USE CASE

ACCESS RIGHTS MANAGEMENT

Securing Assets for the Financial Services Sector

V.2 – Final Draft
May 1, 2014
financial_nccoe@nist.gov

This revision incorporates comments from the public.

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. This IDAM system will, at a minimum, automate the monitoring and analysis of identity related activities in a manner that enables administrators and managers to make timely and informed 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 automated continuous analysis of log data and ensure that the actions of individual users are monitored and can be reported on in a timely and accurate manner
- Which users have access to a particular system or data asset?
  - provide automated continuous analysis of asset log data (i.e. audit log) to account for when an 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
- automated ability to monitor all use of all relevant systems and to detect unauthorized use of any system or data
- automated monitoring and analysis capabilities that feed business security, policy and reliability efforts
- 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 the directory service 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 directory service 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

Scenario 4 – User attempts to access data without proper authorization

A valid and authenticated user is accessing data on the internal corporate web. Instead of accessing data by clicking on the hyperlinks presented to him, the user decides to manually enter document names in the web browser's URL entry bar. The user attempts to access three different documents:

- Document 1 exists and is valid – the IDAM system records the successful attempt and allows the user to access the document
- Document 2 does not exist – the IDAM system records the unsuccessful attempt and returns an "unauthorized" message to the user
- Document 3 exists but requires additional privileges – the IDAM system records the unsuccessful attempt, sends a message to the IT security department and returns an "unauthorized" message to the user

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 (i.e. show all activity for a given user in a certain time period)
- does not introduce new attack vectors into existing systems
- supports multiple access levels for the IDAM system (e.g. administrator, operator, viewer)
- provide fine-grain privilege controls (e.g. groups, users -> directory, file, record)
- provide the ability to attach expiration dates/time limits on access controls
- ability to map users access requests via "service" account access

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
- decrease the amount of time, skill and effort required to detect security issues and policy violations
- 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:

144 o faster and more accurate access policy modifications
145 o less policy violations due to access inconsistencies
146 • simplify compliance by producing automated reports and documentation

147 ## 4. RELEVANT STANDARDS

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

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

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

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

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

161 • Shared assessment program
162 http://sharedassessments.org/

163 • ISO/IEC WD 29146 – Information technology – Security techniques – A
164 framework for access management
165 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumb
166 er=45169

167 • NIST Special Publication 800-162: Guide to Attribute Based Access Control
168 (ABAC) Definition and Considerations
169 http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

170 • NIST Special Publication 800-63 rev. 2: Electronic Authentication Guideline
171 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

172 • NIST Policy Machine: Features, Architectures, and Specifications
173 http://csrc.nist.gov/pm/documents/pm_report-rev-x_final.pdf

- OIX: Attribute Exchange Trust Framework Specification v 1.0
  http://openidentityexchange.org/sites/default/files/OIX-AXN-Trust-Framework-Specification-1.0-7-5-2013.pdf

- ICAM Backend Attribute Exchange v 2.0
  http://www.idmanagement.gov/sites/default/files/documents/BAE_v2_Overview_Document_Final_v1.0.0.pdf

5. Security Control Map

This table maps the preliminary list of desired characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (CSF) and other NIST activities. This is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

Example Characteristic	Cybersecurity Standards & Best Practices							
Security Characteristics	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27002**	**SANS CAG20**	**COBIT5**	**PCI/DSS**
supports multiple access levels for the IDAM system (e.g. administrator, operator, viewer)	Identify Protect	Asset Management Access Control	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established PR.AC-1: Identities and credentials are managed for authorized devices and users PR.AC-3: Access permissions are managed, incorporating the principles of least privilege and separation of duties	AC-5 Separation of Duties AC-6 Least Privilege	11.2: User Access Management	12 - Controlled Use of Admin Privilege 15 - Account Access Based on Need to Know	APO01: Manage the IT Management Framework DSS06: Manage Business Process Controls	8: Identify and authenticate access to system components
complements, and does not replace, existing security infrastructure	Identify Protect	Business Environment Access Control	ID.BE-4 Dependencies and critical functions for delivery of critical services are established PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	AC-20 Use of External Information Systems	10.8: Exchange of Information 11.6: Application and Information Access Control	15 - Account Access Based on Need to Know 16 - Account Monitoring and Control	APO03: Manage Enterprise Architecture	6: Develop and maintain secure systems and applications
utilizes secure communications between all components	Protect	Protective Technology Data Security	PR.PT-4: Communications and control networks are protected PR.DS-2: Data-in-transit is protected	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	12.3: Cryptographic Controls	19 - Secure Network Engineering	DSS05: Manage Security Services	4: Encrypt transmission of cardholder data across open, public networks

