NIST SPECIAL PUBLICATION 1800-18A

Privileged Account Management for the Financial Services Sector

Volume A:
Executive Summary

Karen Waltermire
National Cybersecurity Center of Excellence
Information Technology Laboratory

Tom Conroy
Marisa Harriston
Chinedum Irrechukwu
Navaneeth Krishnan
James Memole-Doodson
Benjamin Nkrumah
Harry Perper
Susan Prince
Devin Wynne
The MITRE Corporation
McLean, VA

September 2018

DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/use-cases/privileged-account-management

Executive Summary

- Privileged accounts are used to access and manage an organization's information assets and systems. Often described as the "keys to the kingdom," these accounts are used by trusted users who perform tasks that ordinary users are not authorized to perform.
- Controlling these accounts is challenging, as the very nature of the functions that they perform requires broad access and authority. Additionally, this broad access makes privileged accounts a tempting target for external and internal malicious actors and increases the impact of accidental mistakes.
- Malicious actors can inflict substantial harm, often without notice. Industry reports have identified that privilege misuse is a major component of reported cyber incidents, with estimates up to 80 percent of all data breaches (Forrester 2016).
- To address this challenge, the National Cybersecurity Center of Excellence (NCCoE) has developed a reference design that illustrates how financial institutions can implement a privileged account management (PAM) system to secure, manage, control, and audit the use of privileged accounts.
- This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide describes how financial-services companies can use commercially available technology to implement PAM to reduce the risk associated with privileged accounts.

CHALLENGE

Financial organizations rely on privileged accounts to enable authorized users to perform their duties with little to no direct oversight or technical control of their actions. Companies have difficulty managing these accounts, which, in turn, opens a significant risk to the business. If used improperly, these accounts can cause substantial operational damage, including data theft, espionage, sabotage, or ransom. Malicious external actors can gain unauthorized access to privileged accounts through a variety of techniques, such as leveraging stolen credentials or social engineering schemes. In addition, there are rare instances of disgruntled employees who abuse their accounts, as well as honest employees who make mistakes. Misuse and mistakes can affect both high-value applications (e.g., payment systems) and core systems (e.g., human resources, database access, access control).

Managing privileged accounts is an important, yet complicated, task. Financial institutions often operate highly complex infrastructure and disparate systems that run on multiple operating systems. Managing and controlling access to these privileged accounts is further complicated by the significant pace of workforce and responsibility changes over time. Lastly, changes made at a system level can be used to bypass controls, to hide activity, and to cause financial institutions to breach their stringent reporting and compliance requirements.

SOLUTION

The NCCoE, in collaboration with experts from the financial services sector and technology vendors, developed a PAM system that controls, monitors, logs, and alerts on the use of privileged accounts. The example implementation highlights how organizations can add a security layer between users and the privileged accounts they access. This guide outlines the practical steps to secure privileged accounts in

your organization. We developed representative use-case scenarios to address specific challenges that the financial services sector faces during normal day-to-day business operations.

This guide references NIST guidance and industry standards, including the Federal Financial Institutions Examination Council Cybersecurity Assessment Tool.

The NCCoE sought existing technologies that provided the following capabilities:

- privileged account control
- privileged account command filtering (allow or deny specific commands, such as disk formatting)
- multifactor authentication capability
- access logging/database system
- password management, including storage (vault)
- separation of duties management
- support least privileged policies
- password obfuscation (hiding passwords from PAM users)
- temporary access management
- automated logging and log management (analytics, storage, alerting)
- secure communications between components, where applicable
- ad hoc reporting to answer management, performance, and security questions
- support for multiple access levels for the PAM system (e.g., administrator, operator, viewer)
- protection from the introduction of new attack vectors into existing systems
- a complement to, rather than the replacement of, the existing security infrastructure

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and information-technology system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

Implementing a PAM system is an essential way for financial institutions to effectively secure, manage, control, and audit the activities of privileged accounts. A properly implemented and administered PAM system can help your organization meet compliance requirements, limit opportunity for and reduce the damage that a privileged user can cause, and improve the enforcement of access policies. The NCCoE's practice guide to address PAM for the financial services sector can help your organization:

- identify vulnerabilities and risk factors within your organization
- limit opportunity for a successful attack by improving control over privileged accounts

- improve efficiencies by reducing the complexity associated with managing privileged accounts, which leads to the following results:
  - minimized damage that results from misuse and mistakes by internal/external actors
  - automated enforcement of existing access policies
- simplify compliance by producing automated reports and documentation

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/privileged-account-management. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at financial_nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

BOMGAR EKRAN IdRamp OneSpan RADIANT LOGIC Remediant RSA splunk> tdi technologies

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

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
Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200