The trade-off will also involve a cost assessment as scaling up compute resources at all end-points could lead to prohibitively high project and installation costs. The architectural design of a PAC system involves many trade-offs between different cross-cutting concerns.

Methodology for Design of Optimal PAC Architecture. Designing the optimal system architecture involves many trade-offs. As we have discussed above, PAC tends towards a distributed architecture. There is a research opportunity in developing methodologies for the systematic design of optimal PAC architecture considering the trade-offs.

6.7 Fault Tolerance

The configuration and installation of electronic barriers must meet specific safety requirements in their security policies. The following policies for failures of power, network, or sabotage are used in practice:

Fail-Close where the barrier will remain in a locked state upon failure. Depending on the type of barrier, a mechanical/manual override may be implemented.

Fail-Open where the barrier will unlock and remain open on failure.

Fail-Safe which is a more general mode used to describe a degradation of service on failure. In this mode, safety requirements should override security requirements. For instance, human subjects should not get locked in as a result of network failure.

Handling failure modes can sometimes be managed at a system-wide level. But, it is mostly context-dependent and should therefore be considered individually for each barrier.

Global Effects of Local Failures. Local failures of barriers can have global impacts in a PAC system. A research challenge is to systematically study the global effects of local failures using "what-if" scenarios. If high-impact failures can be pinpointed in the design phase, appropriate measures like adding redundant components or creating alternative routes can be introduced to mitigate the involved risks at an early stage. Another use-case is taking into account the failure constraints and modeling the impact of local fault situations in the policy conversion process from high-level to enforcement-level policies.

7 POLICY ANALYSIS

Analysis of access control policies is crucial to support policy creation and evolution. Unlike policy analysis in the LAC domain [19, 20, 11], research regarding analysis of PAC policies is sparse. PAC introduces new domain-specific information, processes, and constraints. Therefore, the policy properties and characteristics depending on the newly introduced policy constructs cannot be evaluated using policy analysis techniques for LAC. To illustrate, this would include checking reachability-related constraints or constraints depending on the past and current location of subjects and resources.

In this section, we survey existing work on PAC policy analysis and present what are, in our opinion, notable research opportunities. Our discussion is based on the policy information requirements

Table 1: Comparison of Existing Work on PAC Policy Analysis

#	Authors	Year	Base Model	Security Domain		Policy Information										Policy Analysis Goal								Analysis Method
						Locations		Topology			Time					Quality					Design & Org.			
				Cyber	Physical	Logical	Geo	Connectivity	Containment	Hierarchy	Interval	Relative	Events	Contexts	Access Log	Consistency	Minimality	Relevance	Completeness	Correctness	Change Imp.	Similarity	Structure	
1	Cao et al. [6]	2022	ABAC	●	●	●	○	●	●	○	○	○	○	○	◐[1]	○	○	○	○	●	○	○	●[2]	Bigraphs & BRS
2	van der Laan [38]	2021	RBAC	○	●	●	○	●	○	●	●	○	○	○	○	○	○	○	○	●	●	○	●	EMF+VQL
3	Cao. et al. [5]	2020	RBAC	●	●	●	○	●	●	○	○	○	○	○	◐[1]	○	○	○	○	●	○	○	○	Bigraphs & BRS
4	Pasquale et al. [25]	2017	RBAC	●	●	●	◐[3]	●	●	○	○	○	○	○	○	○	○	○	○	●	○	○	○	Graph Alg.
5	Ben Fadhel et al. [2]	2016	RBAC	●	●	●	●	○	○	○	●	●	○	○	○	○	○	○	○	●	○	○	○	EMF+OCL
6	Tsigkanos et al. [34]	2015	-	●	●	●	○	●	●	○	○	○	○	○	◐[1]	○	○	○	○	●	○	○	●[2]	Bigraphs & BRS
7	Tsigkanos et al. [35]	2014	-	○	●	●	○	●	●	○	○	○	○	○	◐[1]	○	○	○	○	●	○	○	●[2]	Ambient Calc.
8	Turkmen et al. [36]	2013	GBAC[4]	○	●	◐[5]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	●[2]	SAT
9	Fitzgerald et al. [13]	2012	GBAC[4]	○	●	●	○	●	○	○	○	○	○	○	○	●	●	○	●	●	○	○	●	SAT
10	Skandhakumar et al. [30]	2012	RABAC	○	●	●	◐[3]	●	○	●	●	●	○	●	●	●	○	○	○	●	○	○	●	EMF
11	Frohardt et al. [15]	2011	-	○	●	●	○	●	●	○	●	○	○	○	○	○	○	○	○	●	○	○	○	Access Nets

