e·DMZ
SECURITY
Compliance-Driven Security Solutions

Introduces

Compliance and Privileged Password Management Considerations for Financial Institutions

[WHITE PAPER]

Written by

Kris Zupan, CEO/CTO
e-DMZ Security, LLC

May 3, 2007

e·DMZ SECURITY

Compliance-Driven Security Solutions

Compliance and Privileged Password Management Considerations for Financial Institutions

Overview / Table of Contents:

This paper will discuss the issue of shared administrative accounts as it relates to today's growing areas of compliance. It covers the following topics:

I . The Issue:

Privileged access and control of administrative accounts for financial systems has been an area of interest for agencies that are responsible for ensuring the integrity of banking systems. This includes the following agencies:

Office of the Comptroller of the Currency (OCC) - The Office of the Comptroller of the Currency (OCC) charters, regulates, and supervises all national banks. It also supervises the federal branches and agencies of foreign banks.

Federal Reserve Board - In addition to monetary policy responsibilities, the Federal Reserve Board has regulatory and supervisory responsibilities over banks that are members of the System, bank holding companies, international banking facilities in the United States, Edge Act and agreement corporations, foreign activities of member banks, and the U.S. activities of foreign-owned banks.

FDIC - An independent agency created by Congress in 1933, the FDIC supervises banks, insures deposits up to $100,000 and helps maintain a stable and sound banking system.

National Credit Union Administration (NCUA) - The National Credit Union Administration (NCUA is the federal agency that charters and supervises federal credit unions and insures savings in federal and most state-chartered credit unions across the country through the National Credit Union Share Insurance Fund (NCUSIF), a federal fund backed by the full faith and credit of the United States government.

Office of Thrift Supervision (OTS) - The Office of Thrift Supervision (OTS) is the primary regulator of all federally chartered and many state-chartered thrift institutions, which include savings banks and savings and loan associations. OTS was established as a bureau of the U.S. Department of the Treasury on August 9, 1989.

Institutions Examination Council - To help enable the effective examination by these separate agencies, there is the Federal Financial Institutions Examination Council. The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS), and to make recommendations to promote uniformity in the supervision of financial institutions.

The Federal Financial Institutions Examination Council publishes various documents explaining the standards used for evaluation. Specifically, we will look at the "Information Security IT Examination Handbook 4." In part of this handbook it discusses Security Controls Information, and—more specifically—"Logical and Administrative Access Control" (see page 15). One of the standards indicates the following: **Prohibiting shared privileged access by multiple users.**

Today's increasing compliance requirements have focused additional attention on how the enterprise manages and controls these critical accounts and passwords. Your specific compliance, regulatory and internal drivers can vary based on your specific industry and market, and can include:

Sarbanes Oxley: Impacting all public companies in the US and internationally if doing business in the US, Sarbanes Oxley (SOX) audits focus on how the enterprise is able to secure and assure complete accuracy of financial information and disclosure. Sections 302 & 404 relate to the effectiveness of internal controls. A developing area of audit focus is being placed on enterprise management, release control and audit of privileged system and application access controls.

Payment Card Industry: Though not a government driven regulation, the Payment Card Industry (PCI) Data Security Requirements apply to all members, merchants and service providers that store, process or transmit cardholder data. Non-compliance with PCI can result in specific contractual penalties and/or revocation of your rights as an enterprise to process credit cards. PCI has numerous and specific areas that require adequate management, control, audit and storage of privileged level accounts and passwords.

Gramm-Leach Bliley Act (GLBA): GLBA requires that "financial institutions" provide adequate protections of personal information collected about individuals. As system level access provides the ability to bypass most file access controls, it is critical that the enterprise have appropriate controls and management of system level access accounts and passwords to meet the requirements of GLBA.

Shared privileged access on distributed systems

The requirement for shared privileged access is unfortunately very real in distributed environments. In Unix operating environments, there is a special privileged account called 'root.' This account is used to perform various system and security functions. In many cases, it is the only ID allowed to perform certain functions. Due to the fact that typically Unix servers are supported by a staff of systems administrators, sharing of this ID becomes very common. One strategy is to prohibit direct login to 'root,' and only allow the privilege through 'su' access. This shows a log of who went to 'root.' This still requires sharing of the 'root' password.

On Windows systems, the Administrator account raises many of the same issues

Though multiple Administrator level accounts are common, there are many examples of the local Administrator account being mismanaged.

