CAPINTECH

Application Security: Recommendations and Next Steps

By Allison Davis, Senior Manager

As we mentioned in the first part of this series, hackers have many reasons for attacking organizations. But whether a hacker's goal is to wreak havoc, disrupt operations, or steal sensitive information and data, your password management practices could be the layer of control that prevents the realization of the attack.

Various regulatory and governing bodies, societies, and institutes have different guidelines for minimum standards, and these recommendations often change as the threat landscape evolves. When evaluating them, remember that these recommended standards are just that: recommended.

All organizations operate differently and have varying needs and constraints. What may work for one organization is not necessarily effective for another. However, your organization should become familiar with your configured settings and various recommended standards. From there, you can evaluate the deviations.

Our Recommendations

Now let's review our application security recommendations in light of the threats. For each setting, we discuss what the control means, how it can mitigate risk, and our recommended setting.

Setting	Purpose	Recommend Value
Password Parameters		
Password Minimum Length	The minimum number of characters a password must have. Longer passwords are typically harder for hackers and password-cracking software to breach.	8 characters
Password Complexity	The types of characters a password must contain, including alphabetical, numerical, or special characters. Complex passwords are typically harder for hackers and password-cracking software to breach.	A combination of at least 2 of the 3 categories
Password Expiration	The number of days until a password is required to be changed. Expiration settings are important to mitigate the risks associated with password database breaches. If a password is compromised in a breach but is changed frequently, it reduces the likelihood that the password obtained in the breach will still be valid.	Every 90 – 180 days
Password Minimum Age	The number of days a user must wait before changing his or her password again after a password reset. This setting prevents a user from changing an expired password and then immediately changing it back to the original, expired password.	1 day
Password History	The number of passwords remembered by the system. This setting works with the minimum age setting. If the minimum age is one day and the history is five passwords, the user would have to change his or her password five days in a row to get back to the original password. If the minimum age is 90 days and the history is four passwords, the same password could not be used for nearly a year.	3 – 5 passwords

Setting	Purpose	Recommend Value
Account Lockout Settings		
Lockout Threshold	The number of consecutive invalid attempts allowed before a user is locked out. This setting is critical for reducing the likelihood of a successful brute force attack.	3 – 5 invalid attempts
Lockout Duration	The period of time the user is locked out after the threshold is met. This setting is critical for reducing the likelihood of a successful brute force attack.	Require administrator reset to unlock
Lockout Counter Reset	The amount of time that must pass after an invalid login before the failed attempt counter resets. This setting is critical for reducing the likelihood of a successful brute force attack.	At least one day (1,440 minutes)
Other Settings		
Inactivity Timeout	The number of minutes of inactivity before the system automatically logs the user out. This setting is critical for preventing unauthorized access if a user is logged in and leaves the application running and unattended.	Maximum of 15 minutes
Multi-factor Authentication (MFA)	An additional layer of authentication that is a combination of something you know (e.g., user ID and password), something you have (e.g., token, IP address), and/or something you are (e.g., biometrics). This setting is critical to reduce the risk of unauthorized access if a valid password is obtained via password guessing, brute force attacks, or a database breach. Note: Challenge questions were once viewed as a form of MFA, but these are no longer deemed sufficient.	Enable for all externally accessible and high-risk systems

Justifying Deviations

In a previous post, we delved into three steps for creating stronger passwords:

- Understanding the challenges and inherent weaknesses associated with passwords
- Understanding the National Institute of Standards and Technology (NIST) recommendations for password generation
- Layering controls

Some organizations have misconstrued the intention of these recommendations to mean that we don’t need complex passwords of a certain length that change frequently. While NIST acknowledges that some of the controls we have relied on in the past, such as password complexity, length, and expiration, may not be as effective as they once were, it is not saying that these controls are not important. Instead, NIST is reinforcing the idea of a layered control framework and encouraging organizations to look into other application security controls, such as account lockout settings and MFA, with a renewed focus. Rather than considering these settings independently, it’s important to look at them together in layers to determine what you truly need to mitigate your risk.

Many organizations justify the reduction of password complexity and expiration requirements with the implementation of conservative account lockout settings and MFA; however, it’s important to recognize that there are unique risks with data breaches involving encrypted passwords. When a database is breached, a hacker can use tools to run a brute force attack against the database, even if the database is encrypted. Because the hacker is running a brute force attack against the database itself and is not actively trying to use a brute force attack to log into a system, lockout settings and MFA do not provide a control against the passwords being obtained. That means password complexity and expiration are extremely important.

Again, let’s think about what complexity and minimum length do. The longer and more complex a password is, the less likely it is that a brute force attack and password-cracking software will obtain a valid password. Similarly, requiring more frequent expiration reduces the likelihood that one of the passwords in the database is even valid once it’s cracked.

Therefore, we recommend using extreme caution when trying to justify deviations from these recommended settings.

Next Steps

Many people want hard and fast rules. So what steps should you take now?

First, ask these questions:

- Do we have weaker settings that we should enhance?
- Will these enhancements have a significant impact on our user base?
- Does the financial, support, and operational cost associated with implementing the settings outweigh the benefit of increased security?
- Are there other mitigating factors that reduce the risk of these deviations?

You can then consider the following steps to enhance your application security controls for increased peace of mind.

1. **Establish baseline controls for all applications**. What are your minimum required settings for *all* applications? It's especially important to establish a baseline in a decentralized environment where multiple individuals administer the control settings and may not realize what settings they should enable.
2. **Develop a process for addressing deviations from this baseline**. Not all applications are the same, and you may run into situations where you cannot apply the baseline standard. Ensure there is a process for approving deviations and configure the settings as close to the baseline as possible. Consider contacting the vendor to ask about future enhancements.
3. **Document and revisit your settings**. Document the baselines, your application configurations, and any deviations that need to be monitored. Don't set and forget. Revisit the controls annually to ensure the settings still mitigate the risks to a level that is within your risk appetite.
4. **Consider simplifying authentication via single-sign-on (SSO) systems**. Many organizations are moving toward SSO. While SSO systems can be expensive and do require management, once implemented they can significantly strengthen the authentication process. Because users only need to remember one strong password, they are more likely to comply with the strong password requirements and are less likely to write passwords down. SSO can also provide a significant increase in security and authentication controls when coupled with MFA.

Taking the time to inventory, assess, and address your organization's application settings is an important step in protecting your network, data, and employees. Once you've gone through the initial steps, be sure to review your settings annually to make any necessary adjustments.

If you have any questions about application settings or other cybersecurity issues, please contact us at cybersecurity@capincrouse.com. We're here to help!

About the Author

Allison Davis, Senior Manager
CapinTech
adavis@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor and senior manager, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

About CapinTech

Capin Technology, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintechnology.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA

© 2020 Capin Technology LLC