NIST’s New Password Rule Book: Updated Guidelines Offer Benefits and Risk

The updated US National Institute of Standards and Technology (NIST) standards on password security published in the NIST Special Publication (SP) 800-63-3 "Digital Identity Guidelines"[1] represent a novel approach to improve IT security while working with, rather than against, the capabilities and limitations of the weakest link in information security: the users themselves. The updated NIST guidelines offer adopters a number of advantages in usability and security while introducing new risk and implementation challenges. These issues should be carefully considered before, during and after implementation of the new guidelines.

Overview of the New Guidelines

Previous NIST guidelines advocated a conventional approach to password security based on policies such as strict complexity rules, regular password resets and restricted password reuse.[2] NIST’s new standards take a radically different approach.[3] For example, password changes are not required unless there is evidence of a compromise, and strict complexity rules have been replaced by construction flexibility, expanded character types, greater length and the prohibition of “bad” (i.e., insecure) passwords. NIST’s new guidelines have the potential to make password-based authentication less frustrating for users and more effective at guarding access to IT resources, but there are tradeoffs.

The password requirement basics under the updated NIST SP 800-63-3 guidelines are:[4]

- **Length**—8-64 characters are recommended.
- **Character types**—Nonstandard characters, such as emoticons, are allowed when possible.
- **Construction**—Long passphrases are encouraged. They must not match entries in the prohibited password dictionary.
- **Reset**—Required only if the password is compromised or forgotten.
- **Multifactor**—Encouraged in all but the least sensitive applications.

Benefits and Risk, From the User’s Perspective

The updated NIST password guidelines are designed to enhance security by addressing the human factors that often undermine intended password protection. Under the traditional approach to password construction, users are asked to generate highly complex and difficult-to-guess passwords. These passwords must be reset on a regular schedule, and restrictions generally prevent users from consecutively recycling passwords. Users are also instructed to refrain from using the same or similar passwords on multiple IT systems. As all users know, this makes remembering passwords very difficult. Otherwise well-intentioned individuals often cope with these challenges by ignoring advice and defaulting to common, easy-to-remember passwords, cycling previously used passwords, and making only minimal changes between resets, among other effort-reducing strategies.[5] Others simply write them down and post them in a convenient, but insecure location.[6]

Under the new guidelines, users are encouraged to select longer, memorable passphrases rather than cryptic character strings with complex construction rules, as it is easier for users to remember coherent phrases than strings of random characters. This same logic inspired conventional advice to generate secure passwords via acronyms based on easily remembered phrases that are meaningful to the user (e.g., taking the first letter of each word in the phrase “Robert has been a Spartans fan since 2010!" would generate "RhbaSfs2010!").[7] This 12-character acronym generally meets strict password construction requirements and provides sound security. However, the new NIST standards encourage the use of the entire passphrase rather than just the acronym. The 44-character original phrase presents a much greater cryptographic challenge to crack than the 12-character acronym and is probably easier for the user to remember. **Figure 1** compares the NIST password approach to the traditional password approach.

