Messaging, Malware and Mobile Anti-Abuse Working Group
M³AAWG Multifactor Authentication Recommendations

February 2017

Reference URL for this document: www.m3aawg.org/multifactor-authentication-bp

I. Introduction

Passwords, from simple user-selected words to complex phrases containing randomized strings, have many shortcomings. For example, brute-force password cracking attacks have grown faster and more efficient, leading to unauthorized account entry that have resulted in catastrophic losses for both individuals and corporations. And even the most crack-resistant passwords might be compromised.

Yet passwords continue to be the default solution to secure user accounts. M³AAWG believes the time has come for providers to require multifactor authentication, instead of simple passwords, to enhance protection of services with a history or substantial risk of account compromise.

II. What Is Multifactor Authentication?

Multifactor authentication strengthens account security by combining two or more of:

- something the user *knows* (a password or PIN),
- something the user *has* (such as a hard token or a registered smart phone), and
- something the user *is* (a Turing test, fingerprint or other biometric measure).

Using a single factor listed above multiple times does not meet the necessary conditions. For example, just requiring two points "the user knows," like a birthplace and a pet's name, does not qualify as multifactor authentication.

III. Why Multifactor?

Cyber criminals are highly motivated to obtain unauthorized access to user accounts. Anyone who has looked at a service provider's security logs knows that internet-exposed systems are constantly under siege from those intent on gaining unauthorized access. Passwords are often the only mechanism standing between providers' accounts and catastrophe, but passwords alone provide fragile protection.

Multifactor authentication has the potential to substantially improve the strength of account protection. Use of true multifactor authentication can dramatically reduce the risk of successful account-oriented attacks. While a growing number of leading companies offer multifactor authentication as an option, unfortunately many other companies do not offer any multifactor authentication options at all. And, virtually no companies require multifactor authentication for all users.

The time has come for this to change.

IV. M³AAWG Recommendations

- M³AAWG recommends that all providers offer multifactor authentication as an *option* for *all* users of services with a significant history and/or substantial risk of account compromise.

- M³AAWG recommends that multifactor authentication be *required* for *high value, high profile* and *commonly targeted users* such as accounts payable staff, senior company executives or high-profile online personalities.

- M³AAWG recommends that multifactor authentication be *required* for *privileged* users such as system administrators, network engineers, database administrators, security team members, staff with access to financial accounts and other critical users.

These recommendations do not mandate specific technologies; a technology well suited for one environment might be a poor fit in a different environment. Therefore, M³AAWG does not recommend adoption of any particular multifactor solution or provider.

V. Multifactor Deployment Considerations

When considering multifactor options, providers should keep in mind the following deployment considerations:

- Successful deployment of multifactor authentication typically requires both executive sponsorship and enthusiastic support from the company's technical team. If both an organization's leadership and its technical team do not support the idea of multifactor authentication, it will not get deployed.

- Be sure to consider funding requirements, whether for commercial or open-source solutions. Deploying multifactor authentication, even "free" open-source solutions, will not be costless. However, it is worth weighing the deployment expense against the amount the company is losing due to remediating ongoing account breaches and other similar incidents.

- In evaluating potential multifactor solutions, ease-of-use should be the foremost consideration. If a multifactor solution seems "hard to use," it likely *will not* get used.

- In addition to thinking about routine ease-of-use, also think about exception conditions. That is, how will the technical team handle users who have lost or damaged their multifactor authenticators? Can users get emergency-use backup codes to carry with them? Can users register both a hard token and a backup soft token running on their smart phone?

- Be ready for at least some users to underestimate the importance of securing their accounts. It may be necessary to educate these users to help them understand the importance of protecting even a routine account. The reality is that breaching even a general account may dramatically increase an attacker's ability to eventually gain privileged access.

- Think about all platforms the technical team supports. Some users may be on laptops but others may be on tablets or smartphones. Be sure the multifactor solution will work on all common platforms.

VI. Conclusion

M[3]AAWG urges providers not to wait for the rest of the industry to deploy multifactor authentication before doing so themselves. A critical mass of institutions needs to take a leadership role and set the example for their industry peers—otherwise, deadlocks may result.

Furthermore, do not let a "quest for the perfect" solution derail meaningful forward progress. Instead, think "risk minimization." There are many solutions available that may not be perfect but are still far better than ordinary passwords by themselves.

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

M3AAWG106