

# Behind Closed Doors: Let's PLAI

**Mohammad Soleimani**, *Kastle Systems*

**Tim Weil**, *DMI*

**Ed Coyne**, *RBAC consultant*

**W**ithin the realm of corporate security and access control, physical security is often considered separate from logical security. The tools used to safeguard physical assets such as buildings and equipment are typically different from those that safeguard logical assets such as data and software. However, recent developments in cyber-physical security systems have demonstrated the ability to integrate physical access control systems (PACS) and logical access control systems (LACS) with resulting advantages. This integration can be facilitated by combining the technology of identity devices (for example, smart cards, biometric scanners, and mobile devices), PACS equipment (readers, doors, gates, and so on), and IT management systems deploying LACS solutions. An industry alliance of cyber-physical security companies, the Physical-Logical Security Interoperability Alliance (PSIA; <http://psialliance.org>), has described the convergence of PACS/LACS as filling a long-standing requirement in the IT industry:

The benefits of the PSIA specification will include more efficient management of identities without altering the existing logical identity ecosystem, and delivery of an overall lower cost structure, making it easier to develop and articulate a more compelling ROI. More specifically, logical identities and roles could be imported and mapped in a physical security ecosystem without removing the value and features that a physical security solution provides to manage devices in the physical security domain.<sup>1</sup>

Here, we examine the PSIA Physical-Logical Access Interoperability (PLAI) specification,<sup>2</sup> which combines enhanced features of physical security, role-based access control (RBAC), and attribute-based access control to provide facilities management “behind closed doors.” The PLAI specification includes both lightweight directory access (LDAP) for directory information services and RBAC methods<sup>3</sup> to provide distributed access rights to physical control systems managed at the enterprise level. The RBAC approach

realized in the PLAI model builds on the 2012 ANSI standard known as RBAC Policy Enhanced (RBAC-RPE),<sup>4</sup> which provides real-time, policy-based access control decisions implemented by the mechanisms of dynamic constraints and attribute control. We also discuss RBAC-AE (attribute-enhanced), an enhancement of RBAC-RPE that will allow further restriction to physical security devices based on permission granted by personal and situational attributes.

## RBAC and ABAC Models

In RBAC, roles are sets of permissions, and users are assigned to roles. Users don't have direct access to resources as they would with basic mechanisms such as access control lists, which are attached to resources. Instead, they can access only resources that are allowed under their role, possibly with additional constraints. In attribute-based access control (ABAC), attributes such as age, clearance level, location, or other user characteristics are used in determining access. Rules must be defined that grant access, and ABAC policy enforcement mechanisms are required to modify

**Table 1. Taxonomy of options for integrating attributes with RBAC.**

Option	U	R	A	Model	Permission mapping
1	0	0	1	ABAC-basic	$A_1, \dots, A_n \rightarrow \text{perm}$
3	0	1	1	ABAC-RBAC hybrid	$R, A_1, \dots, A_n \rightarrow \text{perm}$
4	1	0	0	ACLs	$U \rightarrow \text{perm}$
5	1	0	1	ABAC-ID	$U, A_1, \dots, A_n \rightarrow \text{perm}$
6	1	1	0	RBAC-basic	$U \rightarrow R \rightarrow \text{perm}$
7	1	1	1	RBAC-A, dynamic roles	$U, A_1, \dots, A_n \rightarrow R \rightarrow \text{perm}$
8	1	1	1	RBAC-A, attribute-centric	$U, R, A_1, \dots, A_n \rightarrow \text{perm}$
9	1	1	1	RBAC-A, role-centric	$U \rightarrow R \rightarrow A_1, \dots, A_n \rightarrow \text{perm}$

\*U = user/subject ID; R = role; A = attributes. RBAC: role-based access control; ABAC: attribute-based access control; ACL: access control list

access control permissions in a dynamic environment.

Recent trends in identity management (IdM) have provided a significant amount of literature, standards, and products that have utilized both role- and attribute-based solutions to protect enterprise systems and information. Although it's beyond this article's scope to provide a broad survey of the solutions these technologies offer, an objective approach is provided in the IdM literature.<sup>5-8</sup> Emerging standards and guidance have been provided by the 2012 updates to the ANSI RBAC standards,<sup>4</sup> and by the US National Institute of Standards and Technology (NIST)'s recently issued special publication 800-162,<sup>9</sup> which has gained significant momentum in the federal sector.

