Risk Insights

Brought to you by: Schauer Group

Proper Password Management

Passwords are used in many ways to protect data, systems and networks. They are used to authenticate users of operating systems (OS) and applications such as email, labor recording and remote access. Passwords are also used to protect files and other stored information, such as password-protecting a single compressed file, a cryptographic key or an encrypted hard drive. In addition, passwords are often used in less visible ways; for example, a biometric device may generate a password based on a fingerprint scan, and that password is then used for authentication.

Password Management

Effective password management reduces the risk of compromise of password-based authentication systems. Organizations need to protect the confidentiality, integrity and availability of passwords so that only authorized users can use passwords successfully as needed. Integrity and availability should be ensured by typical data security controls, such as using access control lists to prevent attackers from overwriting passwords and having secured backups of password files

Ensuring the confidentiality of passwords is considerably more challenging and involves a number of security controls along with decisions involving the characteristics of the passwords themselves. For example, requiring that passwords be long and complex makes it less likely that attackers will guess or crack them, but it also makes the passwords harder for users to remember. This increases the likelihood that users will store their passwords insecurely and expose them to attackers.

Organizations should be aware of the drawbacks of using password-based authentication. There are many types of threats against passwords, and most of these threats can only be partially mitigated. Also, users are burdened with memorizing and managing an ever-increasing number of passwords. Although the existing mechanisms for enterprise password management can somewhat alleviate this burden, they each have significant usability disadvantages and can also cause more serious security incidents because they permit access to many systems through a single authenticator. Therefore, organizations should make long-term plans for replacing or supplementing password-based authentication with stronger forms of authentication for resources with higher security needs.

Authentication can involve something the user knows (e.g., a password), something the user has (e.g., a smart card), or something the user "is" (e.g., a fingerprint or voice pattern). Single-factor authentication uses only one of the three forms of authentication, while two-factor authentication uses any two of the three forms and three-factor authentication uses all three forms.

Using multiple factors makes it more difficult for someone to gain unauthorized access to the system—it is easier to either discover a user's password or steal the user's smart card than it is to both steal the smart card and discover the user's password. To meet various security and operational needs, the selection of authentication methods varies among systems, but passwords are the most commonly used authentication method, and are often used both by themselves and with other authentication factors.

Protecting Your Passwords

Organizations should implement the following recommendations to protect the confidentiality of their passwords:

- **Create a password policy that specifies all of the organization's password management-related requirements.**

  Password management-related requirements include password storage and transmission, password composition, and password issuance and reset procedures. In addition, organizations should also take into account applicable mandates (e.g., Federal Information Security Management Act of 2002 (FISMA)), regulations and other requirements and guidelines related to passwords.

  An organization's password policy should be flexible enough to accommodate the differing password capabilities provided by various OSs and applications. Organizations should review their password policies periodically, particularly as major technology changes occur (e.g., new OS) that may affect password management.

- **Protect passwords from attacks that capture passwords.**

  Attackers may capture passwords in several ways, each necessitating different security controls. For example, attackers might attempt to access OS and application passwords stored on hosts, so such passwords should be stored using additional security controls, such as restricting access to files that contain passwords and storing one-way cryptographic hashes of passwords instead of the passwords themselves. Passwords transmitted over networks should be protected from sniffing threats by encrypting the passwords or the communications containing them, or by other suitable means.

  Users should be made aware of threats against their knowledge and behavior, such as phishing attacks, keystroke loggers and shoulder surfing, and how they should respond when they suspect an attack may be occurring. Organizations also need to ensure that they verify the identity of users who are attempting to recover a forgotten password or reset a password, so that a password is not inadvertently provided to an attacker.

- **Configure password mechanisms to reduce the likelihood of successful password guessing and cracking.**

  Password guessing attacks can be mitigated easily by ensuring that passwords are sufficiently complex and by limiting the frequency of authentication attempts, such as having a brief delay after each failed authentication attempt or locking out an account after many consecutive failed attempts. Password cracking attacks can be mitigated by using strong passwords, choosing strong cryptographic algorithms and implementations for password hashing and protecting the confidentiality of password hashes. Changing passwords periodically also slightly reduces the risk posed by cracking.

  Password strength is based on several factors, including password complexity, password length and user knowledge of strong password characteristics. Organizations should consider which factors are enforceable when establishing policy requirements for password strength, and also whether or not users will need to memorize the passwords.

- **Determine requirements for password expiration based on balancing security needs and usability.**

  Many organizations implement password expiration mechanisms to reduce the potential impact of unauthorized password use. This is beneficial in some cases but ineffective in others, such as when the attacker can compromise the new password through the same keylogger that was used to capture the old password.

  Password expiration is also a source of frustration to users, who are often required to create and remember new passwords every few months for dozens of accounts, and thus tend to choose weak passwords and use the same few passwords for many accounts. Organizations should consider several factors when determining password expiration requirements, including the availability of secure storage for user passwords, the level of threats against the passwords, the frequency of authentication (daily versus annually), the strength of password storage and the effectiveness or ineffectiveness of password expiration against cracking.

  Organizations should consider having different policies for password expiration for different types of systems, operating systems and applications to reflect their varying security needs and usability requirements.