USE CASE

ACCESS RIGHTS MANAGEMENT

Securing Assets for the Financial Services Sector

Draft
November 18, 2013
financial_nccoe@nist.gov

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology works with industry, academic and government experts to find practical solutions for businesses' most pressing cybersecurity needs. The NCCoE collaborates to build open, standards-based, modular, end-to-end reference designs that are broadly applicable and help businesses more easily align with relevant standards and best practices.

This document is a detailed description of a particular problem that is relevant across the financial services sector. NCCoE cybersecurity experts will address this challenge through collaboration with members of the sector and vendors of cybersecurity solutions. The solutions proposed by this effort will not be the only ones available in the fast-moving cybersecurity technology market. If you would like to propose an alternative architecture or know of products that might be applicable to this challenge, please contact us at financial_nccoe@nist.gov.

1. DESCRIPTION

Goal

The current identity and access systems employed by the financial sector are fragmented, operate in isolation from one another, and often incompatible. Operation is thus complex and prone to errors and inconsistencies that can be exploited by attackers or insider threats. In addition, this situation makes it even more difficult to securely embrace new technologies such as mobile and cloud computing. The goal of this project is to demonstrate ways to link together the management of the existing disparate identity and access mechanisms and systems into a comprehensive identity and access management (IDAM) system. This will enable financial sector entities to centrally issue, validate, and modify or revoke access rights for their entire enterprise based on easy-to-understand business rules. This IDAM system will 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. This IDAM system will also produce consolidated reports and statistics so that administrators and managers can make accurate risk management decisions.

Motivation

A foundation of cybersecurity is the principle of least privilege, or the notion that "Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job."[1] To enforce this principle, the IDAM system needs to know the appropriate privileges for a given user or system.

[1] J. Saltzer, Protection and the control of information sharing in multics, *Communications of the ACM*, **17** (7), 388-402 (1974)

Once an identity has been established, the user is placed in various roles and groups according to job position. Traditionally, access management has been a complex process that is not standard across different operating systems. Permissions assigned to particular roles and groups may not translate to the same permissions on a different system. Mistakes are often made and frequently a user is allowed more access than truly required.

Access management must answer the following questions:

- What systems and data does a user have access to?
  - provide an audit log of what a user has accessed and when
- Which users have access to a particular system or data asset?
  - provide an audit log of when the asset was accessed and by whom

Successful identity and access management relies on:

- authentication, authorization and access control requirements across all relevant systems
- ability to centrally manage the authentication and authorization information across all relevant systems
- ability to monitor authorized and unauthorized use of all relevant systems and data
- authentication, authorization and access control mechanisms that meet business security requirements

Example Scenarios

Scenario 1 – A new employee

The company hires a new employee as a member of the mainframe software development team.

- **Phase 1** – The human resources department enters the employee's identity and personal identifiable information (PII) into the human resources database. The employee is assigned a company-wide employee identifier (ID).
- **Phase 2** – A member of the IT support team joins the new employee's ID to the mainframe software development team and assigns all of the necessary privileges using the IDAM system, which
  - adds the new employee into Active Directory as a member of the mainframe software development team group
  - grants access to special applications that the new employee needs based on knowledge of what a mainframe software developer requires
  - adds the new employee to the mainframe access system (e.g., RACF). The mainframe access system may need to take into account any cascading access requirements
  - sends automated messages to the mainframe support team and specialized application owners regarding the newly added user

Scenario 2 – An employee changes work roles

A bank teller changes positions within the company to take on the role of salesperson.

- **Phase 1** – The human resources department modifies the employee's organizational information to reflect the new status of a salesperson. Human resources notifies the employee's current organization (bank tellers), new organization (sales) and support organizations of the organizational change.
- **Phase 2** – The IT support department removes the employee from the bank tellers' group using the IDAM system, which
    - deletes all access privileges used by bank tellers while retaining privileges common throughout the company (for example, email and basic web access)
    - sends automated messages regarding the deleted user to the owners of the bank tellers' group
- **Phase 3** – The IT support department joins the employee's ID to the sales team and assigns all of the necessary privileges using the IDAM system, which
    - adds the employee into the Active Directory sales team group
    - grants access to the applications the employee needs, based on knowledge of a salesperson's requirements
    - sends automated messages regarding the deleted user to the owners of the bank tellers' group

Scenario 3 – Determine who has access to a particular data asset

The IDAM system creates a report on all users who have access to an individual file by performing the following high-level steps:

- for the system being examined, adds the system administrator to the report
- adds all members of "Administrator" or "Root" groups to the report
- enumerates the file to determine which users and groups have access to the file
    - adds all users from the enumeration to the report
    - adds all users in each group enumerated to the report
- reports on any complex cases such as users of web servers that access file sharing and web services

These are difficult tasks because each system handles permissions and access control lists differently. At a minimum, the IDAM must function properly if the file exists on a:

- Microsoft Windows system
- Unix/Linux system
- mainframe

2. Desired Solution Characteristics

- a single system that is capable of interacting with multiple existing access management systems to provide a complete picture of access rights within the organization
- complements, and does not replace, existing security infrastructure

- utilizes secure communications between all components
- automates logging, reporting and alerting of identity and access management events across the enterprise
- can be queried for information (ad-hoc reporting) in order to answer management, performance and security questions
- does not introduce new attack vectors into existing systems
- supports multiple access levels for the IDAM system (e.g. administrator, operator, viewer)

3. Business Value

A properly implemented and administered IDAM system can:

- reduce damage caused by a successful insider threat attack by limiting the amount of data that any one person has access to
- 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
    - less policy violations due to access inconsistencies
- simplify compliance by producing automated reports and documentation

