Messaging, Malware and Mobile Anti-Abuse Working Group

M^{3}AAWG Password Recommendations for Account Providers

February 2017

Shortened URL to reference this document: www.m3aawg.org/password-recommendations-providers

Please Note: M^{3}AAWG is presenting the educational information in this paper as a service to the industry. However, M^{3}AAWG does not endorse nor recommend any specific free or open source product mentioned herein. While this paper includes links to materials created by various third-parties, their products are not affiliated with the Messaging, Malware and Mobile Anti-Abuse Working Group and M^{3}AAWG has no control over this third-party content. All links and information provided here are solely for the user's convenience on an "as is" basis and without any responsibility for their material content.

Table of Contents

I. Executive Summary

This document summarizes M^{3}AAWG recommendations for ISPs and other providers who continue to rely on passwords. It briefly describes the risk model arising from the use of passwords to provide authorized or secure access to resources. It is intended to improve end-user security by encouraging strong passwords.

II. Reasons for Password Recommendations

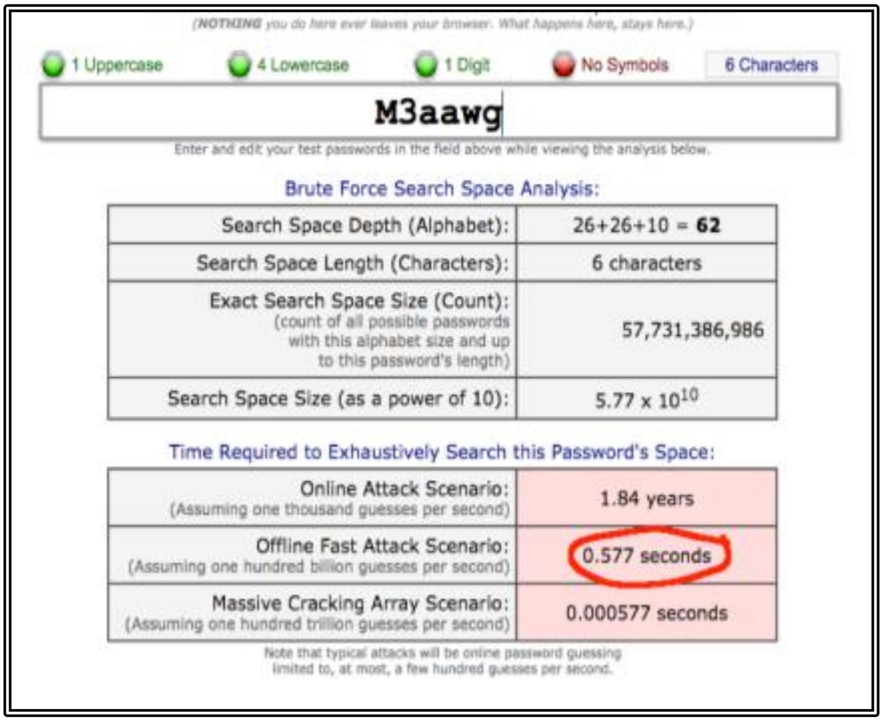
M^{3}AAWG prepares and provides recommendations in the area of password security because:

- Passwords are used virtually everywhere. They are often the primary mechanism for controlling access to sensitive resources. As a result, the basic password continues to play a pivotal role in establishing and maintaining provider security.

- Users often select short and easily guessed dictionary words for their passwords. Such words provide little security against even a weak adversary. Figure 1 below shows data from Gibson Research

Corp.'s Search Space calculator[1] indicating that any six-character password can be cracked in a fraction of a second using easily available computing resources:

Figure 1 – Cracking passwords in a fraction of a second



(NOTHING you do here ever leaves your browser. What happens here, stays here.)