The PLAI specification builds on the RBAC and ABAC solutions proposed in "Adding Attributes to Role-Based Access Control."<sup>5</sup> In this paper, three options (RBAC-A) are described to handle the relationship between roles and attributes. These options all retain some of the administrative and user permission review advantages of RBAC, while allowing the access control system to work in a rapidly

changing environment. Dynamic Roles, Attribute-Centric Roles, and the Role-Centric approach were considered for adoption by the PLAI specification. These options (7-9) are shown in Table 1 and described elsewhere.<sup>5</sup>

### The PLAI Implementation of RBAC-RPE

RBAC-RPE provides a standards-based approach to defining the business roles of employees within an organization. Once functional roles are defined, each role is then assigned logical (applications and data) and physical access privileges (or policies). The PLAI specification augments physical security functionality by providing a mechanism for greater connectivity between both logical and physical domains, and a standardized, more efficient mechanism for physical security administration through the use of PLAI agents.

Figure 1 shows how roles utilized in the logical security domain can be integrated with the physical security domain to create synchronicity between domains.

We introduce the concept of RBAC-AE authorization decisions. Although RBAC-RPE can effectively address suspension of selective role-to-permission relationships based on situational attributes that

generally affect a group of people—for example, threat level, access schedules, and so on—the RBAC-AE extension further facilitates the use of personal attributes to directly suspend specific permissions, and it's well-suited for adoption by PLAI.

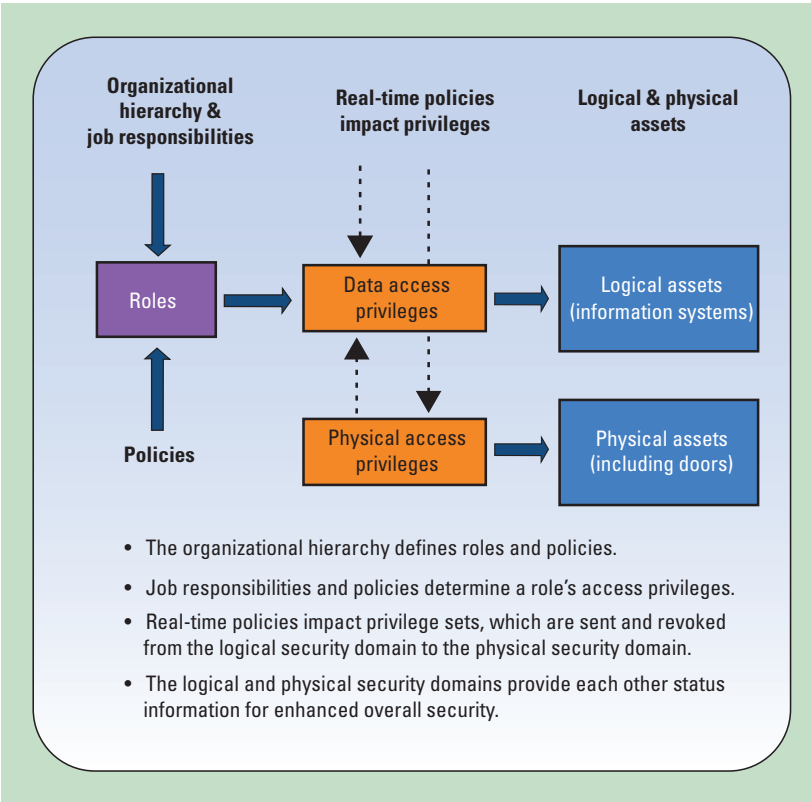
With the RBAC-AE approach, attribute types can be split as follows:

- Attributes associated with the person for whom we are determining access—for example, clearance, person's location, or citizenship. As implemented in PLAI, these attributes come from LDAP for each identity.
- Other (situation-based) attributes—for example, threat level, location of other people, or alarm conditions.

