Physical/Logical Access Interoperability Working Group

Contents

Physical/Logical Access Interoperability

Executive Summary

This document, prepared by the Physical Security Interoperability Alliance (PSIA), discusses the PSIA's plan to develop a specification to unify logical and physical identities using role-based access management (RBAC-RPE). This specification would enable security industry manufacturers, integrators and end users to develop effective, easily administered solutions spanning the physical and logical security domains.

Introduction

In June 2013, the PSIA Board and Profiles working group met in Seattle. During the meetings, PSIA member Kastle Systems delivered an overview to the group about the current status and opportunities to integrate Role Based Access Control (RBAC) between logical and physical domains. Briefly, RBAC entails creating logical and physical access control policies based on a standard definition of an employee's role in a company.

At the conclusion of the meeting, a working group was established to frame an initial document to structure the rationale for developing a new specification.

Leveraging the experience of Kastle Systems and its experiences thus far in integrating roles between logical and physical security domains, the PSIA has framed this document. Several other industry sources have also been consulted to discuss the need for such a project. Helpful reading includes that from *Security Technology Executive*[1] and the Security Industry Association (SIA) *Quarterly Technical Update*[2]

The PSIA will present an overview of the proposed specification on Monday September 23, 2013 in Chicago during the 59th ASIS Seminar and Exhibits. Registration for this event may be found by clicking **here**. An additional working meeting during ASIS is being organized.

[1] See RBAC for Physical Access Control, *Security Technology Executive*, April 2012

[2] *SIA Quarterly Technical Update* D'Agostino, Engberg and Bernard, December 2005

Overview

Business Objective

Create a technical specification to encourage the creation of standards-based solutions that make logical and physical security more functional and their administration more efficient.

Technical Objective

Define a PSIA specification using "Lightweight Directory Access Protocol" (LDAP) to unify logical and physical identities using role-based access management (RBAC).

The PSIA is taking an inclusive approach, inviting members and other groups to participate in the specification working group.

Progress

PSIA members have already created the world's first Area Control specification for physical security, and this specification is being adopted by most of the major access control manufacturers. The specification allows a variety of physical security technologies to interoperate with each other.

The Next Step

To enable the market to create open solutions for enhanced security functionality and more efficient security administration, a specification needs to be created to allow logical and physical security domains to exchange role-based access profile information between each other in a standardized way. We present the business rationale and use case scenarios for such a specification below.

Background

Standards-Based Identity Unification

The unification of H.R., logical and physical security identities is challenging and expensive. The so-called solutions that exist today show no evidence of being standards-based. These proprietary offerings require vendors and integrators to significantly change the workflow cycles and responsibilities in both the physical and logical/IT security domains to create "solutions" to identity unification.

Solutions that lock customers to a particular vendor are usually proprietary and expensive, and cannot be cost effectively integrated with new technologies that security and IT organizations acquire. It is also generally difficult to mesh proprietary non-standard offerings with an organization's broader technology fabric.

Identity Management

Today, it is common practice to populate logical and physical identities using the H.R. Management System (HRMS) as the authoritative data source. Integration to populate either the physical or logical security system using HRMS was solved some time ago and is not the focus of this document.

The Need

Workflow

Logical and physical identities are rarely and efficiently reconciled between each other, without significant expense and duplication.

The typical security workflow is: HRMS → Logical→ Physical and usually involves manual processes which add cost, the potential for error and delay workflows.

Achieving better Enterprise Security Risk Management (ESRM) by enhancing security functionality using the identity assets in both the logical and physical security domains has been a topic of popular conversation but has not been widely adopted. There are several reasons for this, including that often, one domain is forced to change its core functions to suit the other, or because the vendor solution is proprietary and expensive.

There are two apparent reasons that reconciliation between physical and logical security are desired: 1) the need for enhanced security functions; and 2) more efficient physical security administration.

Enhanced Security Functions Needed

- Examples of enhanced security achieved through unified physical and logical identities:
    - A user cannot authenticate to a logical security environment (login to a computer system) in a particular physical location without first having been determined to be physically present, using physical access control.
    - Remote access to logical assets could be questioned when a user is physically present in the location in which those assets exist, and so has no apparent reason for remote access.
        - These authentication and access solutions are especially relevant given that solving ongoing cyber-related intrusions in organizations is a clear and urgent priority.

More Efficient Physical Security Administration

- Access control systems today lack uniformity of approach to administration, and automated privilege management functions. This means that the cost of administration becomes a burden as the system is more actively used or scales upward.
    - Examples: Business activity that creates the need to carry out administration to enact different access privileges:
        - Organizational restructuring
        - Changes to contracts
        - Acquisition or divestment of business units or companies within a group that may then require:
            - Integration of different logical access control systems
            - Integration of different physical access control systems
        - Employees who travel between locations and require temporary access
            - In discussions with one Fortune 50 organization, its Security Managers cited the case of managing nearly 200,000 existing physical identities. Of these, at any given time, several thousand are being administrated to create temporary privilege for workers to access locations while traveling. They state that about 20% of the activity of the 1,200 administrators is to create temporary access for the traveling worker.
            - Automated Privilege Management would allow temporary access to be created by utilizing a travel record to create and then revoke temporary access in a defined physical boundary. The efficiencies gained would be significant.