[1]: Only latest location of subjects and/or resources are kept. [2]: As so far to fix detected policy quality issues. [3]: Using BIM models (only used to determine logical locations and topological information). [4]: Group-based access control [13]. [5]: Access given to doorsides

presented in Section 4 and the policy analysis goals presented by Jabal et al. [19].

7.1 Background: Policy Analysis Goals

Here, we briefly review the main goals of policy analysis as classified by Jabal et al. [19]: verifying a set of quality requirements and supporting policy design and organization.

7.1.1 Assessment of Policy Quality. The following major policy quality requirements can be distinguished for a set of policies [19]. We note that the set of rules in a policy can be considered as *a set of policies* enforced together.

Consistency the set of policies does not include policies that contradict each other.

Minimality the set of policies does not include redundant policies.

Relevance the set of policies does not contain policies that do not apply to any action executed by the users.

Completeness all actions executed in the domain controlled by a policy-based system are covered by some policies.

Correctness the policies are free of faults and compliant with their intended goals and system requirements.

We add that requirements such as minimality are not always strictly desirable. To illustrate, in the case of RBAC, even though two roles might have identical permissions, they might represent different organizational roles. Thus, merging them into a single functional role could be considered undesirable.

7.1.2 Policy Design and Organization. The process of designing and organizing policies can be supported through various types of analyses [19]:

Change Impact Analysis assesses and evaluates a change to a single policy or a collection of policies. This analysis identifies potential consequences and helps to estimate associated risks.

Similarity Analysis performs comparisons among two or more policies. Specifically, it checks for different relationships among policies such as equivalences, possible refinements, redundancies, and conflicts. This analysis is important in tasks such as policy integration and policy version control.

Policy (Set) Structure Analysis analyzes the structure of a single or a collection of policies. This analysis can facilitate tasks such as policy refactoring and maintaining an optimal policy structure.

7.2 Existing Work

We present an overview and comparison of the existing work on PAC policy analysis in Table 1. We compare them in terms of policy information (discussed in Section 4), policy analysis goals (discussed in Section 7.1), and analysis methods (discussed below). We also summarize and discuss their contributions below.

7.2.1 Analysis Goals. Noteworthy, most of the existing works [6, 38, 5, 25, 2, 34, 35, 37, 15] focus on verifying policy correctness by checking various structural, spatial, and/or temporal properties. Some of these works also facilitate policy structural analysis by presenting techniques to propose [6, 34] or perform [35] policy adjustments to prevent and/or cure violations. Turkmen et al. deal with discovering conflicting policy rules and proposing policy adjustments to resolve conflicts [36]. Fitzgerald et al. present how to perform anomaly analysis and check various properties dealing with policy consistency, minimality, completeness, correctness, and the general structure of the high-level policy & physical space model [13]. Skandhakumar et al. present analytical techniques to support policy administration [30].

7.2.2 Policy Information and Specification. Most of the models are based on RBAC. Based on our experience, we believe this trend is due to organizational roles being a natural way to group access

to spaces in an organization-based context. The support for topological information varies. Only a few analysis techniques support time-, event- and/or context-dependent access control. This is problematic since usually real-world PAC policies have time-dependent authorizations and most PAC policies need to support (implicit) event/context-dependent constraints. Arguably, most of the existing work only partially supports access logs in so far that they keep track of the current run-time location of subjects and/or resources and disregard previous locations. None of the presented work takes administrative policies into account.