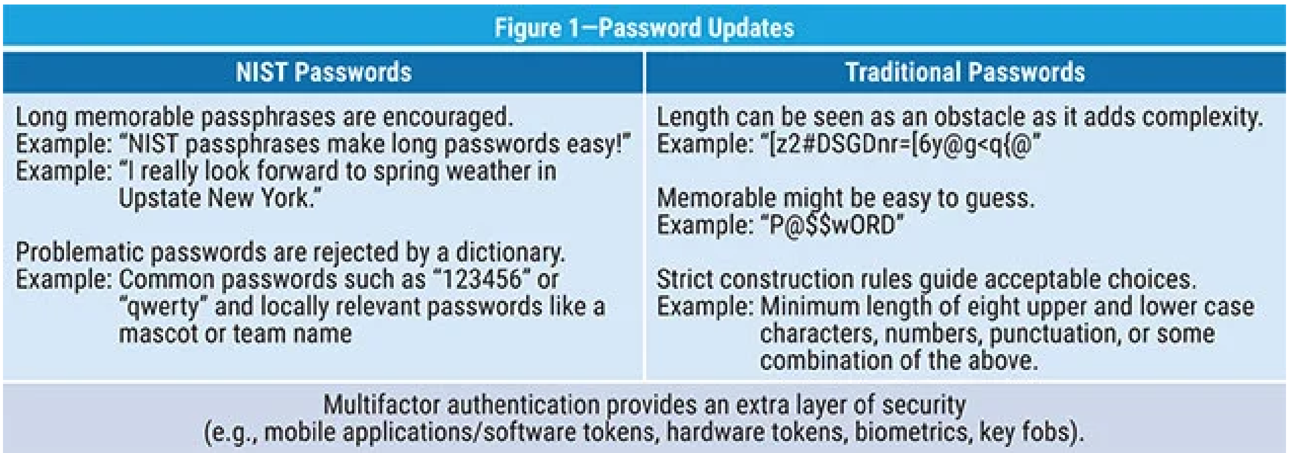

Figure 1—Password Updates

NIST Passwords	Traditional Passwords
Long memorable passphrases are encouraged. Example: "NIST passphrases make long passwords easy!" Example: "I really look forward to spring weather in Upstate New York."	Length can be seen as an obstacle as it adds complexity. Example: "[z2#DSGDnr=[6y@g<q{@"
	Memorable might be easy to guess. Example: "P@$$wORD"
Problematic passwords are rejected by a dictionary. Example: Common passwords such as "123456" or "qwerty" and locally relevant passwords like a mascot or team name	Strict construction rules guide acceptable choices. Example: Minimum length of eight upper and lower case characters, numbers, punctuation, or some combination of the above.
Multifactor authentication provides an extra layer of security (e.g., mobile applications/software tokens, hardware tokens, biometrics, key fobs).	

The new guidelines offer users increased flexibility and security without necessarily forcing them to change their concept of a secure password. While the guidelines facilitate and encourage the use of longer passphrases, the only construction restriction imposed under the NIST guidelines is a minimum eight-character password length. As such, users are not actually required to create passwords that are appreciably different from those to which they are accustomed under traditional complexity rules. They need only ensure that their password or passphrase is of sufficient length and does not appear in a dictionary of prohibited passwords.

Users will also appreciate not having to change their password on a predefined schedule. Regular password changes, which prevent the use of compromised passwords over an extended period of time, create headaches for users who must continually generate and remember new passwords. Users often compensate by making only small modifications to the password (such as adding or switching a single character), which undermines the intent of the policy. The increased effort incurred by forcing users to make regular password changes most likely outweighs the potential benefit unless there is evidence of a system breach or reason to believe a particular account has been compromised.[8] Correspondingly, the new NIST guidelines recommend password resets only in cases where there is a suspected threat rather than forcing resets on a set schedule.

While the updated guidelines make secure password practices easier for users in a number of ways, they also introduce potential problems and pain points. For example, the NIST guidelines require a dictionary validation step whereby commonly used and otherwise insecure passwords are rejected based on a specialized list. In the absence of specific construction rules or transparency into the prohibited list itself, users may become frustrated if they encounter a series of rejections. Moreover, for some users, a message simply stating that their desired password was not accepted because it appears on a prohibited list may not be enough information to make their subsequent attempts successful. For users to take full advantage of the opportunities for increased security, targeted training and support may be necessary. At the very least, users need basic guidance on how to select acceptable passwords under the new NIST guidelines or they may become frustrated with the process.[9]

A lingering threat is the ability of attackers to use personal information from public sources or to employ social-engineering techniques to make intelligent guesses at credentials. The example passphrase "Robert has been a Spartans fan since 2010!" has many of the hallmarks of a good password: It is easy for the user to remember, is sufficiently lengthy and includes a variety of character types. However, if the individual posts his university affiliation, interest in school sports and graduation date on Facebook (or other social media), a motivated attacker could easily gather and use this kind of personal information to shorten the path to a successful password guess. This type of vulnerability is not unique to the NIST guidelines, but the greater flexibility allowed in password construction could make this weakness a more significant issue.

Benefits and Risk, From the Security Professional's Perspective

Security professionals are well aware that existing guidelines designed to make passwords more difficult to guess often provide a false sense of security. "Pa$$w0Rd12" satisfies conventional construction requirements, but would be among the first passwords guessed with an attacker's standard tool set.[10] The NIST SP 800-63-3 guidelines reflect the fact that users are typically the weakest link in security by addressing some of the factors that motivate users to make poor security decisions. As such, the updated NIST guidelines have the potential to help information security professionals increase the strength of authentication safeguards without increasing the burden on users.