● 1 Uppercase ● 4 Lowercase ● 1 Digit ● No Symbols 6 Characters

M3aawg

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10 = **62**
Search Space Length (Characters):	6 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	57,731,386,986
Search Space Size (as a power of 10):	5.77 x 10^{10}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	1.84 years
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	0.577 seconds
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	0.000577 seconds

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

- Providers' password strength requirements vary widely, even among similar entities. Some providers allow passwords so short and simple that they are easy to crack, while others may insist on passwords that are unnecessarily long and complex. If the community continues to rely on passwords, the industry can benefit from guidance on consensus values for basic password attributes.

- While passwords may seem to be "free" since they require no special hardware or software, in reality, they can be very expensive for providers. The most frequently mentioned password-related costs are those associated with maintaining password-based authentication systems, including processing resets when customers forget their passwords.

- Ironically, aggressive attempts at improving password security can frustrate both users and the support staff. Excessively stringent password requirements result in more annoyance, more passwords that need to be reset, and increased costs for the providers.

- If password policies are too lax, weak passwords may result in breached accounts. Mitigating and recovering from password-related breaches for accounts that involve PII (personally identifiable information) can potentially cost as much as $200 per record breached[2].

III. Risk Model

To ensure that passwords are used as securely as possible, it is essential to understand how passwords are being attacked and overcome at the provider level. Examples of major threats include:

- Insecure password reset options
  Unsafe reset options, such as easily answered "trivia" questions or mailing a new password in plain text to a potentially compromised alternative email account, allow hijacking by a third party.

- Social engineering
  In these attacks, system administrators or help desk staff are tricked into improperly disclosing or resetting a user's password.

- Sniffing passwords or password-derived credentials, such as authentication cookies
  This is possible when these credentials are transmitted in plain text over unencrypted network links.

- Brute force or dictionary attacks
  These attacks might end in unauthorized access to an account or cause legitimate users to be denied access if an account is locked after too many password errors.

- Password hash attacks
  Password hashes have been stolen and cracked at high speed via use of cloud computing services, high performance GPU arrays, and the rainbow table method.

- Password-stealing malware
  Malware on an infected computer can steal passwords as the user enters them.

- Untrustworthy system administrators and network engineers
  Employees can exploit their privileged access.

- Existing system vulnerabilities
  These vulnerabilities can be used to compromise a system and install server-side malware. An intruder might also make unauthorized modifications to other facilities involved in authentication, authorization or access control.

- Default passwords that go unchanged
  With some products, all units are shipped with the same hard-coded passwords that the manufacturer assumes will never be noticed nor maliciously exploited.

- A shared root password
  Often shared by multiple members of an administrative or operational team for system administrative purposes, the shared password goes unchanged even when a team member leaves or is discharged.

- Password reuse
  This is often for administrative convenience.

Providers should also be aware of additional client-side password-related threat vectors that exist but are not included here.

IV. M^{3}AAWG Basic Password Recommendations for Providers

1. Allow users to add factors to augment their password, such as:

   - An entity the user has; e.g., a user's pre-registered cell phone number or a hardware cryptographic fob

   or

   - An entity that is unique to the user; e.g., biometric factors such as the user's fingerprint, voiceprint or a picture of the user's eye

   Multifactor protection is increasingly common, especially for uncommon or particularly high impact transactions. For example, if a user who normally logs in from New York suddenly logs in from Europe, that anomaly might trigger a request for a second factor proof of identity. See M^{3}AAWG Multifactor Authentication Recommendations for more details at www.m3aawg.org/multifactor-authentication-bp.

2. Encourage use of "password safe" software. Password safes provide a cryptographically secure database to store user credentials, thereby reducing or eliminating the need for users with many accounts to memorize their passwords. By largely eliminating reliance on users' memories, password resets can be reduced or eliminated and users are given the ability to easily use strong and unique passwords for each of their accounts. However, if a password safe's master password is forgotten or compromised, the impact can be substantial.

3. Whenever passwords are used, require strong passwords or strong passphrases. Specific recommendations for what constitutes a strong password or strong passphrase appear in Section V.

