NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ACCESS RIGHTS MANAGEMENT

Secure Access for the Financial Services Sector

The National Cybersecurity Center of Excellence (NCCoE) is addressing Access Rights Management (ARM) for the financial services sector through collaboration with members of the sector and vendors of cybersecurity solutions. This effort will result in the development of a practice guide—a practical, user-friendly document that facilitates the adoption of standards-based approaches to cybersecurity. It will include an example solution to this challenge, but given the continually evolving cybersecurity technology market, is not the only solution. Please contact us at financial_nccoe@nist.gov with suggestions and comments.

CHALLENGE

Some of the identity and access systems employed by the financial services sector are fragmented, incompatible, and operate in isolation from one another. Their operation, therefore, is complex and prone to errors and inconsistencies that could be exploited by attackers or insider threats. This situation makes it difficult for enterprises to securely embrace new technologies such as mobile and cloud computing.

The financial services sector needs the ability to centrally issue, validate, and modify or revoke access rights for an entire enterprise based on easy-to-understand business rules. The goal of this project is to demonstrate ways to link the management of existing disparate identity and access mechanisms and systems into a comprehensive access rights management (ARM) solution.

SOLUTION

ARM is meant to abstract, unify, and simplify the complex task of dealing with multiple types of access systems, such as Windows Active Directory, Unix/Linux, Resource Access Control Facility (RACF), automatic class selection (ACS2), and myriad legacy and internally developed application-specific mechanisms. The capability will also produce consolidated reports and statistics so that administrators and managers can make accurate risk management decisions.

The example solution proposed here is designed to provide:

- a single system that is capable of interacting with multiple existing access management systems for a complete picture of access rights within the organization
- secure communications between all components
- automated logging, reporting, and alerting of identity and access management events across the enterprise
- ad-hoc reporting to answer management, performance, and security questions
- support for multiple access levels for the ARM system (e.g. administrator, operator, viewer)
- protection from the introduction of new attack vectors into existing systems
- a complement to, rather than replacement of, existing security infrastructure

BENEFITS

A properly implemented and administered ARM system can:

- reduce damage caused by a successful insider threat attack by limiting the amount of data to which any one person has access
- limit opportunity for a successful attack by reducing the available attack surface
- increase the probability that investigations of attacks or anomalous system behavior will reach successful conclusions
- reduce complexity, which leads to:
  - » faster and more accurate access policy modifications
  - » fewer policy violations due to access inconsistencies
- simplify compliance by producing automated reports and documentation

EXAMPLE SCENARIOS

A new employee is hired: ARM uses business rules to develop and implement access rights across the enterprise (e.g., Active Directory, Unix, mainframes) for the new employee.

An employee changes work roles: ARM examines business rules to delete, modify or add access rights across the enterprise that are relevant to the new work role.

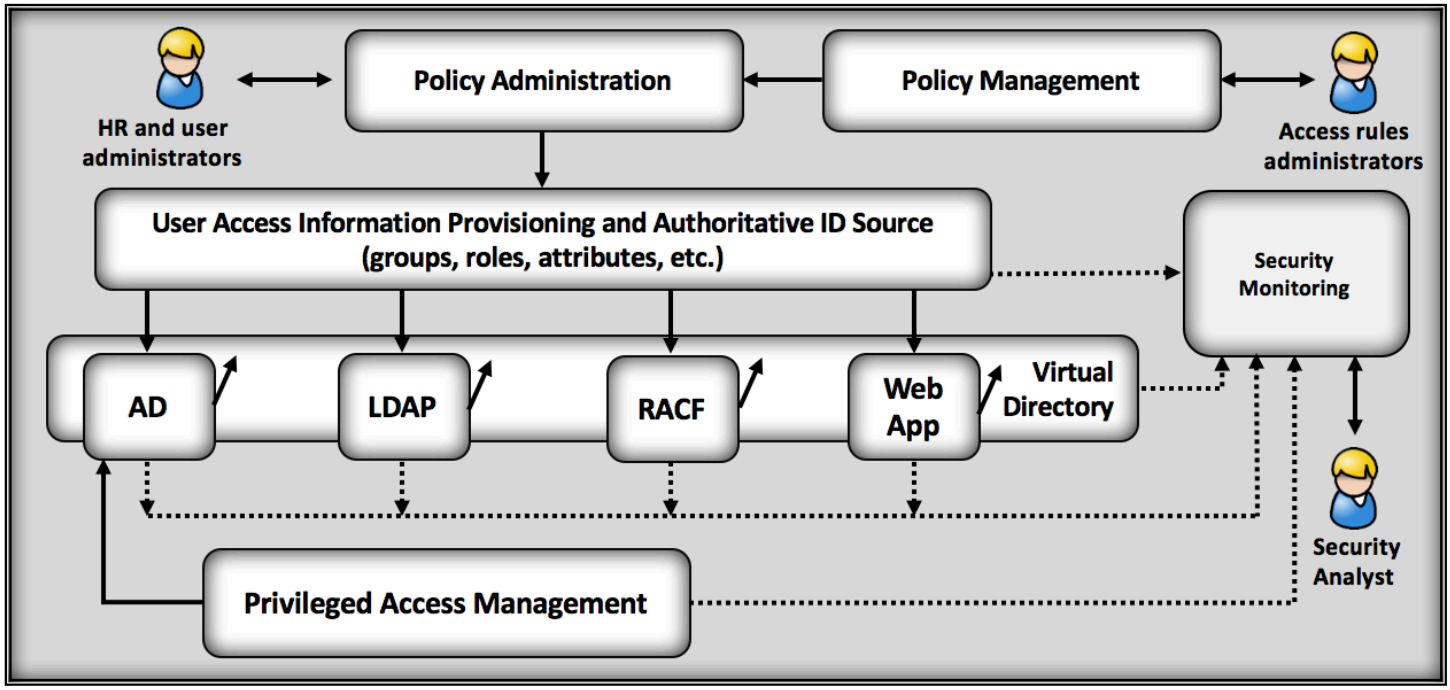
The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

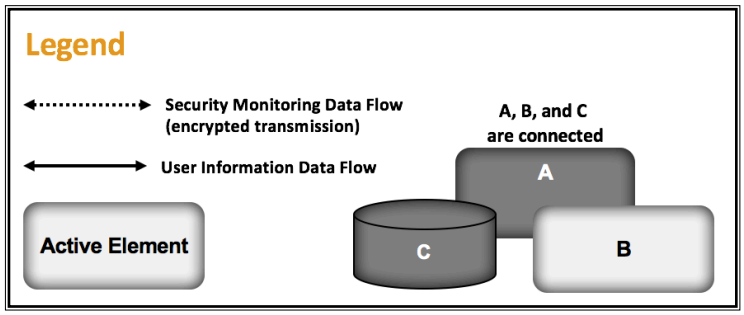
LEARN MORE ABOUT NCCOE
Visit https://nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE

ARM is a single solution with the ability to interact with existing and future access rights systems by using available communication standards.





TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:

AlertEnterprise! HYTRUST NEXTLABS RADIANT LOGIC splunk> tdi technologies VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

Certain commercial entities, equipment, products, or materials may be identified in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD THE PROJECT DESCRIPTION

For more information about this project, visit: https://nccoe.nist.gov/projects/use_cases/access_rights_management

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this project, please email financial_nccoe@nist.gov.