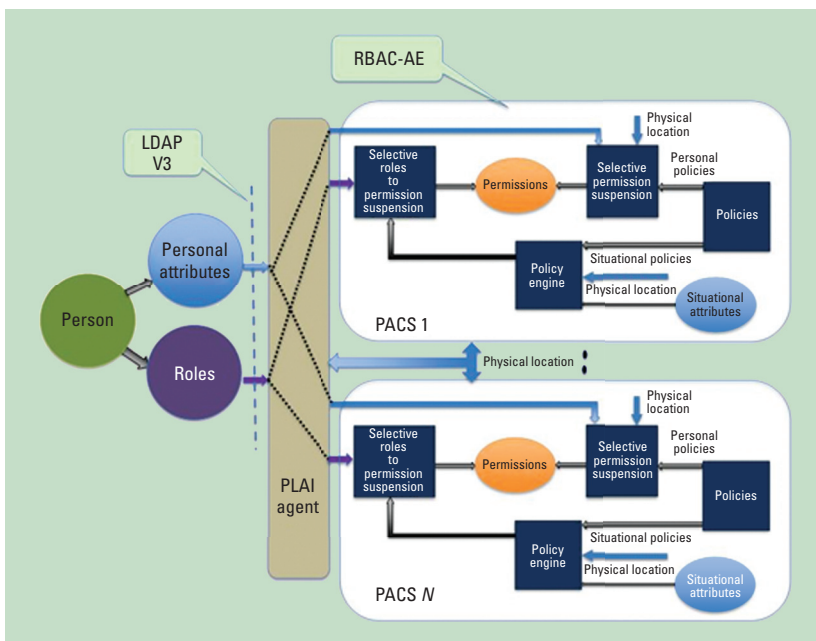
Similarly, policies can be split into two types:

- Policies that apply to personal attributes (no access to labs without valid clearance).
- Policies that apply to situational attributes (for example, the removal of critical access during high threat levels or no roof access during holidays).

Figure 2 shows how roles in the RBAC-AE model specify all the



**Figure 1. Physical or logical access interoperability.** Roles utilized in the logical security domain can be integrated with the physical security domain to create synchronicity between domains.



**Figure 2. Physical-Logical Access Interoperability (PLAI) and RBAC-AE (role-based access control attribute enhanced).** Roles in the RBAC-AE model specify all the permissions a person may have.

permissions a person *may* have (scope). User roles are augmented by two policy engines:


- One that applies to personal attributes and policies. This engine does not add to the scope of the permissions that a person has, but only limits them by suspending access to a set of permissions for that person.
- One that applies to the situational attributes and policies. This engine does not add to the scope of the permissions that the roles have, but only limits them by suspending the access rights of a role to a set of permissions.

## Cyber-Physical Security and the Internet of Things

At the intersection of cyber-physical security and the Internet of Things (IoT), access control systems present an opportunity for innovation to expand established practices and products prevalent in the physical security controls market with the ubiquity of device management technologies emerging from the rapid growth in IoT control systems. Access control components (identity devices, biometrics, credential management, logical systems, or physical systems) offer a broad range of tools and devices that must be controlled in the dynamically changing conditions represented in the IoT domain.

The PLAI specification was designed ground-up to nicely play in the IoT world by making identification of each of its information elements (identity, credential, attribute, PACS, and location) universally unique (by using 128 bit UUIDs).

**P**hysical and logical access control could benefit from a common source of constructs and architectures, and models such as RBAC-RPE and

RBAC-AE can help in designing and implementing access control systems. The new PLAI specification provides business and security benefits, including management of role-based privileges from an authoritative identity source and the propagation of this logical data throughout multiple PACS; the propagation of an employee's credential information from one PACS to others, thus supporting access control at multiple facilities using one credential; and the easy revocation of physical access privileges across multiple PACS. 

