Title: Securing and Governing Privileged User Access

Category: Cybersecurity

State: Pennsylvania

Contact: Sandra Patterson, Chief Information Officer, Health and Human Services Delivery Center

Project Initiation and Completion Dates: July 2017 to December 2018

Executive Summary

In today's cyber threat landscape, data breach is one of the major cyber risks impacting large organizations. A common attack vector for these data breaches is compromised privileged account credentials. Privileged accounts, referred to as "the keys to the kingdom", are used by system administrators and applications to perform actions that ordinary accounts cannot.

Unfortunately, privileged users are prone to the same behaviors that can lead to the compromise of regular user accounts, such as creating weak passwords, rarely updating them and sharing with others. Privileged account credentials may also be "hard coded" into applications, making them difficult to change.

The threat of cyber-attacks is real and expensive, and the compromise of a privileged account potentially multiplies the impact of a breach. For centralized government services like Pennsylvania's Health and Human Services (HHS) IT delivery center that supports the Departments of Human Services (DHS), Health, Military and Veteran Affairs, Aging and Drug and Alcohol Programs, the need to protect personally identifiable information (PII) and personal health information (PHI), as well as comply with regulatory and audit requirements, is especially great.

To help safeguard its complex landscape of critical servers, databases and applications, HHS has implemented a comprehensive privileged access management (PAM) solution that secures over 600 privileged credentials used by over 300 privileged account users, along with performing periodic password rotation and session monitoring for user accountability. The PAM solution addresses the major weaknesses associated with privileged credentials by managing passwords without user involvement. This key aspect of the solution eliminates vulnerabilities posed by human error, thereby preventing malicious actors from taking advantage of weak, shared passwords or hard-coded credentials within applications.

In addition to securing privileged credentials, the PAM solution engages business owners to regularly certify which users should have privileged access. This aspect of the solution helps to ensure that only certified users are using privileged accounts. HHS uses the PAM solution to protect critical systems through password management, access certification, around-the-clock session monitoring capabilities along with being compliant with policy requirements.

This comprehensive PAM solution aligns with NASCIO's number one State CIO Top Ten Policy and Technology Priorities for 2019: Security and Risk Management. Additionally, Gartner identified Privileged Access Management as the number one security project for CISOs to focus on in 2018 and 2019. The solution offers an infrastructure for protecting sensitive data from administrative access, while providing governance over those who have that access.

The compliance savings and breach cost avoidance savings from the PAM solution are estimated at $1.8 million per year. With further expansion of the use of PAM solution to additional resources and applications, we will see growing savings, cost avoidance, and increased security.

