beyond passwords: a fine-grained approach to Privileged Identity Management

Russell Miller
Security Management /CA Technologies
# table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive summary</td>
<td>3</td>
</tr>
<tr>
<td>SECTION 1: Challenge</td>
<td>4</td>
</tr>
<tr>
<td>Managing access is a business problem</td>
<td></td>
</tr>
<tr>
<td>SECTION 2: Opportunity</td>
<td>7</td>
</tr>
<tr>
<td>Think ahead!</td>
<td></td>
</tr>
<tr>
<td>SECTION 3: Benefits</td>
<td>10</td>
</tr>
<tr>
<td>Get more from Privileged</td>
<td></td>
</tr>
<tr>
<td>Identity Management</td>
<td></td>
</tr>
<tr>
<td>SECTION 4:</td>
<td>11</td>
</tr>
<tr>
<td>Conclusions</td>
<td></td>
</tr>
<tr>
<td>SECTION 5:</td>
<td>11</td>
</tr>
<tr>
<td>References</td>
<td></td>
</tr>
<tr>
<td>SECTION 6:</td>
<td>11</td>
</tr>
<tr>
<td>About the author</td>
<td></td>
</tr>
</tbody>
</table>
Privileged Identity Management and Virtualization Security

executive summary

Challenge

Privileged Identity Management lies at the core of any program to reduce insider threats. Privileged accounts have the access needed to view and steal sensitive information, as well as to cause damage to an organization’s network. But the risks associated with privileged identities go beyond insiders. When attackers breach a network perimeter as part of a targeted cyber-attack or Advanced Persistent Threat, they nearly always seek to gain access to privileged accounts in order to gain further access to data, to install software such as rootkits and backdoors, and to cover their tracks. Unauthorized access to critical servers can wreak havoc with reputation and brand equity, as well as potentially leaving the organization at risk of significant liability.

A common starting point that organizations deploy in order to reduce the threats posed by their privileged accounts is to control passwords, which is frequently called shared account management or privileged user password management. While important, this approach fails to sufficiently reduce the risks posed by privileged accounts. Controlling access to privileged accounts by only controlling the password does not limit what malicious users can do once they are using the privileged account. Without further controls, an organization is still at significant risk.

Opportunity

Organizations must reduce their risk beyond simply controlling access to their privileged accounts. Fine-grained access controls can be used to control what a person can do after they are logged into an account. Organizations can also use identity controls to implement the security principles of “least privilege” access and “segregation of duties.” Tracking shared account actions to individuals can also lead to accountability for users that are currently anonymous.

Benefits

Advanced Privileged Identity Management capabilities far surpass password management and address the inadequacies of operating system and hypervisor security by offering fine-grained access controls. These capabilities enable organizations to not only protect themselves against insider threats and external cyber-attacks, they can help improve security, simplify and reduce the cost of server administration, and provide significantly improved audit capabilities needed to address regulatory compliance and security best practice requirements.
Section 1: Challenge

Managing access is a business problem

Organizations of all types are storing and processing ever-growing quantities of data. From “Big Data” initiatives to the natural growth of records, information sprawl has become not just an IT issue. Lost or stolen data, such as protected health information (PHI), credit card numbers, social security numbers, confidential employee information and more can impact operations and lead to negative publicity, loss of brand equity, and liability. This affects everyone in an organization.

The nature of the threat

Security threats must be considered from both inside and outside of an organization. Heavily publicized breaches indicate that attacks can come from many sources, from state-sanctioned groups to disgruntled insiders.

While organizations can be targeted in many ways, the most damaging attacks have something in common: the use of privileged accounts, or identities. By their nature, these accounts have the permissions—or privileges—to affect significant change to a system, application, or database. Actions using these accounts have the potential to be uniquely destructive.

When many people think about insider threats, they think of a disgruntled employee or IT administrator, seeking to cause damage or steal and sell sensitive data. This is true in many cases, but it is not the only risk. Naïve insiders can be an entry point into a network by savvy and malicious outsiders. “Social engineering” trickery and techniques such as “spear phishing” (targeted phishing attacks) can enable outsiders to obtain passwords and access to internal resources intended for trusted insiders.

An often-unrecognized risk also comes from what we call “Stopping Stupid”. All people make mistakes—even when using business-critical systems. An unintentional keystroke or momentary loss of focus can lead even a well-intentioned administrator to cause significant damage to systems and data loss.

The risks associated with privileged accounts are varied and complex

One of the most critical risks to a system is shared privileged, or “superuser”, accounts (e.g., “root” in UNIX and Linux and “Administrator” in Windows). The lack of granularity in the enforcement of access rights is one of the most profound problems in system security.
Any administrator who has more entitlements than he or she needs is an active security risk. What is needed is the ability to associate specific access rights to each individual, based on the actual needs of their job function. In this way, each user conforms to the model of “least privilege” access that can help prevent unexpected security problems. In addition, each administrator needs to have an individual identity and needs to be authenticated using that identity. This eliminates the problem of many, essentially anonymous administrators, all sharing the same account with excessive access rights.

This risk is amplified when administrators and developers share a password. This creates a serious lack of accountability because it is difficult, if not impossible, to determine which individual performed a particular destructive act, since there is no tracking of shared account actions back to each individual.

While managing passwords for privileged identities can help prevent unauthorized access to these accounts, that alone cannot enable least privilege access once someone has access to an account. Further controls are needed.

Native Operating System security is inadequate!

Protecting an organization’s most sensitive electronic assets, such as customer databases, hospital patient records or proprietary information, is difficult because native operating system capabilities do not provide adequate protection against inadvertent or intentional attack, nor do they provide reliable auditing of the entire server environment. This problem is intensified when any critical systems or information are exposed to contractors, hosted by service providers, or when the hosting systems for external customers contain confidential data and critical applications.
Operating system access controls are also at risk of being analyzed and avoided because they are known controls. When a malicious attacker gains access to a privileged account—either an outsider with unauthorized access or an insider—a common first step is to do research on the security settings. This includes viewing operating system permissions and looking for vulnerabilities in the controls that can be exploited. Malicious users will also look to modify operating system logs in order to “hide their tracks.” Even on systems where access controls are rigorously enforced, well-trained attackers will simply avoid taking actions that would generate alerts and lead to detection. Only a fully externalized security system can bring unexpected and unknowable elements to a security system and provide the access controls and user activity logs needed to truly secure a system.

Operating systems are also inherently incapable of ensuring the integrity of their own controls. All systems have privileged accounts which can change or bypass that system’s security controls. A user with the proper access can disable the controls necessary to perform an unauthorized action and can modify system log files to erase records of that activity.

Another problem with relying on operating system security controls is their lack of uniformity. There can be significant variance of capabilities and availability of security controls across platforms (e.g., UNIX file/directory controls are significantly different than Windows). This can lead to tangible security issues:

- Security policies must accommodate systems limitations and do not meet business needs
- Errors and omissions caused by added complexity of security management

Don’t ignore the hypervisor

The hypervisor is more critical than an individual physical server, as it can support many virtual machines, not just one. The hypervisor also serves as a single management point to all virtual machine images and as a control for many critical services, creating a vulnerability leverage point. Compromising the hypervisor to download an image or introduce a rogue virtual machine is equivalent to bypassing physical security to break into a server room in order to steal a machine or introduce an external one. Virtualization management applications can be bypassed and the hosting operating system or virtualization console can be accessed directly by privileged users. Due to the unique power of hypervisor administrators, Privileged Identity Management is more critical than ever in virtual environments.

The heart of the problem

The problem with dealing with privileges is that it’s hard. In even a small organization, many people need many different types of access to numerous systems and data. This leads to many organizations tackling password security first, without a well-formed plan to expand their identity controls to offer more comprehensive protection over time.
Section 2: Opportunity

Think ahead!