Security Workflow Scenario for Identities

Discussion among PSIA members reveals that one possible identity unification workflow scenario is to use the privilege structure defined in the logical security domain to organize and manage physical security privileges. The PSIA specifically is considering developing a specification that would enable the migration of RBAC (specifically RPE – RBAC Policy Enhanced Standard) from the logical domain to the physical security domain.

RBAC-RPE is 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). Roles are then assigned to employees, in contrast to assigning physical and/or logical access privileges directly to an individual.[3]

The PSIA specification would thus augment physical security functionality by providing a mechanism for greater connectivity between both domains, and a standardized, more efficient mechanism for physical security administration through the use of RBAC.

Providing a standard method for the physical security community to gain such connectivity to logical RBAC will enable the creation of interoperable tools by the market that address the security and business needs described in this document.

These needs and the benefits of addressing them are not new, but end users and integrators have only rarely tried to address them because no standardized, industry-wide mechanism to implement has existed.

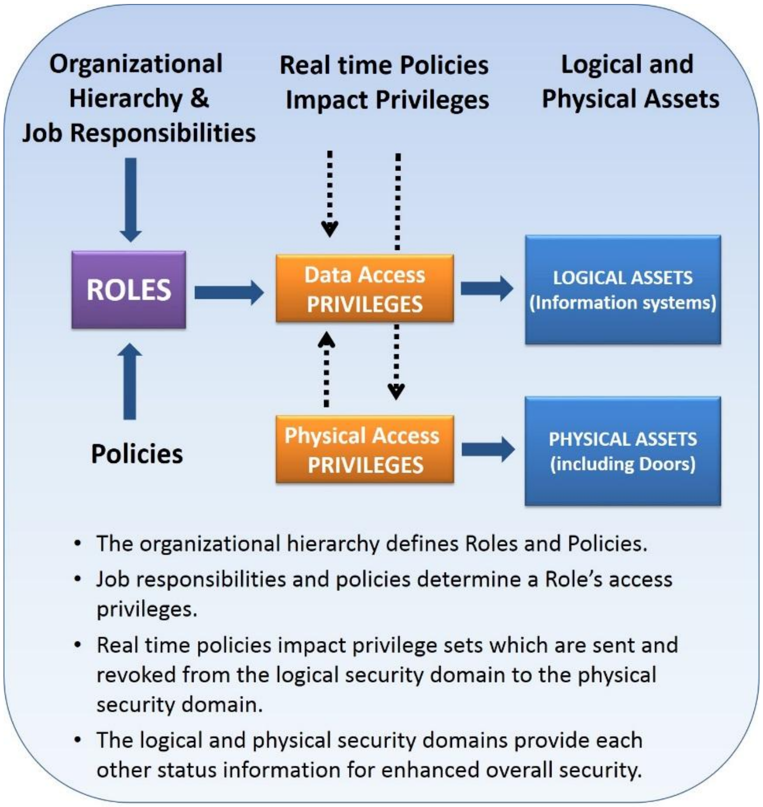
The Project

The proposal is to establish a formal PSIA working group for Physical-Logical Access Interoperability that will define a new specification to address the identify unification problem. This specification will enable the creation of solutions that allow logical and physical identities to be mapped relevant to each other. The PSIA specification will likely utilize the existing standard LDAP at its core, because LDAP is a published, widely adopted directory standard. 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.

[3] http://csrc.nist.gov/groups/SNS/rbac/, accessed 8/27/13

Conceptual Model – Physical/Logical Access Interoperability


Organizational Hierarchy & Job Responsibilities
Real time Policies Impact Privileges
Logical and Physical Assets
ROLES
Data Access PRIVILEGES
LOGICAL ASSETS (Information systems)
Policies
Physical Access PRIVILEGES
PHYSICAL ASSETS (including Doors)

- The organizational hierarchy defines Roles and Policies.
- Job responsibilities and policies determine a Role's access privileges.
- Real time policies impact privilege sets which are sent and revoked from the logical security domain to the physical security domain.
- The logical and physical security domains provide each other status information for enhanced overall security.

Figure One[4] : Physical/Logical Access Interoperability (Conceptual).

Figure One above shows how roles, utilized in the logical security domain, may be replicated to the physical security domain to create synchronicity between domains. The PSIA Working Group would develop a comprehensive definition of the required functionality as the foundation for a detailed specification.

Summary

Creating a specification that enables solutions to be created to map the same identity and role in logical and physical security environments using RBAC will provide significant cost and functional benefits for Enterprise Security Risk Management, and lay the groundwork for automating privilege management.

[4] Thank you to Ray Bernard for providing a base graphic which was adapted to represent the concept.