RBAC Driven Least Privilege Architecture for Control Systems

Modular toolset for system-wide role based access control (RBAC) and enforcement

Background

The computer security community has long advocated the concept known as least privilege, which provides to a user or process only the minimum set of access rights necessary to perform a specific task or role. Similarly, corporate information technology and military organizations are realizing the benefits of having fine-grained access control mechanisms enforce least privilege. However, many energy delivery control devices and supervisory control and data acquisition (SCADA) systems today have inadequate access control models that are not capable of enforcing least privilege.

Barriers

- Legacy, single-user energy delivery control systems devices share a password among many users
- Legacy field devices have limiting computing environments, which makes security upgrades difficult
- Most legacy control devices do not provide for adequate user roles and lack the ability to specify user rights
- Least privilege driven cryptographic key management is difficult and costly

Project Description

This project will create role based access control (RBAC) driven least privilege architecture for energy delivery systems. The team will develop a modular toolset integrated with Lightweight Directory Access Protocol (LDAP) enterprise authentication and the Experion® Process Knowledge System product suite. The Experion distributed control system provides control at all four levels of the Purdue reference model together with advanced applications to unify management of assets, processes and people. The Experion system is used extensively within the oil and gas industry. The RBAC technology will be implemented on a Honeywell Experion system, evaluated by a security team from Idaho National Laboratory, and then demonstrated to the U.S. Department of Energy and members of the electric power, oil and gas industries.

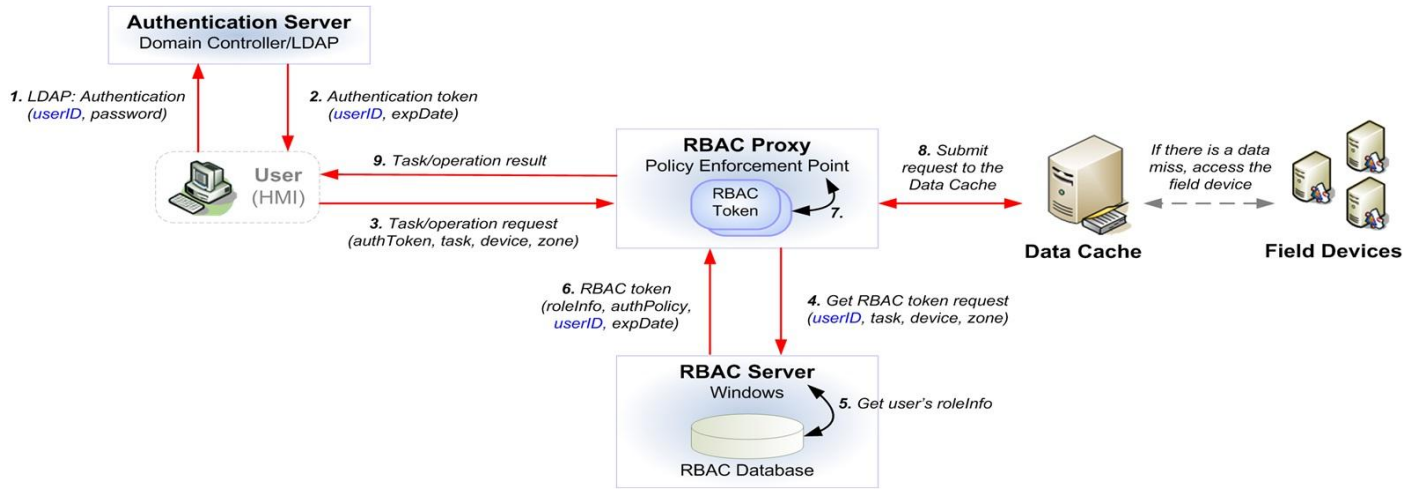
Benefits

- Links access control and key management, eliminating time consuming, error-prone human processes previously required
- Allows user rights management to be specified based on the role, operating mode and end device
- Integrates devices conforming to the Open PCS (process control system) Security Architecture for Interoperable Design (OPSAID) to ensure secure communication
- Supports using existing enterprise authentication services such as Active Directory and token based systems
- Extends an access control enforcement mechanism to the end device or process

Partners

- Honeywell Laboratories and Honeywell Process Solutions
- The Information Trust Institute at the University of Illinois – Urbana-Champaign
- Idaho National Laboratory

RBAC System Overview showing process flows of a typical user request to a target device



Technical Objectives

The objective of this project is to create an RBAC driven least privilege architecture for energy delivery control systems.

The technical approach for achieving these objectives includes the following:

- Create a modular authentication technology for users and processes that supports using existing enterprise authentication services such as LDAP, Active Directory and token-based systems
- Develop role based access control models that allow user rights management to be specified based on the role, operating mode and end device
- Link access control and Internet Protocol Security (IPsec) key management
- Develop role engineering tools to support moving from existing access control approaches to an integrated role based model
- Integrate RBAC policy enforcement point technology with secure communications to extend the access control enforcement mechanism to the end device or process
- Demonstrate the integration of RBAC technology with the Experion process knowledge system

Honeywell intends to share the architecture solution so that it can be adopted by standards bodies such as the International Society of Automation for use within multiple industries (e.g., electric power, oil and gas). This will provide a common roadmap for other vendors to build interoperable products.

End Results

Project results will include:

- A rally point for common SCADA security architecture: Successful implementation of the RBAC tool set can be a common solution for meeting SCADA security requirements
- Reduced vulnerabilities: Implementing the RBAC tool set will achieve a marked reduction in the amount of unnecessary access to system devices, which will eliminate many of the existing vulnerabilities linked to poor access control
- Near net-zero impact on operational costs: The solution will link to existing enterprise authentication servers, thus minimizing additional administrative workload. Role engineering and management tools linked to the RBAC model will provide semi-automated policy configuration

Content last updated: August 2012

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

Tom Markham
Engineering Fellow
Honeywell International
763-954-6840
tom.markham@honeywell.com

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov