Role Based Access Control for Physical Access Solutions
Today’s evolving threats are both physical and digital. From the latest hacking attack to the more devastating school shootings, threats are everywhere. Access control plays an essential role in safeguarding both physical security and electronic information security. As global security risks and regulatory compliance requirements continue to grow, strengthening access control becomes a higher priority for everyone. We will discuss several ways that Role-Based Access Control (RBAC) — now in widespread corporate use for electronic information systems (i.e. IT security) — can be successfully applied to physical security, either by leveraging IT security efforts or by following applicable portions of the 2004 ANSI/INCITS standard for Role-Based Access Control (RBAC, commonly pronounced “are-back”).

Restoring Physical Access Integrity

In most but not all organizations, the state of physical access management is far from ideal. Many risks exist due to weaknesses in access management and have been either overlooked or downplayed, particularly in situations where available security resources and tools simply do not fully match up to the access management burden. This has occurred for mechanical locks and keys as well as for Physical Access Control Systems (PACS) that are typically card-based access systems.

A poor state of lock and key management is often tolerated within organizations because of the difficulty and complexity of the problem. Bringing locks and keys back to a known good state would entail a huge level of effort at an unacceptable financial cost. Not only is it costly and expensive but there are no safeguards to ensure it will not just happen again. A painful interruption to a business that would result from the wholesale rekeying of locks that are immediately at risk all over just doesn’t make financial sense.
Even when starting from a clean slate for access management (cards, fobs, etc.) and mechanical key management, the initially accurate privilege and key assignments do not last for long. Often, due to traditional PACS product limitations in managing card access privileges, compromises are made in access level definitions, to the point where over time the access level names no longer accurately represent the scope of access privilege being provided. Thus, access management is no longer transparent, and the integrity of privilege management is too hard to maintain.

When mechanical keys are lost or unreturned by departing personnel, locks are often not rekeyed according to desired practice. Key record-keeping easily becomes outdated, and the integrity of the mechanical key program degrades quickly.

Now, thanks to “Bring Your Own Device” (BYOD) solutions, such as personal mobile phones, you no longer need to worry about getting keys or cards back from personnel. As one of the new BYOD solutions, pdqSMART allows organizations to quickly and cost effectively deploy access control solutions to these areas that were previously left vulnerable. With pdqSMART, both physical key control corrections and more widespread use of electronic access control solutions are financially feasible for business.

Technology has advanced to the point where any organization can upgrade the caliber of their access management, and maintain its integrity going forward with considerably less effort than has been required in the past. pdqSMART+ brings lock and key management in line with access credential management, enabling a unified approach to be taken for all of the physical access management.
The Next Logical Step in Physical Access Management

RBAC has become the single-most effective approach to managing access control, and the American National Standards Institute (ANSI) adopted it as a standard in 2004. RBAC is also the next step in the historical progression of physical access control management.

There is already a similarity between RBAC and conventional access control group mechanisms. Figure 1 shows the historical development of physical access privilege management, culminating in the use of cardholder groups to help simplify the management of access privileges. There are, of course, a number of variations to access privilege schemes, but most systems have the elements shown in Figure 1 in common.
Figure 1 shows the historical development of physical access privilege management, culminating in the use of cardholder groups to help simplify the management of access privileges. There are, of course, a number of variations to access privilege schemes, but most systems have the elements shown in in Figure 1 in common.

The main purpose of RBAC is to allow access roles to align with an organization’s actual personnel roles and related job responsibilities, as shown in Figure 2.
One purpose of RBAC is to allow access roles to align with an organization’s actual personnel roles and related job responsibilities, as shown in Figure 2.

In a PACS that supports groups of users or credential holders (which can play the part of Roles in an RBAC scheme) and groups of devices, RBAC can be established and managed by simple procedures. pdqSMART delivers exactly that functionality, allowing users to be grouped as well as devices.