4. Encrypt all connections over which passwords are entered to deter password sniffing. For example, use 'https" rather than "http;" use secure shell instead of telnet; use "sftp" instead of "ftp;" or use cryptographic challenge protocols that do not transmit plain text passwords at all.

5. Recognize that password stealing malware is a material threat to password authentication. Follow the industry best practices in this area described in the "Anti-Bot Code of Conduct for Internet Service Providers."[3]

6. Ensure that initially assigned end-user passwords are unique and strong. If an account is not activated within a prescribed period, disable the idle account.

7. Provide a mechanism that makes it easy for users to securely change their password should they want or need to do so. If a user does not know their current password, they need to be able to use a secure password reset mechanism. In-person password resets done after presentation of reliable photo ID are likely the most secure mechanism, but this approach might only be practical in an organization with a single location.

   When face-to-face password resets are impractical, consider creating a secure alternative or backup password. Customers can use two or more previously-registered alternative access mechanisms to reset their own passwords; e.g., an alternative email account plus confirmation via a cell phone number.

   We recognize that many users routinely access their email via their mobile phones. If a mobile device is lost or stolen, and the device does not require a PIN or other access code such as a screen pattern or fingerprint, any person who has that mobile device may be able to access both the user's email and provide telephonic confirmation of their password reset request.

This vulnerability can be reduced if users ensure that: (a) mobile devices are configured to require entry of a PIN or other security code for access; (b) email on mobile devices is not configured to automatically use a pre-saved password; or (c) the mobile device user is asked to register a landline instead of a mobile phone number.

8. Passwords should not be stored in plain text nor in a reversibly encrypted format. Credentials should only be stored in a salted and one-way hashed form, using a strong and thoroughly cryptanalyzed password-hashing algorithm such as SHA-2[4]. Use shadow password files to limit non-privileged user access to hash values.

9. Authorized security staff should routinely attempt to crack their organization's own password files. If weak passwords are found, require the user to change it. Sanctioned staff, given access to a provider's password hashes, can use password auditing tools found on www.openwall.com[5] and www.sectools.org[6], among other websites, to identify weak user passwords.

10. Leverage federated authentication. Decoupling identity providers from service providers can potentially reduce or eliminate the need to create and manage local authentication entirely.

11. Minimize opportunities for MITM (Man-in-the-Middle) attacks against passwords. For example, use globally trusted SSL/TLS server certificates, secure wireless access points with 802.1X, and protect DNS resolution against cache poisoning attacks with DNSSEC. More details on MITM attacks and how to protect against them can be found in M^{3}AAWG Initial Recommendations for Addressing a Potential Man-in-the-Middle Threat available at https://www.m3aawg.org/sites/default/files/M3AAWG-Man-in-the-Middle-Recommendations2015-07.pdf.

12. Monitor login attempts and take appropriate steps when anomalies are detected. If a user logs in locally and soon afterward from a remote destination, it may be a sign that a legitimate user and an unauthorized user both have access to an account. Providers should consider employing fail2ban[7], or a similar solution, to automatically deter brute force login attempts.

13. Ensure default passwords are changed at install time.

14. Providers can use "sudo" instead of "su" for Unix/Linux administrative/privileged access, thereby avoiding the need for users to know the super-user password.

15. Providers can implement limiting login rates (tries per unit of time) and extend the time between failed login attempts. For example, enforce a 10-minute delay between the third and fourth login attempts then raise the delay to 30 minutes after five failed attempts. This avoids the hard lockout issues described below in Section VI and makes automated password brute force attacks ineffective.

16. Automatically monitor system daemons and other critical files to detect attempts at switching critical programs or files with malware infected replacements. This can be done with programs like Tripwire[8,9] that monitor the checksums of critical files.