Cryptographically, longer passwords with multiple character types are more secure, but traditional construction guidelines generally make long, complex passwords difficult to remember and may actually discourage users from creating more secure passwords.[11] Some legacy systems even limit password length or restrict character types for simplicity, forcing users into less secure passwords.[12] NIST now recommends that systems be configured to allow phrases of at least 64 characters or more and to accept expanded sets of character types including spaces, punctuation and even nonstandard characters such as emojis (where feasible) to encourage stronger passwords without enforcing unwieldy complexity rules.

NIST's guidelines also encourage multifactor authentication in all but the least sensitive applications. As with other aspects of the new NIST guidelines, multifactor authentication can significantly increase security while minimizing the impact on users. Whether through biometrics, smartphone-enabled applications, key fobs or cryptographic keys, multifactor authentication provides a strong second line of defense in authentication security without unduly burdening users.[13]

While the new guidelines offer significant advantages, security professionals should carefully consider the tradeoffs that come with implementing these guidelines and not expect an easy solution for secure authentication. For instance, much of the improved security in the NIST SP 800-63-3 guidelines comes from making it easier for users to adopt longer passwords, but they are not actually required to change their normal password behavior. An individual could create a simple password as short as eight alpha (or numeric) characters. If the password is not restricted by the prohibited password list, the user could conceivably select a password that is simpler to crack than would otherwise be possible under traditional complexity rules.

The prohibited password dictionary is central to the improved security provided by the NIST guidelines and deserves special attention from security professionals. An important consideration is that NIST does not prescribe a particular bad password list, so implementers must adopt or develop and maintain their own. There are open-source repositories of compromised and commonly used passwords such as "SecLists" on Github,[14] in addition to a number of commercial services that provide professionally maintained dictionaries of bad passphrases. An example password validation tool based on SecLists, "NIST Bad Passwords," is available on Github[15] and can be evaluated as a proof of concept for individuals interested in dictionary implementations. However, such lists are of limited use as they are not designed to address problematic context-specific passwords.

Appropriately restricting context-specific passwords is a particularly vexing challenge. For example, the inclusion of a user's own username, the website name, associated organization name or other related terminology is less secure when authenticating a user on the related system. In the context of protecting a university system, the inclusion of the university's name, its mascot or derivations thereof in a passphrase could make an attacker's job of guessing easier. Thoughtful construction of the prohibited password dictionary may reduce some of this risk. For instance, if the mascot of a university happens to be a Spartan, it would be wise to add this word and related derivations to the prohibited dictionary. Eventually, graduates of the university will join other organizations that would have no apparent reason to restrict the same words even though the affiliation remains an important part of the user's personal identity. Therefore, a generic dictionary approach cannot reasonably block all of the easily discernable affiliations and preferences associated with an individual user, nor would this necessarily be a good idea. The same word may be an easily guessed affiliation for one person and an obscure and relatively secure choice for another.

This is a nontrivial issue as no standard dictionary will be able to handle these types of "local vulnerabilities." Each organization needs to develop a policy and process to incorporate reasonable user- and organization-specific password restrictions and revisit them regularly. As systems and organizations evolve over time, the types of keywords and other relevant information that should be restricted can change along with them and a process needs to be in place to track and implement protections against new threats. Moreover, if a breach occurs, compromised passwords need to be promptly added to the prohibited list.[16] Incorporating these additional restrictions is probably the most technically challenging and process-intensive aspect of implementing the NIST password guidelines.

Regardless, the NIST SP 800-63-3 guidelines make it clear that users should be prevented from using unsafe password heuristics beyond those blocked by the prohibited password dictionary. For example, users should not be permitted to use repetitive or sequential characters.[17] These additional password construction hazards could potentially be included in a dictionary, but may be simpler to implement programmatically.

The NIST guidelines eschew scheduled mandatory password resets, instead requiring them only when there is suspicion of a breach. Periodic password resets have been used in part to limit the length of time a system would potentially be exposed to a compromised account,[18] a practice that adds security only under the assumption that there has, in fact, been a breach. Unnecessary password resets not only frustrate users, but also add work for administrators and support personnel. If passwords changes are not required, it is important that system administrators have the tools and resources to effectively monitor user activity to identify compromised accounts or potential breaches so the threat of unauthorized access can be handled quickly. This aspect of the NIST guidelines deserves careful thought. Security professionals need to know the risk profile of their systems, users and the information they protect to make intelligent decisions about breach monitoring and policies around password resets.