7.2.3 Analysis Methods. Various techniques and formalisms have been used to perform policy analysis in PAC systems, as shown in Table 1. We briefly elaborate on the lesser-known methods. The Eclipse Modeling Framework [1] (EMF) is a modeling framework and code generation facility for building applications based upon structured data models. With a model specified using the Ecore modeling language, EMF can produce a basic editor and a set of Java classes for the model, along with a set of adapter classes that enable viewing and editing of the model. The Object Constraint Language [2] (OCL) is an expressive and flexible declarative language that can describe rules that can be checked against models made with EMF. The Viatra Query Language [3] (VQL) is a datalog-based language comparable to OCL. Its main advantage over OCL is that it allows expressions to be recomputed incrementally. Access Nets are a Petri-Net-like formalism where tokens are used to model persons and transitions capture the movement of persons from one place to another. Ambient calculus is a process calculus used to model concurrent systems that include mobility [7]. Noteworthy is the move of Tsigkanos et al. [35] from ambient calculus to bigraphs and bigraph reactive systems (BRSs) [21] to verify policy correctness [34], a formalism that has also been used by Cao et al. [6, 5]. Bigraphs combines the advantage of π-calculus and ambient calculus, considering both linking and hierarchical structure [5]. Bigraphs can model the locations of entities (nested relationships represented by the *place graph*) which can form connections with each other (represented by the *link graph* - a hypergraph). Together with reaction rules, they form BRSs. Bigraphs and BRSs have been frequently used to model and analyze cyber-physical systems.

7.3 Research Opportunities

Beyond Policy Correctness. A major research opportunity lies in further exploring policy analysis beyond just policy correctness. Based on our review of related work, analyzing consistency, minimality, relevance, completeness, and overall structure of PAC policies has received little attention. The same holds for analyzing the impact of changes. We have found no research addressing how to perform similarity analyses for PAC policies.

To illustrate some opportunities, we note that guarantees regarding consistency and completeness would help ensure a basic level of policy correctness. Arguably, however, it might be better to guarantee these by design instead of through analysis (e.g., through a deny-first policy). Analyzing policy minimality and optimizing policy structure could help during policy refactoring. This is a notably difficult task as PAC systems evolve and grow from their original design. To limit business disturbance, organizations tend to over-entitle organizational roles and employees as time passes and not remove obsolete permissions. Fifty to ninety percent of employees are over-entitled in large organizations [28]. Moreover, being able to analyze the impact of changes would help in policy refactoring, day-to-day policy administration (e.g., assigning/removing permissions), and understanding the impact of new requirements on the high-level policies (e.g., new rules and regulations). Policy similarity analysis could help when an organization needs to compare or integrate multiple high-level policies. A situation where this need arises is during company mergers or acquisitions. Furthermore, when one crafts a policy from scratch, it would be helpful to detect missing permissions compared to the prior policies.

Supporting Complexity of Real-World Policies. The applicability of the existing analysis techniques to real-world PAC use-cases is often limited as they cannot take policies with time, context, and event-dependent constraints into account. Research is needed in developing techniques with more comprehensive support of various policy information types.

Incremental Analysis. Most of the existing solutions for PAC policy analysis (as well as for LAC) have not been designed to analyze evolving policies [38]. For example, all policy verifiers surveyed by us here and by Jabal et al. [19] analyze policies in their entirety (with one exception [38]). In practice, this means that after each small change the whole analysis has to be redone. This is often unnecessary and highly inefficient when dealing with evolving policies, especially considering the complexity of high-level policies and the scale of enforcement-level policies in PAC. An incremental policy analysis approach [38] can reuse intermediary computations and results from previous analysis attempts. This would limit the set of computations to redo, the properties to recheck, and/or the set of access control entities to reconsider upon a change - all in all resulting in significant improvement in analysis speed in the real world.

8 CONCLUSION

In this paper, we characterized physical access control (PAC) systems. With the help of our proposed PAC architecture, we captured the key concepts and processes in these systems and discussed research challenges and opportunities within them.

While the PAC domain has been the focus of this paper, several of the proposed research directions are generalizable to other access control domains. For instance, the concept of automated policy conversion and modeling of the enforcement points as part of the policy design process is applicable in other domains with distributed policy enforcement, especially when using heterogeneous mechanisms. Beyond pursuing the discussed research opportunities, as future work, we intend to compile a set of guidelines to help with the evaluation of the research on PAC systems based on real-world use-cases. We hope that our discussions in this paper pave the way for flourishing research interest in the PAC domain, and would welcome further discussion and engagement with the community.