4. Relevant Standards

- NIST Cybersecurity Framework - Standards, guidelines, and best practices to promote the protection of critical infrastructure
http://www.nist.gov/itl/cyberframework.cfm

- NIST National Strategy for Trusted Identities in Cyberspace
http://www.nist.gov/nstic/notices.html

- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

- Identity Ecosystem Steering Group
http://www.idecosystem.org/content/standards-coordination-committee

- ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems - Requirements
http://www.iso.org/iso/catalogue_detail?csnumber=42103

- Shared assessment program
http://sharedassessments.org/

- ISO/IEC WD 29146 – Information technology – Security techniques – A framework for access management http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45169

5. Security Control Map

Security Characteristic	NIST 800-53 Security Controls	SANS 20 Security Controls
Supports multiple access levels for the IDAM system (e.g. administrator, operator, viewer)	AC-2 Account Management AC-3 Access Enforcement AC-7 Unsuccessful Login Attempts AC-8 System Usage AC-18 Wireless Access AC-19 Access Control for Mobile Devices AC-20 Use of External Information Systems	12 - Controlled Use of Admin Privilege
Complements, and does not replace, existing security infrastructure	AC-20 Use of External Information Systems	15 - Account Access Based on Need to Know 16 - Account Monitoring and Control
Utilizes secure communications between all components	SC-8 Transmission Integrity SC-9 Transmission Confidentiality SC-12 Cryptographic Key Establishment and Management SC-13 Use of Cryptography SC-17 Public Key Infrastructure Certificates SC-23 Session Authenticity	
Automates logging, reporting and alerting of identity and access management events across the enterprise	AU-4 Audit Storage Capacity AU-6 Audit Review, Analysis, and Reporting AU-9 Protection of Audit Information IR-6 Incident Reporting	18 - Incident Response and Management

Security Characteristic	**NIST 800-53 Security Controls**	**SANS 20 Security Controls**
Can be queried for information (ad-hoc reporting) in order to answer management, performance and security questions	RA-1 Risk Assessment Policy and Procedures	
Does not introduce new attack vectors into existing systems	RA-5 Vulnerability Scanning SI-7 Software and Information Integrity SC-3 Security Function Isolation SA-11 Developer Security Testing	
Supports multiple access levels for the IDAM system (e.g. administrator, operator, viewer)	AC-5 Separation of Duties AC-6 Least Privilege	15 - Account Access Based on Need to Know

5. Component List

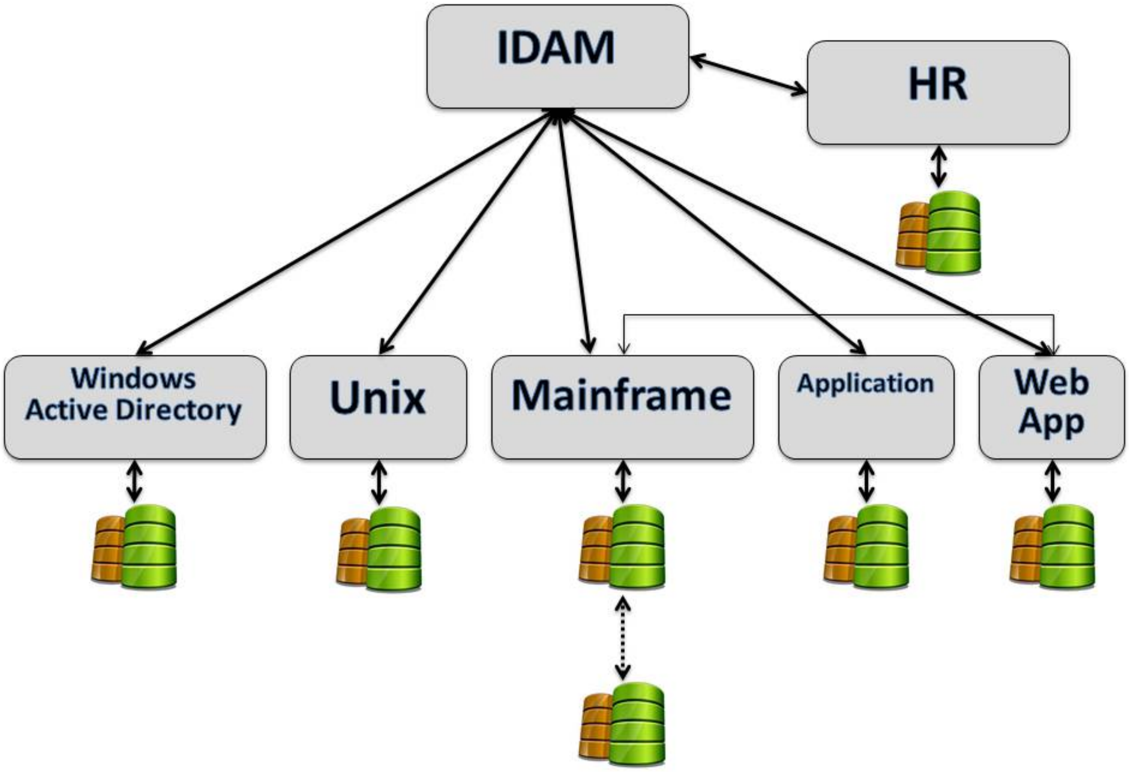
The NCCoE has a test environment for hosting development of the use case including the following features:

- network with machines using Active Directory
- virtualization servers
- network switches
- remote access solution with Wi-Fi and virtual private network

Partners will need to provide any specialized components and capabilities to realize this use case including, but not limited to:

- mainframe (may be simulated or remotely accessed) such as RACF
- representative financial sector application(s) with local user database
- access logging/database system

6. High-Level Architecture


IDAM
HR
Windows Active Directory
Unix
Mainframe
Application
Web App