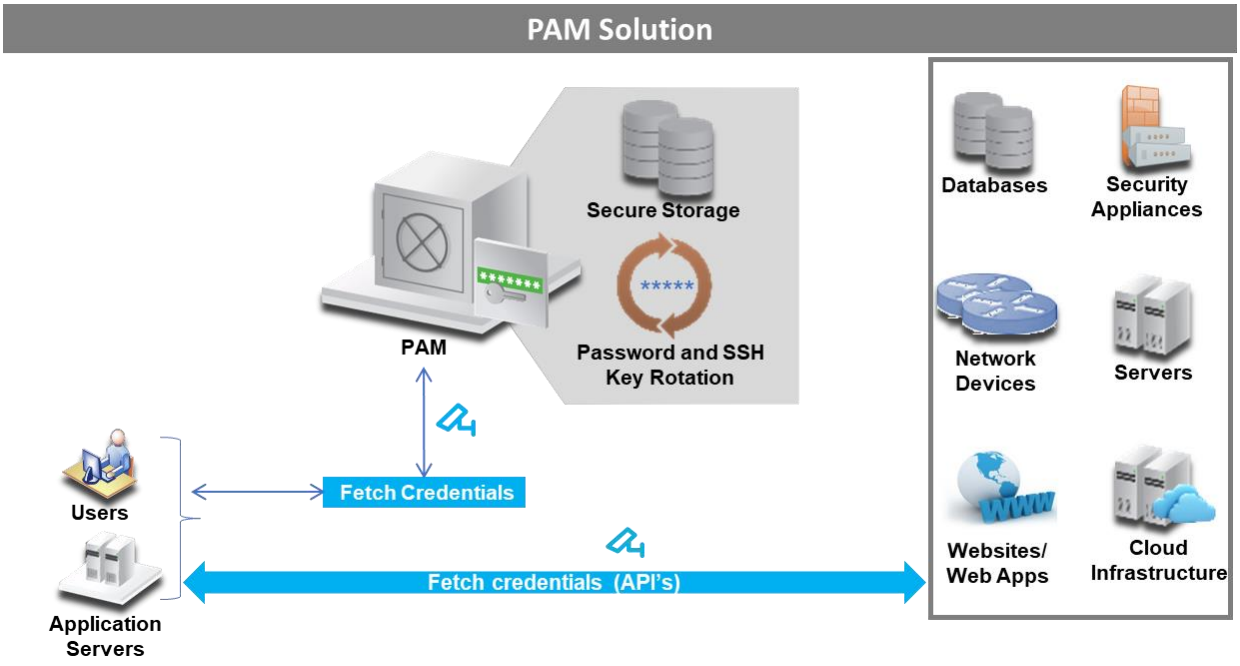
Concept

The PAM solution manages the privileged credentials in two different ways:

- Service Account Management
- Application Identity Management

Service Account Management: When privileged users need to perform administrative activities, they navigate to the PAM solution's intranet portal and 'check-out' the account they need to use. Access to the intranet portal is secured by two-factor authentication consisting of user credentials and a one-time password generated on a mobile device. The solution provides privileged credentials to access a specific secured system without user involvement. The 'privileged session' is video recorded by the PAM solution for auditing purposes. Finally, the privileged account password is rotated as soon as the session is complete. Throughout the process, the user has no exposure to the privileged account's password.

Application Identity Management: Before an application tries to connect with other protected systems for data exchange, it is configured to request a privileged system account credential from the PAM solution. These credentials are then passed along with the request to the downstream system for a successful data exchange. This approach eliminates hard-corded application identities within the application configuration files and gathering corresponding system fingerprints. These credentials are also rotated on a periodic basis with reduced application downtime while meeting regulatory requirements.



Given the power of the administrative service accounts housed in the PAM solution, it is vital to ensure that access is restricted to only those individuals who need it. Unwarranted access to administrative accounts, whether due to changing job functions, errors in provisioning or termination of employment,

increases the risk of improper actions, whether unintentional or carried out in a malicious insider threat scenario. To mitigate this risk, periodic access reviews for privileged users are performed.

HHS maintains an ongoing access certification campaign for users with access to privileged accounts. Prompted by an email notification, managers review users' access within two weeks of access being granted. After initial review, the manager reviews access on a pre-determined frequency to determine if it is still appropriate for the user's job function. The manager can either approve or revoke the access based on the user's business need. Upon revocation, the user's access is automatically removed based on pre-determined rules. This frequency of access verification is determined based on the criticality of the user's risk profile. Access by managers to the PAM solution is also protected by two-factor authentication.

Significance

HHS has leveraged the PAM solution to address both its business and security requirements surrounding privileged access. The solution gives HHS IT staff the privileged access they need to perform their jobs, while keeping the privileged credentials hidden from those users. Below diagram depicts the capabilities of the PAM solution.