[1] https://www.eclipse.org/modeling/emf/
[2] https://projects.eclipse.org/projects/modeling.mdt.ocl
[3] https://www.eclipse.org/viatra/

ACKNOWLEDGMENTS

We thank Daphne Yao and anonymous reviewers for their valuable feedback that helped us improve this work.

REFERENCES

[1] C. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati. Access Control in Location-Based Services. In *Privacy in Location-Based Applications*, pages 106–126. 2009.

[2] A. Ben Fadhel, D. Bianculli, L. Briand, and B. Hourte. A Model-driven Approach to Representing and Checking RBAC Contextual Policies. In *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, CODASPY '16, pages 243–253, 2016.

[3] E. Bertino, P. A. Bonatti, and E. Ferrari. TRBAC: A temporal role-based access control model. *ACM Trans. Inf. Syst. Secur.*, 4(3):191–233, 2001.

[4] R. Bhatti, E. Bertino, and A. Ghafoor. A Trust-Based Context-Aware Access Control Model for Web-Services. *Distributed and Parallel Databases*, 18(1):83–105, 2005.

[5] Y. Cao, Z. Huang, Y. Yu, C. Ke, and Z. Wang. A topology and risk-aware access control framework for cyber-physical space. *Frontiers of Computer Science*, 14(4):144805, 2020.

[6] Y. Cao, Y. Ping, S. Tao, Y. Chen, and Y. Zhu. Specification and adaptive verification of access control policy for cyber-physical-social spaces. *Computers & Security*, 114:102579, 2022.

[7] L. Cardelli and A. D. Gordon. Types for mobile ambients. In *Proceedings of the 26th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '99, pages 79–92, 1999.

[8] S. M. Chandran and J. B. D. Joshi. LoT-RBAC: A Location and Time-Based RBAC Model. In A. H. H. Ngu, M. Kitsuregawa, E. J. Neuhold, J.-Y. Chung, and Q. Z. Sheng, editors, *Web Information Systems Engineering – WISE 2005*, LNCS, pages 361–375, 2005.

[9] R. B. CHS-III PSP. Fixing the gaps in your PACS. Security Info Watch. 2017. URL: https://www.securityinfowatch.com/access-identity/article/12293604/fixing-the-gaps-in-your-pacs.

[10] M. L. Damiani, E. Bertino, B. Catania, and P. Perlasca. GEO-RBAC: A spatially aware RBAC. *ACM Trans. Inf. Syst. Secur.*, 10(1), 2007.

[11] A. Datta, S. Jha, N. Li, D. Melski, and T. Reps. Analysis Techniques for Information Security. *Synthesis Lectures on Information Security, Privacy, and Trust*, 2(1):1–164, 2010.

[12] eXtensible Access Control Markup Language (XACML) Version 3.0 Plus Errata 01, OASIS, 2017. URL: http://docs.oasis-open.org/xacml/3.0/errata01/os/xacml-3.0-core-spec-errata01-os-complete.pdf.

[13] W. M. Fitzgerald, F. Turkmen, S. N. Foley, and B. O'Sullivan. Anomaly analysis for Physical Access Control security configuration. In 7th International Conference on Risks and Security of Internet and Systems (CRiSIS), pages 1–8, 2012.

[14] Flight Systems Stolen From Arik Air Boeing 737. Simple Flying. 2022. URL: https://simpleflying.com/arik-air-737-system-theft/.

[15] R. Frohardt, B. E. Chang, and S. Sankaranarayanan. Access Nets: Modeling Access to Physical Spaces. In *VMCAI*, 2011.

[16] M. Ge and S. L. Osborn. A design for parameterized roles. In C. Farkas and P. Samarati, editors. IFIP TC11/WG11.3 Eighteenth Annual Conference on Data and Applications Security, pages 251–264, 2004.

[17] Glossary of Key Information Security Terms. Glossary NISTIR 7298 Rev. 3, NIST. URL: https://csrc.nist.gov/glossary/term/lacs.

[18] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST SP 800-162, National Institute of Standards and Technology, 2014. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf.