V. Password Strength

While a multifactor solution is generally better, multifactor deployment sometimes cannot be justified or customers can be reluctant to use multifactor authentication. In such instances, we recommend ensuring that the passwords used are as strong as possible. Consider these three examples of policies that a provider might adopt:

<u>Option I: Strong Conventional Password</u>

Figure 2 below shows that a strong conventional password resists brute force and dictionary attacks through the use of a minimum password length, a required character set, and other password complexity requirements. M^{3}AAWG consensus recommendation is that a strong conventional password will have:

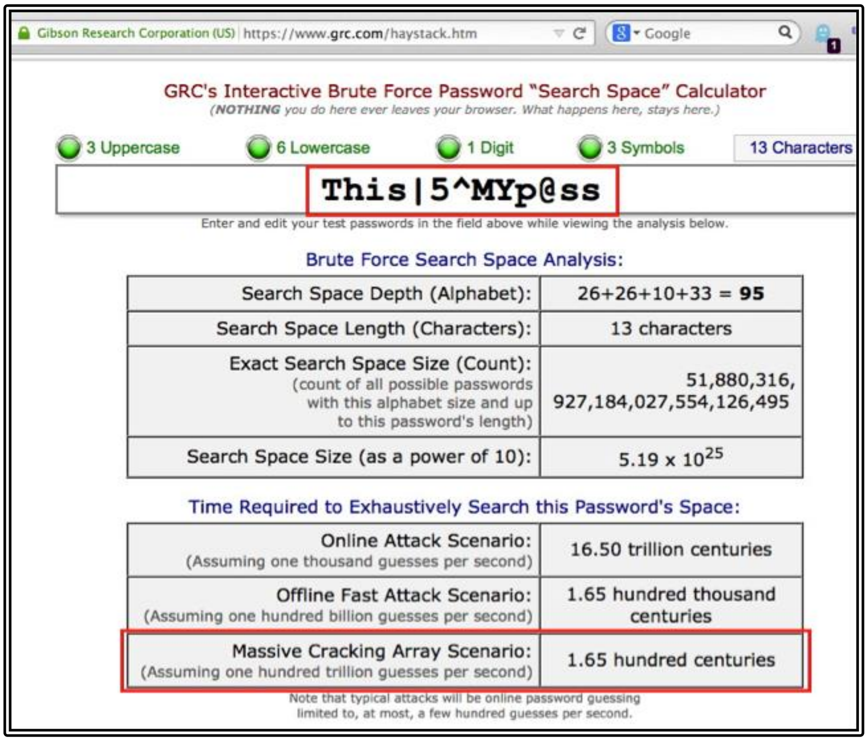
1. A minimum length of 12 (twelve) printable characters

2. A required rich character set that includes upper case alphabetic letters, lower case alphabetic letters, numbers and special symbols

3. No repetition of the same letter, number or other password element three or more times in a row

4. No use of dictionary words, people's names, or sequential keyboard strings; e.g. QWERTY, as part of a password

Figure 2 – Strong passwords are much harder to crack



Gibson Research Corporation (US) https://www.grc.com/haystack.htm
Google

GRC's Interactive Brute Force Password "Search Space" Calculator

(*NOTHING you do here ever leaves your browser. What happens here, stays here.*)

● 3 Uppercase ● 6 Lowercase ● 1 Digit ● 3 Symbols 13 Characters

This|5^MYp@ss

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10+33 = **95**
Search Space Length (Characters):	13 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	51,880,316, 927,184,027,554,126,495
Search Space Size (as a power of 10):	5.19×10^{25}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	16.50 trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	1.65 hundred thousand centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.65 hundred centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

Option II: Strong Passphrase

Passphrases, while being longer than passwords, relax the required character set complexity and allow use of dictionary words. The ability to essentially use a short phrase or simple sentence makes it easier for users to remember their passphrase compared to memorizing totally random conventional passwords. M^{3}AAWG consensus recommendation is that a passphrase should:

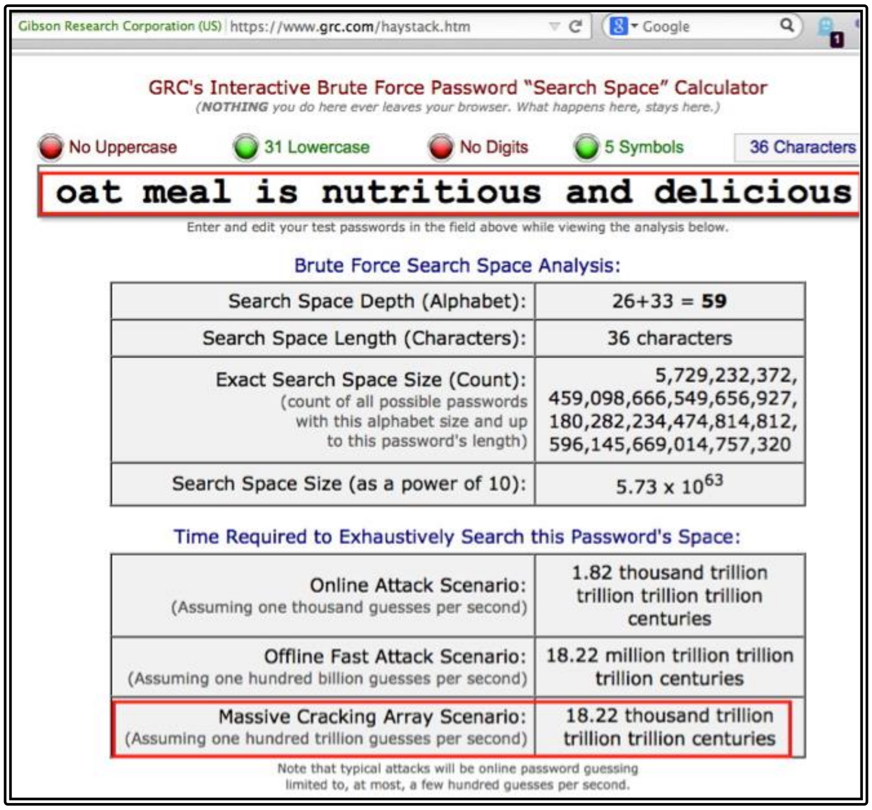
- Have a minimum length of 24 (twenty-four) printable characters

and

- Avoid the use of common natural language phrases; e.g., "world champion football team," "Jack and Jill ran up the hill," etc.

See work by Joseph Bonneau and Ekaterina Shutova for additional information on the "Linguistic Properties of Multi-word Passphrases."[10]

Figure 3 – Passphrases are also hard to crack



Gibson Research Corporation (US) https://www.grc.com/haystack.htm
Google
GRC's Interactive Brute Force Password "Search Space" Calculator
(NOTHING you do here ever leaves your browser. What happens here, stays here.)

No Uppercase
31 Lowercase
No Digits
5 Symbols
36 Characters

oat meal is nutritious and delicious

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+33 = **59**
Search Space Length (Characters):	36 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	5,729,232,372, 459,098,666,549,656,927, 180,282,234,474,814,812, 596,145,669,014,757,320
Search Space Size (as a power of 10):	5.73×10^{63}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	1.82 thousand trillion trillion trillion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	18.22 million trillion trillion trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	18.22 thousand trillion trillion trillion centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

Option III: Stronger Still – Very Long Randomly Generated Passwords

With this option, users do not need to remember or enter passwords. If users all have password safes, it is possible to have very long and complex machine-generated passwords; e.g., 100 random characters.

Because the user never needs to recall or enter them, these exceptionally-long, generated passwords can have very high entropy that make them extremely robust against brute force attacks. However, sniffing attacks against unencrypted traffic or password stealing malware attacks remain possible.

Unfortunately, while some password safes can generate high quality and very long random passwords, many systems either disallow exceptionally long passwords or tolerate them but disregard all characters past some relatively brief limit. Providers wishing to use this option need to ensure their systems and applications allow long passwords and that they use the entire password, not just part of it.