## References


1. "Microsoft Global Security Commits to Physical-Logical Access and Interoperability Spec," PSIA press release, 29 Sept. 2014; <http://psialliance.org/documents/PSIAAnnouncement09-29-2014.pdf>.
2. "Physical/Logical Access Interoperability Working Group," PSIA Alliance, white paper, 2013; [www.psialliance.org/documents/PSIAPhysicalLogicalAccessInteroperability.pdf](http://www.psialliance.org/documents/PSIAPhysicalLogicalAccessInteroperability.pdf).
3. *ANSI INCITS 494-2012 Information Technology—Role Based Access Control—Policy-Enhanced*, Int'l Committee for Information Technology Standards (INCITS), Aug. 2012; <http://webstore.ansi.org/RecordDetail.aspx?sku=INCITS+494-2012>.
4. *ANSI INCITS 359-2012 Information Technology—Role Based Access Control*, Int'l Committee for Information Technology Standards (INCITS), May 2012; <https://www.techstreet.com/products/1837530>.
5. D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role-Based Access Control," *Computer*, vol. 43, no. 6, 2010; <http://csrc.nist.gov/groups/SNS/rbac/documents/kuhn-coyne-weil-10.pdf>.
6. A. Karp, H. Haury, and M. Davis, "From ABAC to ZBAC: The Evolution of Access Control Models," HP Laboratories, HPT02009-30, 21 Feb. 2009; [www.hpl.hp.com/techreports/2009/HPL-2009-30.pdf](http://www.hpl.hp.com/techreports/2009/HPL-2009-30.pdf).

7. M. Kunz et al., "Analyzing Recent Trends in Enterprise Identity Management," *Proc. 25th Int'l Workshop Database and Expert Systems Applications (DEXA)*, 2014, pp. 273-277.
8. V.C. Hu, R. Kuhn, and D.F. Ferraiolo, "Attribute-Based Access Control," *Computer*, vol. 48, no. 2, 2015, pp. 85-88; doi:10.1109/MC.2015.33.
9. V.C. Hu et al., "SP800-162 Guide to Attribute-Based Access Control (ABAC): Definition and Considerations," Nat'l Inst. Standards and Technology, Jan. 2014; <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf>.

*Mohammad Soleimani is CTO at Kastle Systems and chairman of PSIA. His research interests include identity management, mobile credentials, physical logical convergence, and the IoT. Contact him at [msoleimani@kastle.com](mailto:msoleimani@kastle.com).*

*Tim Weil is a Risk Management Lead (contractor) at the US Department of Interior. His research interests include security architecture, risk management, identity management, and network engineering. Contact him at [trweil@ieee.org](mailto:trweil@ieee.org).*

*Ed Coyne is an RBAC consultant and IEEE senior member. His research interests include access control models, IT standards, and role engineering. Contact him at [edcoyne@iname.com](mailto:edcoyne@iname.com).*

 Selected CS articles and columns are available for free at <http://ComputingNow.computer.org>.

## ADVERTISER SALES INFORMATION

### Advertising Personnel

Marian Anderson  
Sr. Advertising Coordinator  
Email: [manderson@computer.org](mailto:manderson@computer.org)  
Phone: +1 714 816 2139  
Fax: +1 714 821 4010

Sandy Brown  
Sr. Business Development Mgr.  
Email: [sbrown@computer.org](mailto:sbrown@computer.org)  
Phone: +1 714 816 2144  
Fax: +1 714 821 4010

### Advertising Sales Representatives (display)

Central, Northwest, Far East:  
Eric Kincaid  
Email: [e.kincaid@computer.org](mailto:e.kincaid@computer.org)  
Phone: +1 214 673 3742  
Fax: +1 888 886 8599

Northeast, Midwest, Europe, Middle East:  
Ann & David Schissler  
Email: [a.schissler@computer.org](mailto:a.schissler@computer.org), [d.schissler@computer.org](mailto:d.schissler@computer.org)  
Phone: +1 508 394 4026  
Fax: +1 508 394 1707

Southwest, California:  
Mike Hughes  
Email: [mikehughes@computer.org](mailto:mikehughes@computer.org)  
Phone: +1 805 529 6790

Southeast:  
Heather Buonadies  
Email: [h.buonadies@computer.org](mailto:h.buonadies@computer.org)  
Phone: +1 973 585 7070  
Fax: +1 973 585 7071

### Advertising Sales Representative (Classified Line)

Heather Buonadies  
Email: [h.buonadies@computer.org](mailto:h.buonadies@computer.org)  
Phone: +1 973 304 4123  
Fax: +1 973 585 7071

### Advertising Sales Representative (Jobs Board)

Heather Buonadies  
Email: [h.buonadies@computer.org](mailto:h.buonadies@computer.org)  
Phone: +1 973 304 4123  
Fax: +1 973 585 7071