RSA SecurID® Authentication in Action: Securing Privileged User Access
RSA SecurID® solutions not only protect enterprises against access by outsiders, but also secure resources from internal threats

The most critical systems in the enterprise—such as operating system platforms, networking infrastructure and databases—must be administered by privileged users. These users have greater control over the physical and logical infrastructure, and organizations need to implement best practices for controlling and logging privileged user access.

Two-factor authentication of privileged users helps organizations to ensure that these influential employees prove their identities before making administrative changes to systems. By deploying RSA SecurID® solutions, organizations can protect access to critical systems, track and monitor privileged user access and manage the credentials of IT administrators so they can only access the systems for which they are responsible. RSA SecurID solutions not only protect enterprises against electronic access from outsiders, but also secure enterprise resources from internal threats.

Granting – and Securing – Privileged User Access

A privileged user is one who is allocated powers within the computing system that are significantly greater than those available to the majority of users. Providing privileged users with increased control over computing systems is essential, because the enterprise needs highly skilled technical professionals to administer systems, infrastructure and applications. Privileged users are responsible for the performance of the computing system; creating and maintaining user accounts; troubleshooting operational issues; administering system upgrades and any reconfigurations required in the course of ongoing operations.

Privileged users have the ability to manipulate infrastructure and application configurations, and with this increased power comes increased responsibility—and increased security risks for the enterprise. Examples of privileged users include:
- Systems administrators,
- Network administrators,
- Application support engineers,
- Database administrators (DBAs),
- Help desk staff and
- IT executives.

These hard-working professionals are crucial for designing, maintaining and evolving the computer and communications systems at the heart of many organizations. These administrators need the ability to instantly access IT resources so they can tune systems to support business processes and high performance for end-users.

While organizations traditionally focus on protecting systems from external attack, it is essential to protect enterprise systems from threats coming from inside the enterprise. The management of users and groups that have privileged access is essential for protecting enterprise resources. Although many organizations encourage privileged users to be constantly alert, they should also be alert to the need to monitor and manage the activities of the privileged users themselves to protect against abuse.

“An Insider Threat Survey” conducted last year by the Computer Emergency Response Team (CERT) at Carnegie Mellon University found that 57 percent of insider security attacks identified were carried out by employees who at one time had privileged user status. It is not enough to monitor the behavior of holders of user accounts—organizations should also monitor the behavior of privileged users to prevent potential fraud and abuse.

Two-factor authentication not only protects the enterprise from the possibility of data theft or fraud by privileged users—it also protects privileged users themselves by enabling a clear audit trail of activity. By logging authentication activity, organizations can pro-actively identify potential risks and prevent
unwanted access. They can also perform forensics on violations to determine the root cause of security violations and clear innocent privileged access users of any wrongdoing.

Protecting enterprise information can be a double-edged sword. While organizations are increasingly taking steps to protect access to information, collaboration and collusion by employees becomes a greater threat. Criminals intent on accessing enterprise systems can use covert measures—such as stealing user passwords—or overt measures, such as blackmailing or threatening a privileged user to gain access. Insider collaboration can be unwitting (by thieves stealing passwords) or intentional. Carefully monitoring access activity is a responsible step for businesses to take to ensure best practices for protecting information.

Organizations have to protect systems against individuals who have fraudulently obtained privileged access credentials, and passwords are insufficient for protecting access by privileged users. They are frequently lost and can be easily stolen, and the theft of a privileged user’s password could potentially result in a devastating impact on enterprise operations.

Organizations also have to protect systems against disgruntled privileged users who may seek to harm the enterprise by disrupting the operations of business systems. An unhappy privileged user could potentially delete critical information, disable the network or prevent users from accessing the information they need to perform their jobs. The ability to centrally manage the access credentials for privileged users is essential so that organizations can easily revoke the privileged access privileges of a disgruntled administrative user.

Best Practices for Protecting Access
CERT found that 20 percent of all electronic crimes are committed by insiders, and concluded that the primary motives for attacks from insiders is a response to a negative event or revenge against the employer. CERT developed the following summary of best practices:

- Conduct background checks
- Institute periodic employee security training
- Enforce separation of duties
- Implement strict password and account management policies
- Log, monitor and audit employee online actions
- Use additional controls for systems administrators and privileged users
- Actively defend against malicious code
- Use layered defenses against remote attacks
- Monitor and respond to suspicious or disruptive behavior
- Deactivate access following termination
- Collect and save data for use in investigations
- Implement secure backup and recovery processes
- Clearly document insider threat controls

An unhappy privileged user could potentially delete critical information, disable the network or prevent users from accessing information.
The Need for Two-factor Authentication

Organizations can protect enterprise information and operations by deploying two-factor authentication solutions from RSA, The Security Division of EMC. RSA products help organizations protect private information and manage the identities of people, devices and applications accessing and exchanging that information. RSA SecurID® two-factor authentication is based on something you know and something you have, providing a much more reliable level of user authentication than reusable passwords.