Example Characteristic	Cybersecurity Standards & Best Practices							
Security Characteristics	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27002**	**SANS CAG20**	**COBIT5**	**PCI/DSS**
automates logging, reporting and alerting of identity and access management events across the enterprise	Protect	Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU-4 Audit Storage Capacity AU-6 Audit Review, Analysis, and Reporting AU-9 Protection of Audit Information IR-5 Incident Monitoring IR-6 Incident Reporting	13: Information Security Incident Management	14 - Maintenance, Monitoring and Analysis of Audit Logs 18 - Incident Response and Management	APO13: Manage Security	10: Track and monitor all access to network resources and cardholder data
can be queried for information (ad-hoc reporting) in order to answer management, performance and security questions	Protect	Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	RA-1 Risk Assessment Policy and Procedures AU-4 Audit Storage Capacity AU-6 Audit Review, Analysis, and Reporting	11.1: Business Requirements for Access Control 13.2: Management of Information Security Incidents and Improvements 15.3: Information Systems Audit Considerations	14 - Maintenance, Monitoring and Analysis of Audit Logs 18 - Incident Response and Management	APO13: Manage Security	10: Track and monitor all access to network resources and cardholder data
does not introduce new attack vectors into existing systems	Detect	Security Continuous Monitoring	DE.CM-8: Vulnerability scans are performed	RA-5 Vulnerability Scanning SI-7 Software and Information Integrity SC-3 Security Function Isolation SA-11 Developer Security Testing	12.6: Technical Vulnerability Management	19 - Secure Network Engineering	DSS05: Manage Security Services	6: Develop and maintain secure systems and applications

6. Component List

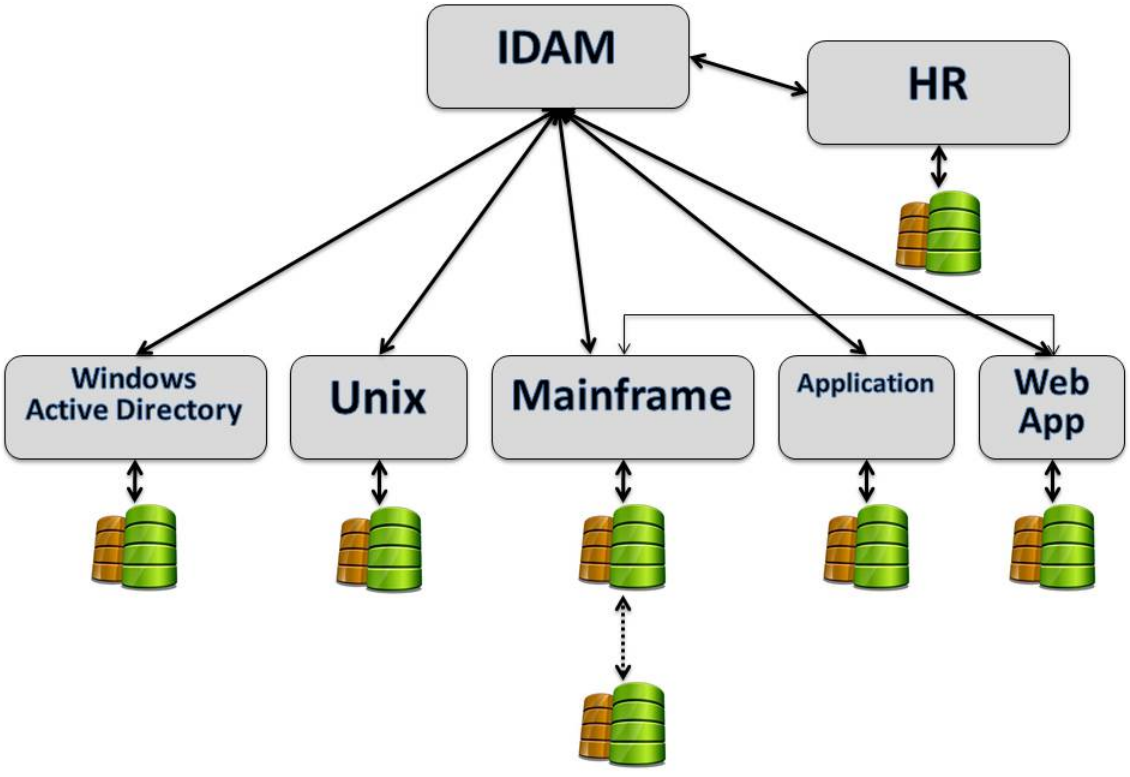
The NCCoE has a lab environment for hosting development of the use case including the following features:

- network with machines using a directory service
- 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

7. High-Level Architecture



8. COMMENTS

We received 28 comments regarding the draft use case. Some comments have been bundled into a single brief statement. We have provided a response to each statement and revised the use cases accordingly.

1. The goal of the use case should be reframed in terms of focusing on facilitating high assurance customer identity credentials, rather than employee identity management.

   Response: The financial sector members who shared their opinions with the NCCoE indicated that they were more concerned with internal users across their extended enterprises. External customer identity is being considered for future work by the NCCoE.

2. How do you validate the principle of least privilege in both the provisioning of users and continued access (systems modification)?