For DBMS systems, the problem is with the 'sa' account

This ID has similar power and issues as 'root' or 'administrator' with respect to the database. Since databases serve as the core for many ERP and financial applications, it also is of particular concern.

Operational issues are also associated with these IDs

If the ID is shared by multiple users, changing the password becomes very difficult and dangerous. The password must be available in case of systems problems, which is why the problem is so significant. This leads to many cases where the most powerful ID on a system has a shared password that is not changed.

For embedded/hard coded IDs and passwords

Does the enterprise have IDs and passwords embedded and hard coded into application programs or scripts? If so, how are password changes managed across these applications and scripts?

II. Historic Solutions

Since this issue has existed for many years, solutions have been implemented to address this issue. Some of the most common ways of addressing the issue are:

Store and control the password physically. In many cases, the password is written on a piece of paper, sealed in an envelope, and then stored within a secure location. This storage is then controlled by an operations group, which is tasked with retrieving the correct envelope when needed for system access. Typically, another group is responsible for changing the password of any account that has been used. These process based solutions are sometimes referred to as 'firecall IDs.'

Store and control through an application. The passwords are stored as an excel document, word document, database or other available application tool. Policy and procedures are established to try and control the release, distribution and updates.

Internally developed 'automated' solutions. Solutions developed, maintained and supported in-house to automate, control and audit the release and management of privileged passwords.

III. Deficiencies in Historic Solutions

The most obvious deficiency to an envelope based process is scale. This may work for 20 accounts, but does not scale well to 100 or 4000. The process is also very manual, requiring processes to ensure that an accurate inventory is maintained.

Application based solutions have inherent security issues associated with storage and access. Typically the application was not designed to deliver the level of trust and accountability required for today's compliance driven environment.

Internally developed solutions can have significant life-cycle maintenance costs and may not be able to support the expanding system, device and application requirements.

Other deficiencies with historic solutions can include:

Scale - Manual processes quickly become unmanageable.

Change - How long between when an ID is used, and when it is changed. Also, whether the passwords are rotated based on time and not just usage. Are embedded/hard coded passwords changed, and if so, at what frequency and cost? Is the change process manual or automated?

Individual Accountability - Since a human being sets the password on the managed account, a process needs to ensure that the password is not disclosed prior to being put under control.

Accuracy - Since a human being must transcribe the password onto the paper or document, accuracy becomes a critical issue, especially for strong passwords.

IV. Technology Based Solutions

Commercial Solutions - There are a number of commercial solutions that exist that try to address some of the issues around passwords. These are summarized below:

Identity Management Solutions - Identity Management solutions strive to reduce the number of passwords a user is required to manage. This is done by allowing technology to create a mapping of a single credential to multiple credentials. Different vendors have taken different approaches, but most achieve the same goal of allowing a user to use one credential to access multiple systems.

Identity management does not address the issue of shared administrative accounts. Since these accounts are not 'owned' by any one individual, there is no way to reduce the number of IDs. Also, any synchronization of system account passwords presents a significant security issue, as access to one system implies access to all systems.

Self-Service Password Reset Tools - These tools strive to allow users to reset an unknown password using a known password. This process allows the intermediate server to talk to the target server and reset a credential based on a successful authentication. This theoretically could help with the problem of shared administrative accounts, since the admin account could have a new password generated when required by an individual. The problem with this approach is that it requires the target system to be functioning in normal multi-user mode with network accessibility. In many cases, the shared administrative account is needed to restore a system that has ceased to function normally.

Password Storage Tools - A secure password store provides an alternative to envelopes, but does not address the issue of managing the account on the target system. This solves one part of the problem, but does not eliminate the majority of the manual processes involved in updating and managing the target account.

In-house Developed Solutions - Many organizations have taken the steps to design their own technology solution to address this issue. The end result is typically dependent on the amount of time and resources used to solve the problem. The issues that typically surface in 'built' solutions:

> **Support -** Since this is normally not the core competency of the group, if key individuals leave the organization, the ability to support the solution may be jeopardized.
>
> **Maintenance -** Most solutions are point in time solutions, which typically are not maintained to respond to security threats or new requirements.
>
> **Scalability -** Many times solutions are built to address a current need, and typically do not address scale or availability issues that become apparent as the system is used to manage more systems.
>
> **Quality -** Since many systems are created as 'special projects' or one-offs, the quality may not be as good as the commercial systems they support. Encryption technology and security development guidelines are disciplines that require special skills, so that an application programmer who typically develops workflow systems may not have the required skillset to design a security solution.