Conclusion

The updated NIST SP 800-63-3 password guidelines represent an opportunity for organizations of all types to modernize their user authentication policies and practices. While many US government-related entities are required to implement NIST's recommendations, any organization is free to adopt (in whole or in part) the updated guidance that appears within the standard.[19]

Passwords have long been a thorn in the side of both users and security professionals. The NIST guidelines take a step forward in addressing many of the pain points of passwords while encouraging improved security practices by taking into consideration the weakest link in system security—users themselves. However, organizations that have adopted or may be considering adoption of the NIST SP 800-63-3 guidelines should ensure they have a thorough understanding of the rationale and mechanisms behind the changes in authentication security procedures. They should also be cognizant not only of the potential advantages of the NIST guidelines compared to traditional password policies, but also of residual risk to user security that are not directly addressed by the new guidelines. Organizations should also consider the potential investment in change management required as users adapt to new rules and the challenge of developing and maintaining the prohibited password dictionary, which is central to improved security under the NIST guidelines.

Endnotes

[1] National Institute of Standards and Technology (NIST), "Digital Identity Guidelines," NIST Special Publication (SP) 800-63-3," USA, June 2017, https://csrc.nist.gov/publications/detail/sp/800-63/3/final

[2] McMillan, R.; "The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1-d!" *The Wall Street Journal*, 7 August 2017, https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118

[3] Risk Control Strategies, "The New NIST Guidelines: We Had It All Wrong Before," 8 January 2018, https://www.riskcontrolstrategies.com/2018/01/08/new-nist-guidelines-wrong/

[4] *Op cit* NIST

[5] *Op cit* McMillan

[6] Culp, S.; "The Ten Immutable Laws of Security," Microsoft Corporation, 2003

[7] United States Computer Emergency Response Teams, "Security Tip," (ST04-002), 21 May 2009, https://www.us-cert.gov/ncas/tips/ST04-002

[8] Cranor, L.; "Time to Rethink Mandatory Password Changes," Federal Trade Commission, USA, 2 March 2016, https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes

[9] Meyer, T.; "Training Your Users to Use Passphrases," *Medium.com*, 18 May 2018, https://medium.com/@toritxtornado/training-your-users-to-use-passphrases-2a42fd69e141

[10] Mitchell, W.; "Password Cracking," *Web.cs.du.edu*, 2018, http://web.cs.du.edu/~mitchell/forensics/information/pass_crack.html

[11] *Op cit* McMillan

[12] The GNU C Library, "DES Encryption and Password Handling," 2018, https://ftp.gnu.org/old-gnu/Manuals/glibc-2.2.3/html_chapter/libc_32.html#SEC661

[13] De Cristofaro, E.; H. Du; J. Freudiger; G. Norcie; "A Comparative Usability Study of Two-Factor Authentication," 2013, https://arxiv.org/abs/1309.5344

[14] danielmiessler, "SecLists," GitHub, https://github.com/danielmiessler/SecLists/tree/master/Passwords

[15] Li, C.; "NIST Bad Passwords," 2018, https://cry.github.io/nbp/

[16] *Op cit* NIST

[17] *Ibid*.

[18] Henry-Stocker, S.; "Periodic Password Changes—Good or Bad?," *Network World*, 8 August, 2016, https://www.networkworld.com/article/3104015/security/periodic-password-changes-good-or-bad.html

[19] ISACA, *Implementing the NIST Cybersecurity Framework*, July 2014

Bachman Fulmer, Ph.D., CISA
Is an assistant professor of accounting at the University of Tampa (Florida, USA). He has worked in technology risk and assurance services for EY and as an internal auditor focused on technology, compliance and business process improvement.

Melissa Walters, Ph.D.
Is an associate professor of accounting at the University of Tampa. She has worked in systems implementation, control and support areas and teaches information systems and information systems control/auditing.

Bill Arnold, CISSP
Is the director of information security at the University of Tampa and is an information security

analyst working in the areas of information security planning, implementation, assessment and management.