PAM Solution Capabilities				
Privileged User Access Control	**Password Rotation for Privileged Accounts**	**Application Identity Management**	**Enhanced Auditing Capabilities**	**Session Recording Capabilities**
Privileged user access control is implemented for Windows/Linux servers, SQL Server database, Remote Business Partner connection to a remote desktop	Periodically rotating passwords for privileged user accounts improves security	Application identity management is implemented to safeguard application service account credentials	Auditing capabilities for privileged user actions is enhanced using Privileged User Management	Session recording of privileged user actions is enhanced using PUM

Along with enhanced security, the PAM solution enhances HHS auditing capabilities. Every privileged session established through the PAM solution is video recorded and stored on a PAM server. Approximately 400-500 account usage sessions per week are recorded and monitored. In the event of a security incident, HHS personnel can review the video recordings to assist with the investigation. Each video recording is tied to the user who accessed the privileged resource through the PAM solution, which gives HHS a tool to identify whose credentials may have been compromised and used to access the privileged resource; or to identify a potential insider threat scenario. This capability helps HHS meet various regulatory requirements in relation to systems that store PII and PHI. In addition, the PAM solution helps manage risks related to internal and external threat scenarios.

Insider threat scenarios exist when a user has authorized access to the IT systems of an enterprise and performs an action that puts those systems at risk. This action can be unintentional such as clicking on a spam email or intentional such as the leak of data by a disgruntled employee. By locking down critical systems so that only PAM accounts can access them, HHS ensures that all access to these systems is

performed in a PAM privileged session. Additionally, the access certification portion of the solution enforces the principle of least privilege; if a user no longer needs access, then their manager will be prompted to revoke that access. As the number of users with access to the PAM solution decreases, it further decreases the risk of an insider threat scenario.

External threats occur when an external malicious actor attempts to gain unauthorized access to IT systems. To further protect against an external threat scenario, HHS integrated the PAM solution with its Risk-Based Authentication solution. When logging into the PAM solution, users are prompted to provide a second form of authentication, such as a one-time password generated on a mobile device. In this scenario, even if the malicious actor steals administrator credentials, it would not allow access to the PAM solution.

Impact

By implementing the PAM solution, HHS has benefited from the reduced common attack perimeter and attained better security incident prevention and monitoring capabilities. Specific benefits include:

Enhanced security and compliance

- **Privileged credentials are no longer shared among privileged users leading to reduced number of privilege accounts**
- **Enables compliance with Federal and State regulatory requirements i.e. CMS MARS-E 2.0, SSA, IRS PUB 1075**
- **Enabled risk-based authentication for privilege user access**

Enhanced risk management

- Hard-coded static authenticators have been removed from over ~280 application configuration files
- Since the inception of access certifications for privilege user accounts, more than one third of the existing privilege account user population access is revoked
- Reduced risk from dormant accounts and excessive entitlements
- Cost avoidance from enhanced security thereby lessening the chances of a potentially expensive breach
- Proactive monitoring of privilege user's access
- Utilization of a common PAM system across multiple servers and applications

Enhanced Efficiencies

- Increased operational efficiencies by performing periodic password rotation resulting in reduced application downtime and reduced business cost due to automation
- Simple, repeatable, processes for onboarding identities and infrastructure to the PAM solution and ease of periodic password rotation meeting compliance requirements
- Simple, repeatable, processes for staging and launching User Access Certification campaigns

Increased user accountability

- Administrators have access to specific privileged credentials as applicable in one portal

- Over 400 privileged sessions are recorded each week and are archived to promote auditability and aid with incident response
- Captures device fingerprint during application-to-application interaction thereby preventing man-in-the-middle attack and eliminating the need for the administrators in knowing service account credentials

As per a study[1] by a leading research analyst firm, the compliance savings from PAM user session monitoring is $613,009 annually and breach avoidance cost savings is $1,268,295 annually.

From a pure risk mitigation perspective, privileged access management is an important control which reduces the risks associated with compromised privileged accounts. HHS is expanding the scope of PAM landscape to include new features, support more platforms and integrate with enterprise Security Information and Event Management (SIEM) solution to provide real time monitoring and alerting of privileged access.

[1] Source: https://www.ca.com/content/dam/ca/us/files/industry-analyst-report/the-total-economic-impact-of-the-ca-privileged-access-manager-solution.pdf