V. Design Requirements for an Administrative Password Management Solution

The design requirements for an Administrative Password Management Solution should address the following requirements:

- Password Storage
- Password Release
- Password Update
- Auditing

Password Storage - Since this system will be storing the 'real' passwords, encryption and server security are key areas. The encryption algorithm must be up to the standards of the financial systems that are being protected, currently AES256. Key management must be done in a secure way, and the system which will house the passwords must be hardened to prevent unauthorized access.

Password Release - The password release mechanism should support dual control to help achieve the segregation of duties for the managed accounts. In addition, the release mechanism must be secure (encrypted) and support strong authentication. Granular authorization should allow for systems to only allow the required users to request the password.

Password Update - The system should generate and update the passwords to be managed. Not only does this ensure that strong and random passwords are utilized, but also ensures that individual accountability can be maintained as no user has access to the password until released. The system should also allow passwords to be rotated on a periodic basis, to ensure that these passwords are changed frequently. Finally, the system should be able to change the managed password immediately after use, so that the person requiring access does not have the access any longer than needed.

Dynamic Embedded Passwords - The system should support a full featured CLI and API, to allow hard coded embedded application and script passwords to be replaced with dynamic 'calls' into the system to assure use of the most current password.

Auditing - The system must provide robust auditing so that the process can be reconciled frequently, and reports demonstrating the integrity of the environment can be produced. Reports showing when passwords have been released, password inventories, etc. should all be automatically produced.

In addition, the system must address the following operational issues:

- **Resiliency -** The system should be highly available.
- **Retention -** The system must provide retention criteria and archiving capabilities.
- **Password availability -** The system should verify that managed passwords are correct so that the system can be accessed when needed.

VI. The Password Auto Repository™ (PAR)

The Password Auto Repository (PAR) has been specifically designed to provide a commercial solution to the problem of shared administrative password management. Designed in a purpose built appliance form factor, the PAR addresses the storage, release, and update of administrative passwords.

Storage - The PAR is a purpose built hardened appliance. A commercial embedded firewall (CyberGuard SG640) protects the network interface. No interactive access is allowed. The hard disk is encrypted using

AES256 disk encryption to protect against physical attack. The passwords themselves are also AES256 encrypted prior to being stored on the PAR. The interface to the PAR is HTTPS, which offers token authentication to further strengthen the access control. Connections from PAR to managed systems utilize the strongest available protocol, typically SSH Version 2. The high availability option ensures that these critical passwords are replicated to multiple sites, with an IPsec tunnel protecting the communication between PARs. An encrypted (AES256) backup file is created daily for added resiliency.

Release - The highly granular release mechanism can enforce dual control. SMTP (email) messages are sent from PAR to alert the respective approvers that a request requires their attention. Role based access control (RBAC) is utilized to segregate users into requestors, approvers, administrators, auditors, etc. The release mechanism is done through an HTTPS session, displayed for only 20 seconds at a time to reduce the opportunity for exposure. An CLI/API mechanism allows PAR to be integrated into a current workflow system.

Update - To ensure that individual accountability is preserved, PAR generates a new strong password (with configurable options) and changes the password on the managed system. This auto change feature is currently (v 1.3) available across multiple UNIX variants (Solaris, AIX, HPUX, Linux), Windows (2000, XP and 2003), and multiple firewalls/network devices (Cisco, CyberGuard, Netscreen). In addition PAR can also manage database privileged accounts such as “SA” for Oracle, Sybase and MS SQL Server. PAR is designed to change a managed account password two hours after it has been released. In addition, PAR will ensure that passwords are changed periodically (monthly, etc.) in accordance with a company’s security policy.

CLI & API - PAR supports a full featured CLI and API access into PAR for password retrieval and other functions allowing interaction from required applications and/or scripts replacing fixed hard coded embedded passwords with dynamic calls into PAR.

VII. Summary

As compliance regulation, requirements and audits continue to expand, the tolerance for manual or process driven solutions to the management and control of privileged accounts and passwords will continue to diminish. The historic answer of “best efforts” is becoming unacceptable, driving the need for implementing a solution like PAR. It is truly becoming a question of when—*not if*—the area of privileged password management will become an audit concern for your enterprise.

The PAR has also been embraced by technology leading companies like DuPont, where it is being utilized as a control for Sarbanes Oxley compliance. The fact that the PAR can provide a single solution for many platforms (UNIX, Windows, Cisco) also played into their architectural direction.