While much attention is placed on perimeter controls, such as firewalls, organizations are realizing that further controls are necessary. Each individual user should have exactly the privileges he or she needs for precisely as long as needed. This requires a higher level of granularity of identification and access entitlements than is offered by native operating systems or by using privileged user password management controls.

Organizations should plan for continuous improvement of their capabilities, so that they reduce their risks over time. One potential implementation strategy is to focus on the “quick win” that shared account/privileged password management can provide, while planning for more advanced controls. Capabilities such as fine-grained access controls may be a small part of a new implementation, but grow over time to exceed password management in importance.

Figure B.

Privileged Identity Management implementation over time

Organizations should consider their future needs when beginning an initiative to control privileged users.
Privileged Identity Management and Virtualization Security

Fine-Grained Access Controls
When evaluating access controls, organizations should consider how their needs may change over time to encompass increasingly advanced capabilities. A Privileged Identity Management solution should have a wide-ranging list of capabilities that will help ensure the solution will remain relevant and grow with an organization’s security needs over time. Required functionality should include:

- **Virtualization/hypervisor controls.** Control privileged user activity on the hypervisor to enable segregation of duties and least-privilege access on the hypervisor.

- **Superuser (administrator/root) containment.** Inspect all requests at the system level, and enforce authorization based on the defined rules and policies, so that not even the privileged administrative account can bypass the controls.

- **Role-based access controls.** Best practice dictates that each administrator has sufficient privileges to perform his or her job functions and no more. By providing a sophisticated role-based access control environment, administrators are unable to share an administrator password and potentially take advantage of its associated privileges.

- **Network-based access controls.** Today’s open environments require strong control over user access and information flowing over the network. Network-based access control adds another layer of protection to regulate access to the network.

- **Login controls.** Enhance login security by limiting user login by originating IP address, terminal ID, type of login program or time of the day. Limit the concurrent login sessions of a user to enforce stringent user access to a server. Users can be automatically suspended after too many failed login attempts, protecting systems against brute force attacks. Additionally, help ensure secure suspension and revocation of user accounts in distributed environments.

- **Additional granular controls.** Controls that offer specific privileges for file, services and other OS-level (rename, copy, stop, start) functions can be assigned to a specific administrator or an administration group.

- **Different levels of enforcement.** A “Warning Mode” is commonly used by organizations to determine if proposed security policies are too strict or too lenient so they can be modified accordingly.

- **Enhanced ACLs.** Enhanced ACL capabilities can augment the security administrator’s ability to properly assign access rights to authorized users including Program Access Control Lists (PACL), which only allow resource access from a particular program or binary.

- **Impersonation control.** Manage surrogate user delegation capabilities to reduce the exposure of unauthorized users running applications with enhanced privileges and achieve accountability of shared account activity.

“Adopt a “least privilege” model for assigning superuser privileges. Establish more-granular control over and visibility into the way that these privileges are granted and used.”

– Gartner
**Externalized access controls—beyond OS security**

With an external security function, it is often possible to detect and contain attackers much earlier in the process: when an insider or attacker attempts to escalate his or her privileges, change systems security controls or exercise privileges that have not been granted. While an attacker may successfully bypass traditional OS-level controls and logs, external detection processes can catch them unawares. In essence, an organization can implement an access control policy behind the scenes—in a powerful and unexpected way.

In order to provide a comprehensive defense against attacks that use privileged identities, security configurations must be applied as equally as possible to all platforms. Any limitations and inconsistencies must be understood and tracked.

This is another reason that organizations should not solely rely on operating system security. External tools can provide a universal platform to apply a security paradigm across environments, allowing for a centralized, streamlined and business specific approach to security.

**Audit controls**

Reliable audit trails are an essential component of any security solution. Administrators need to track changes to system configuration, and effective incident response depends on reliable audit data. If the need to analyze criminal action arises, you will need to be able to demonstrate that your audit data that is secure and complete. In addition, highly-secure audit logs can dramatically ease the problem of proving compliance with relevant governmental or industry regulations.