RSA SecurID authentication has been on the market for over 15 years—with no reported security breaches. RSA SecurID authentication tokens provide "hacker-resistant" two-factor authentication, resulting in easy-to-use and effective user identification.

Based on RSA’s patented time synchronization technology, authentication tokens generate a simple, one-time authentication code that changes every 60 seconds. To access resources protected by the RSA SecurID system, users simply combine their secret personal identification numbers (PINs)—something they alone know—with the token codes generated by their authenticators—something they carry.

The result is a unique, one-time-use passcode that is used to positively identify—or authenticate—the user. If the code is validated by the RSA SecurID system, the user is granted access to the protected resource. If it is not recognized, the user is denied access.

Organizations worldwide already rely on RSA SecurID solutions for two-factor authentication from their desktop or from a remote PC. RSA offers a wide range of SecurID authenticators—from hardware tokens that can fit in a wallet or are small enough to attach to a key chain to software tokens usable on a laptop, phone or BlackBerry. Two-factor authentication not only enables secure access for privileged users, it can also be deployed to the entire user community to protect access to information and prove the identities of users accessing critical business applications.

Locking Down Infrastructure Access

Two-factor authentication allows companies to positively identify a privileged user before that user is granted access. Companies can lock down enterprise infrastructure and require privileged users to authenticate before accessing critical infrastructure, including:

- **Routers and Switches** – Networking infrastructure is essential for delivering information and ensuring the ongoing performance of business processes, and privileged users should authenticate before changing the configurations of routers and switches. Reconfiguring routers and switches can shut down the network or disrupt access for certain floors, departments or buildings. By entering something they know—their PIN—and something they have—the constantly changing passcode on their token—privileged users can authenticate before being granted access privileges.

- **Remote Access Equipment** – Virtual private network (VPN) and remote access servers should also require privileged users to authenticate. This protects the enterprise from attacks emanating from beyond the boundaries of the enterprise. Organizations can centrally monitor the activities of privileged users to prevent the creation and utilization of rogue accounts that provide remote access to unauthorized users.

- **Firewalls** – Just as organizations rely on firewalls for protecting the enterprise from external attacks, organizations should also protect firewalls from potential internal attacks. A privileged user could potentially change the port settings on firewalls to expose the enterprise to attack, resulting in a “the front door is locked, but the windows are open” scenario that potentially harms enterprise applications.

- **Remote Administration** – It is essential that privileged users gain remote administrative privileges so they can maintain and troubleshoot servers in remote data centers or infrastructure in small offices. Two-factor authentication can enable secure remote administration to centrally protect the security in offsite locations.
Web Servers – The corporate website has become the primary face of most organizations. If web servers are not properly secured with two-factor authentication, they can more easily be hacked, resulting in websites being defaced, hijacked or taken down entirely. It is critical that only privileged users have the ability to create, edit and delete web content, set access and file policies, and access log files. Securing access to web servers protects not only organizational productivity but also the value of the company brand.

Locking Down Server Platforms
Local and remote server platforms process the information that runs a business, and while privileged users need the ability to instantly configure and adapt server platforms, the organization needs the ability to monitor access to server settings. Two-factor authentication allows the organization to protect access to application servers, web servers and file servers, and it enables cross-platform security across Microsoft Windows®, Linux and Unix server platforms.

Access to a server through a privileged user account could have a devastating effect on a business. For example, a hostile user with a privileged user account could erase saved data, add or delete users, mine human resources of social security and birthday information to enable identity theft, steal financial reports and make trades based on this illegally obtain information or siphon off intellectual property by gaining illegal access to product development or corporate strategy documents.

Best practices for securing the enterprise require organizations to lock down server platforms, and two-factor authentication enables the centralized management of credentials so the organization can carefully define who has privileged access to what information and which server resources.

Locking Down User Administration Functions
There are many user administration functions that must be secured to prevent damage by corrupt privileged users. Organizations need to protect the integrity of all databases as well as the database schema to ensure ongoing operations and prevent exposure to the risk of lost or stolen information.

Private information, such as human resources data, e-mail information or accounting reports, needs to be secured from prying eyes. Information assets—such as software source code—must be carefully secured, and organizations must have the ability to provide access to valid users while locking out invalid user accounts. User administration functions for managing access...
Because the RSA Authentication Manager software logs all transactions and user activity, it can be utilized as an auditing, accounting and compliance tool. It includes report templates that can be easily tailored to administration needs, including activity, exception, incident and usage summaries.