[19] A. A. Jabal, M. Davari, E. Bertino, C. Makaya, S. Calo, D. Verma, A. Russo, and C. Williams. Methods and Tools for Policy Analysis. *ACM Computing Surveys*, 51(6):121:1–121:35, 2019.

[20] D. Lin, P. Rao, E. Bertino, N. Li, and J. Lobo. EXAM: a comprehensive environment for the analysis of access control policies. *Intl. Journal of Information Security*, 9(4):253–273, 2010.

[21] R. Milner. *The Space and Motion of Communicating Agents*. 2009. 215 pages.

[22] J. Newman and K. Griffith. Facebook's WFH policy made 7-hour outage worse. Daily Mail. 2021. URL: https://www.dailymail.co.uk/news/article-10060447/WFH-Facebooks-outage-worse-75-60-000-workforce-not-office-fix-it.html.

[23] ONVIF™ Access Rules Service Specification, ONVIF: Open Network Video Interface Forum Inc., 2019. URL: http://www.onvif.org/specs/srv/access/ONVIF-AccessRules-Service-Spec.pdf.

[24] OSS Standard Offline (OSS-SO). OSS-Association. URL: https://www.oss-association.com/en/oss-association/oss-standards/oss-standard-offline-application/.

[25] L. Pasquale, C. Ghezzi, E. Pasi, C. Tsigkanos, M. Boubekeur, B. Florentino-Liano, T. Hadzic, and B. Nuseibeh. Topology-Aware Access Control of Smart Spaces. *Computer*, 50(7):54–63, 2017.

[26] J. Saltzer and M. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, 1975.

[27] R. S. Sandhu, E. J. E. Coyne, H. L. Feinstein, and C. E. C. Youman. Role-based access control models. *Computer*, 29(2):38–47, 1996.

[28] B. Schneier. Essays: Is Perfect Access Control Possible? - Schneier on Security. URL: https://www.schneier.com/essays/archives/2009/09/is_perfect_access_co.html.

[29] D. Servos and S. L. Osborn. Current Research and Open Problems in Attribute-Based Access Control. *ACM Comput. Surv.*, 49(4):65:1–65:45, 2017.

[30] N. Skandhakumar, F. Salim, J. Reid, and E. Dawson. Physical Access Control Administration Using Building Information Models. In *Cyberspace Safety and Security*, volume 7672, pages 236–250, 2012.

[31] L. Tandon, P. W. L. Fong, and R. Safavi-Naini. HCAP: A History-Based Capability System for IoT Devices. In *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, SACMAT '18, pages 247–258, 2018.

[32] The Physical Security Business 2021 to 2026 - Access Control, Video Surveillance & Intruder Alarm / Perimeter Protection Research, Meemoori Research AB, 2021-Q4.

[33] P. Tsankov, M. Dashti, and D. Basin. Access Control Synthesis for Physical Spaces. *29th IEEE Computer Security Foundations Symposium (CSF)*, 2016.

[34] C. Tsigkanos, L. Pasquale, C. Ghezzi, and B. Nuseibeh. Ariadne: Topology Aware Adaptive Security for Cyber-Physical Systems. *37th IEEE International Conference on Software Engineering*, 2015.

[35] C. Tsigkanos, L. Pasquale, C. Menghi, C. Ghezzi, and B. Nuseibeh. Engineering topology aware adaptive security: Preventing requirements violations at runtime. In *22nd IEEE International Requirements Engineering Conference (RE)*, pages 203–212, 2014.

[36] F. Turkmen, S. Foley, B. O'Sullivan, W. Fitzgerald, T. Hadzic, S. Basagiannis, and M. Boubekeur. Explanations and Relaxations for Policy Conflicts in Physical Access Control. In *Proc. 25th IEEE International Conference on Tools with Artificial Intelligence*, ICTAI '13, pages 330–336, 2013.

[37] D. Unal and M. U. Caglayan. A formal role-based access control model for security policies in multi-domain mobile networks. *Computer Networks*, 57(1):330–350, 2013.

[38] J. van der Laan. *Incremental Verification of Physical Access Control Systems*, University of Twente, 2021. URL: http://essay.utwente.nl/85634/3/Laan_MA_EEMCS.pdf.