Native operating systems do not provide the level of security or assurance for the audit logs that is required for forensic analysis or regulatory compliance. In effect, it is not possible to ensure that the information in log files is either accurate or complete. Anyone who obtains unrestricted privileged access can delete or modify any of the log files of the operating system to cover their tracks.

An effective Privileged Identity Management solution should provide capabilities to improve the accuracy, security and accountability of the audit logs, and:

- Restrict access of audit logs to only the most trusted administrators
- Create audit entries for any administrative action related to the security of any asset, including the audit log itself
- Restrict the ability to change the access policies of the audit log, and audit any attempts to do so
- Provide configurable alarms for any administrator action, including the ability to identify actions that succeed, fail, or both. These configurable actions should be based on the sensitivity of the resource involved. Alarms should also be supported for a range of devices (pagers, email, etc), and a range of definable severity levels
- Audit only events related to specific resources, or for specific individuals
- Provide detailed real-time traces of any defined administrator action
- Provide self-protection against any attacks or attempts to shut down the auditing service
- Consolidate audit logs from distributed systems onto one central system for secure archival and easier correlation and analysis of log information

“You don’t want to gamble with your privileged users; the administrator is the weakest link.”

– Forrester Research
In order to meet the increasing burden of regulatory compliance and standards such as PCI, HIPAA, SOX, and ISO 27001, and to help ensure accountability for administrators, many organizations are looking to record all privileged user activity.

Video session recording can provide a deep understanding of what truly is taking place on corporate servers and desktops. Video replay provides clear-cut evidence of precise user actions. And unlike system logs, video records can show exactly which applications were run and what files or URLs were accessed. This can eliminate blind spots that currently exist for applications that do not produce their own logs, including many of the most common desktop and cloud-based applications. Video logs supported by deep analytical capabilities can be essential to a forensic investigation.

Section 3: Benefits

Get more from Privileged Identity Management

Privileged Identity Management tools have the ability to fundamentally change your approach to security. By controlling not only how individuals gain access to administrative accounts, they can control what people do once they have that access. Each individual can be given only the access required to do their jobs, helping eliminate the security risks associated with excessive privileges.

By implementing a comprehensive Privileged Identity Management solution, you can:

• **Reduce risk.** Mitigate risk by securing privileged user passwords and reducing the risk of password cracking programs being used to gain illegal access to the server or application—thereby reducing risk and increasing data integrity. Enable accountability by tracking all actions back to individuals to facilitate accountability for insiders, including administrators. Also, help to stop "stupid mistakes" by administrators who may unknowingly perform a highly-damaging action.

• **Improve auditing and facilitate compliance.** Track user activity actions by individuals, even those using shared accounts, helping to facilitate compliance.

• **Reduce costs and complexity.** Centrally administer server access policies, user accounts, UNIX authentication and automated management of privileged user passwords to ease the burden of managing security across global, distributed, multi-platform enterprises.

• **Security based on business requirements.** By implementing access controls evenly across operating systems platforms, security can be provided according to business need rather than constrained by system limitations.
Section 4: Conclusions

When planning to control your privileged identities, make sure you think ahead. The controls that you need today may not meet your needs as they evolve. A strong implementation plan will start with a “quick win.” This is very commonly shared account, or privileged user password, management.

Managing passwords for privileged accounts is a starting point towards securing your IT environment, but more needs to be done. You can help ensure all of your environments are protected, implement least-privilege access, streamline your administration, and record all privileged user sessions. These complementary capabilities combine to enable accountability and reduce your risks.

Section 5: References


Section 6: About the author

Russell Miller has spent over six years in network security in various roles from ethical hacking to product marketing. He currently manages marketing for CA Privileged Identity Management and Virtualization Security solutions. Russell has a B.A. in Computer Science from Middlebury College and a M.B.A. from the MIT Sloan School of Management.
CA Technologies (NASDAQ: CA) provides IT management solutions that help customers manage and secure complex IT environments to support agile business services. Organizations leverage CA Technologies software and SaaS solutions to accelerate innovation, transform infrastructure and secure data and identities, from the data center to the cloud. Learn more about CA Technologies at ca.com.