   Response: The technologies used to address this use case should accomplish this. The simple business rules must map correctly to valid machine-usable access rights. We have added to the desired solution characteristics: “Provide fine-grain privilege controls (e.g. groups, users -> directory, file, record)” at Line 131.

3. How do you validate (audit) that the single federated credential is not stolen, shared, or otherwise inappropriately utilized?

   Response: While this approach will have the ability to revoke credentials, detecting stolen credentials is out of the scope of this use case. It may be addressed by another project.

4. Have you thought about adding in a modeling and simulation component to the use case? The operations of this use case from a people and process perspective as important as the technology.

   Response: Simulation may help to prove the use case but it was not a requested feature and therefore not included. However, options for testing platforms are still being considered.

5. Automated continuous monitoring: While this use case addresses reporting, a successful IDAM effort requires automated monitoring that is periodically reviewed so that detection of anomalies can be part of risk management and other security, policy, and reliability activities and decisions.

Response: We agree that continuous monitoring is critical and have made the following suggested changes:

- added "This IDAM system will at a minimum automate the monitoring and analysis of identity related activities in a manner that enable administrators and managers to make timely and informed risk management decisions" to Line 18.
- added "Provide automated continuous analysis of log data that ensures the actions of individual users are monitored and can be reported upon in a timely and accurate manner" at Line 34.
- added "an automated ability to monitor all use of all relevant systems and to detect unauthorized use of any system or data" at Line 45.
- added "automated monitoring and analysis capabilities that feed business security, policy and reliability efforts" at Line 47.
- added “Scenario 4” at line 106 in which a user attempts to access data without authorization and the IT security department is notified, demonstrating continuous monitoring.
- added a bullet at Desired Solution Characteristics (Line 123) that is an example of automated alerting or response based on automated monitoring and analytics.

6. The Business Value section does not identify the need to reduce the time or effort required to detect policy violations or security issues.

   Response: We made the suggested change of adding a bullet that states, "Decrease the amount of time, skill and effort required to detect security issues and policy violations” (Line 138).

7. The usability of access request functionality is important.

   Response: This is already included in “Scenario 1 – A new employee,” and “Scenario 2 – An employee changes work roles.”

8. Include account provisioning and deprovisioning.

   Response: Provisioning is already mentioned in Scenario 1; deprovisioning in Scenario 2.

9. Include functions to enhance the usability of account re-certification/re-authorization.

   Response: We added “provide the ability to attach expiration dates/time limits on access controls” as a desired solution characteristic at Line 132.

10. The usability of password management is important.

Response: The IDAM system proposed here can support multiple existing identification schemes including password.

11. Include function for privileged user management, i.e.: user and non-user/service accounts

    Response: This is already mentioned at Line 94.

12. Include functions for role based management: discovery, engineering, assignment, separation of duties, etc.

    Response: The roles will be mapped to both high-level business rules that people can understand and lower-level privileges that the individual systems and machines can understand.

13. Support multiple identity types, e.g. user, non-user, system and service accounts.

    Response: We added “ability to map user access requests via “service” account access” to the Desired Solution Characteristics at Line 133.

14. Include functions for identity warehouse: integration with outside feeds/sensors, security intelligence capabilities and risk-based analytics capabilities.

    Response: These characteristics are outside the scope of this use case but may be a topic for another use case.

15. Include resource integration functions for Windows AD/LDAP, mainframe, Unix/Linux and cloud.

    Response: This is already included at line 14.

16. Address implementation challenges: system must be scalable, work with legacy systems, and be cost effective.

    Response: These elements are already accounted for in the Desired Solution Characteristics section.

17. Add to the Business Value section “Meets compliance obligations.”

    Response: The NCCoE hopes to help organizations meet compliance requirements; however, as a non-regulatory agency, the NCCoE does not set or enforce compliance requirements.

18. In the architecture diagram:
    a. a human resources information system of record needs to include contingent labor and other identity sources (they may be different repositories).

b. show integration with outside feeds

Response: The high-level architecture is notional and not intended to reflect every data source or type. The included HR identity store does not specify the type of identities included therein. Integration with outside feeds may be outside of scope of this use case, but may be considered for a future version.

19. Include attribute based access controls (ABAC) in addition to the traditional role based access controls (RBAC).

    Response: The IDAM system should be able to interface with existing rights management schemes (ABAC/RBAC) that are present on each end system (mainframe, Windows, Linux, etc.). This use case will leverage the other work being done at the NCCoE including an energy sector use case on IdAM and an ABAC building block.

20. Recommend best practices and emphasize standards-based approaches that can improve identity and access management mechanisms in other sectors as well. Publish emerging recommendations as part of this use case.

    Response: The NCCoE is committed to using standards-based products in all of its reference designs. Since this use case is being developed for the financial sector, it must be consistent with rules and regulations for the financial sector. However, we hope it will have broader applicability. Some of the relevant standards have been listed starting at line 148.