VI. A Few Password Practices to Avoid

- **Hard Lockouts**

To preclude potential DoS (Denial of Service) exposure, unless there is a compelling business justification, providers should not use hard lockouts. A hard lockout happens when an attacker repeatedly tries to login to a user's account and fails. After some number of failed attempts, logins are administratively forbidden until that account is manually re-enabled by an administrator.

Soft lockouts, by way of contrast, automatically end after login attempts cease for a designated period of time. M^{3}AAWG also urges providers to distinguish between lockout mechanisms that:

- Block access to a particular username from ***any*** internet-wide IP

and

- Solutions that block access to an account from individual IP addresses that have been repeatedly trying and failing to login

The former is prone to DoS attacks against legitimate users while the latter is not. However, if the concern is that an attacker has many hosts from which to conduct a distributed attack, failing to recognize aggregated attack capacity would be risky.

- **POP/IMAP Consolidation with User-supplied Saved Passwords**

Some email providers allow their users the ability to automatically consolidate email from one or more alternative email accounts that they also use via POP or IMAP. Unfortunately, to be able to do this, the provider doing the POP/IMAP consolidation usually must have access to the login credentials for the user's other email accounts. Those usernames and passwords must either be stored totally unencrypted or stored in a reversibly-encrypted database. That makes for a tempting attack target and is inconsistent with our earlier recommendation that passwords only be stored in salted and hashed formats using strong cryptographic algorithms. Some providers mitigate the risk by providing application passwords and allow each password to be used only from a single service or device.

Additional background on password use throughout the industry can be found on various websites. (See References[11,12,13,14,15.])

VII. Conclusion

While passwords are not ideal security credentials, they will be with us for a long time. Good practices such as requiring strong passwords or passphrases, password safes, and encrypted server-side password storage can greatly improve password security without undue cost.

VIII. References

[1] Gibson Research Corporation – GRC's Interactive Brute Force Password "Search Space" Calculator, https://www.grc.com/haystack.html.

[2] Ponemon Institute, "Ponemon Study Shows the Cost of a Data Breach Continues to Increase," https://www.ponemon.org/news-2/23

[3] U.S. FCC CSRIC III, U.S. Anti-Bot Code of Conduct for Internet Service Providers (ABCs for ISPs), https://www.m3aawg.org/system/files/20120322_WG7_Final_Report_for_CSRIC_III_5_0.pdf.

[4] Unix crypt using SHA-256 and SHA 512, https://www.akkadia.org/drepper/SHA-crypt.txt.

[5] John the Ripper password cracker, http://www.openwall.com/john/.

[6] Top 125 Network Security Tools, http://sectools.org/tag/crackers/.

[7] Fail2ban.org, http://www.fail2ban.org/wiki/index.php/Main_Page.

[8] Tripwire.org, www.tripwire.org

[9] Sourceforge.net, https://sourceforge.net/projects/tripwire/

[10] University of Cambridge Computer Laboratory – Linguistic Properties of Multi-word Passphrases, http://www.cl.cam.ac.uk/~jcb82/doc/BS12-USEC-passphrase_linguistics.pdf.

[11] ENISA - European Union Agency for Network and Information Security, "Basic security practices regarding passwords and online identities," https://www.enisa.europa.eu/media/news-items/basic-security-practices-regarding-passwords-and-online-identities.

[12] Schneier on Security, "Choosing Secure Passwords," https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html.

[13] CPNI – Centre for the Protection of National Infrastructure, "Password Guidance: Simplifying Your Approach," https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf.

[14] The Inquirer, "GCHQ wants UK industry to simplify its passwords. OK, then," http://www.theinquirer.net/inquirer/news/2425771/gchq-wants-uk-industry-to-simplify-its-passwords-ok-then.

[15] SANS Institute, Consensus Policy Resource Community, "Password Protection Policy," https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy.

As with all best practices that we publish, please check the M^{3}AAWG website (www.m3aawg.org) for updates to this document.