With Authentication Manager software, an audit trail of each login attempt and operation performed is automatically generated. Audit trails extend to the user, which helps prevent losses from insider abuse or employee laxness regarding security policies. The automated log maintenance feature lets administrators create settings for archiving log files. This “set and forget” feature ensures that usage logs are safely preserved without intervention. Reports can be designed to view an activity, exception or incident, as well as usage summaries.

RSA SecurID solutions not only help organizations to protect user access and privileged user access, they also help organizations to comply with regulatory requirements for protecting information, such as the Sarbanes-Oxley Act for protecting financial information or the HIPAA regulations requiring healthcare providers to protect patient records. By centrally tracking privileged user access activity, the enterprise can monitor illegal access attempts, detect abuse trends, enable compliance with regulatory initiatives and provide oversight over privileged users that is both prudent and reasonable. Organizations can understand how, when and why privileged users are accessing systems, and centrally track and manage administrative access to business systems. The enterprise can manage access privileges over time and upgrade a user’s access privileges or revoke credentials as needed.

Organizations can also manage security and track privileged user activity by selecting an appliance-based solution. The RSA SecurID Appliance is based on RSA Authentication Manager software and is available as an integrated, rack-mountable hardware appliance.

RSA SecurID solutions not only help organizations to protect user access and privileged user access, they also help organizations to comply with regulatory requirements for protecting information, such as the Sarbanes-Oxley Act for protecting financial information or the HIPAA regulations requiring healthcare providers to protect patient records. By centrally tracking privileged user access activity, the enterprise can monitor illegal access attempts, detect abuse trends, enable compliance with regulatory initiatives and provide oversight over privileged users that is both prudent and reasonable. Organizations can understand how, when and why privileged users are accessing systems, and centrally track and manage administrative access to business systems. The enterprise can manage access privileges over time and upgrade a user’s access privileges or revoke credentials as needed.

Organizations can also manage security and track privileged user activity by selecting an appliance-based solution. The RSA SecurID Appliance is based on RSA Authentication Manager software and is available as an integrated, rack-mountable hardware appliance.
Leveraging Agents to Protect Applications

RSA® Authentication Agent software enables e-business by controlling access to corporate networks and web applications. Combined with SecurID authenticators and the Authentication Manager authentication engine, RSA Authentication Agents protect sensitive data assets stored within the enterprise by requiring two-factor authentication before access is granted.

Authentication Agent software functions like a security guard, enforcing security policy as established by the Authentication Manager. The software intercepts access requests and requires designated users or groups—whether local or remote—to authenticate to the Authentication Manager or the RSA SecurID Appliance via a SecurID authenticator prior to gaining access to protected resources.

RSA Authentication Agent software enables use of the same RSA SecurID authenticators to protect an unlimited number of resources—providing a high return on investment. Simply configure the Agent built into and designed to work with an application and that resource is instantly protected with RSA SecurID two-factor authentication. In addition, central user administration means that new users can be added and new systems protected with minimal effort.

Turnkey Interoperability with Existing Infrastructure and Applications

RSA Authentication Manager software and the RSA SecurID Appliance are interoperable with many of the major network infrastructure and system products on the market—including more than 300 products from over 200 vendors—providing maximum flexibility and investment protection.

Through the RSA Secured® partner program, leading vendors of remote access products, VPN platforms, firewalls, wireless network devices, web servers and business applications have built RSA Authentication Manager compatibility into their products. They have created or installed their own RSA Authentication agents to enable seamless interoperability with SecurID solutions. For more information on the RSA Secured partner program—including products that are certified as compatible with RSA solutions, visit the RSA Secured Solutions Directory at http://rsasecurity.agora.com/rsasecured/.

Summary

Providing privileged users with easy access to enterprise resources is essential for ensuring the ongoing operation of business applications and infrastructure, but it is important to manage the identities of privileged users and centrally monitor and control access to servers, network equipment, firewalls and applications to protect enterprise resources. While privileged users are primarily stellar employees, a disgruntled or compromised privileged user could wreak havoc on enterprise systems and it is important to centrally monitor and manage access privileges so organizations can effectively control access to information.

RSA offers proven, two-factor authentication solutions that allow the enterprise to safeguard corporate resources. Privileged users can rely on RSA SecurID solutions to gain the access they need to support enterprise computing and communications, and the organization can capture and monitor usage to protect enterprise assets and ensure the ongoing operations of applications, databases, networks and information systems.
RSA is your trusted partner

RSA, The Security Division of EMC, is the expert in information-centric security, ensuring the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.