Make Access Control Simpler

RBAC provides the ability to approve the access privileges that are assigned to a specific role, instead of having to individually approve them for each person who will be assigned to the role. This significantly reduces the number of approval workflows required, which at times can be burdensome and can result in delays in access privilege assignments. Such delays often translate into delays in getting individuals functioning in their assigned positions. RBAC can eliminate them.
The process of naming roles that reflect the various organizational positions is termed “Role Engineering.” The resulting roles are called a “Role Catalog,” and its contents reside in the corporate directory or HR management system. Roles engineering is significant work, but the results are incredibly valuable for both physical security and IT.

Company Roles, not IT Roles

Many IT departments, especially in medium or large enterprises, are implementing or already have implemented an Identity and Access Management (IAM) program, to “once and for all” get a good handle on corporate identity management and information systems access management. The program is called Identity and Credential Access Management (ICAM) in the U.S. government because it uses a single smart card for both physical and logical security. Secure enrollment and card issuance processes are critical to the integrity of access management. pdqSMART relies on 13.56 mHz smart card technology, for this reason, smart cards allow interoperability with many other business devices and systems. BLE and NFC are beginning to appear as solutions as well, both of which are supported by pdqSMART.

Because the IAM/ICAM programs and projects are run by IT departments, there is a tendency (especially for physical security practitioners) to think of the roles that are developed as “IT roles,” when in fact, they are really the staff’s role in the organization. Physical access privilege assignments are generally simpler than IT permissions. For example, where an accounts payable department may have many sets of information access requirements, most of the Accounts Payable personnel will have common physical access requirements. The roles used stay the same. It is generally simpler work establishing RBAC for physical security than for IT security.

Implementing RBAC

The best way to implement RBAC for Physical Access is by creating a directory of personnel and clearly noting their job descriptions and roles prior to setting up the system. pdqSMART offers an Excel fill-out sheet to help assist with this. This information should come from the HR department or similar source within the organization. Roles can be assigned to groups and the group names can be the roles in the...
organization. Access Rules are then assigned to the Groups of users. This contributes to scalability since in most organizations more than one person has the same role (sales person, accountant, auditor, receptionist and so on). Roles change less frequently than personnel; thus, assigning and updating access privileges is simplified. Roles are designed to parallel actual organizational roles, which simplifies management and allows role assignment to be done as part of the personnel enrollment process. This lightens the end user’s burden in physical access management. While it is possible to implement a one-role-per-person policy, that becomes very cumbersome quickly. A hierarchical approach makes it possible to restrict role assignment to one role per person.

The use of documented organizational hierarchy can establish RBAC, as depicted in Figure 3.

*Figure 3: Organizational Hierarchy (Users)*

Owner/CEO/President

- Access Group 1 (Managers)
  - VP Sales
    - Inside Sales
    - Access Group 2 (Sales)
  - VP Engineering
    - Customer Service
    - Engineering Manager
    - Eng. Staff 1
    - Access Group 3 (Engineering)
    - Eng. Staff 2
  - Operations Manager
    - Production Lead
    - Operator 1
    - Operator 2
    - Access Group 4 (Operations)
According to security practitioners who have implemented RBAC, about 75 or 80 percent of the requirements are covered with role-based access rule assignment, and the remainder is covered by individual access assignments. A physical security example of the individual access assignment is the card/credential for a manager’s own office door. Only the manager has access to his/her office door, except perhaps for emergency and cleaner access privileges. So, while the majority of personnel have cubicles and or desks in common areas, office door management may be an individual privilege assignment per credential holder for a subset of personnel. This in no way lessens the value of the simplification RBAC provides in access management. The “one-off” and “individual assignment” cases are reduced by up to 80%. The confusion factor is practically eliminated and audit reviews are streamlined.

Audit-Proof Physical Access

“Audit-proof physical access” requires a physical access control management process that is clearly defined, is easily managed, and by which access privileges are assigned and updated in a timely manner according to job positions, responsibilities and duties. If you don’t have that now, consider using RBAC to help you create that state for physical access management.

The goal after buying and deploying pdqSMART+ should be to have a far simpler and more easily managed keying and access control system in place that reduces longterm maintenance needs and enhances your operations. Contact PDQ today to discuss your facility needs and requirements at sales@pdqsmart.com