Student Papers in Public Policy

Volume 2 | Issue 1 Article 3

2020

Implement Multi-Factor Authentication on All Federal Systems Now

Megan Walsh
Purdue University, walsh93@purdue.edu

Implement Multi-Factor Authentication on All Federal Systems Now

Megan Walsh

Undergraduate Student, Department of Computer Science

Purdue University

INTRODUCTION

The White House Office of Management and Budget recorded 31,107 information security incidents in fiscal year 2018. The most common attacks to gain access to a user's login credentials were e-mail/phishing, web-based attack, and brute force entering of username/password combinations. Given this high number of incidents, strong reliance on computers for everyday business, and common attacks that target passwords, information security should be a priority for information technology administrators working in federal agencies. Yet, not all federal departments are using multi-factor authentication for privileged users with high levels of administrative access and control.

Multi-factor authentication requires users to have access to two or more different forms of verification to access an account. For example, entering a correct username/password combination as well as a fingerprint to log in constitutes multi-factor authentication. Using a single factor to access information, such as only a password, opens up systems to greater risk of exploitation. Many employers, schools, and private companies enforce multi-factor authentication as a requirement to access account information and to use the service. It is time for all government data to be protected by multi-factor authentication.

Security

Virtually all account compromise attacks are prevented when users have multi-factor authentication enabled on their accounts. Passwords alone are not secure because weak passwords are easily hacked by using a list of common passwords, and complex passwords can be deciphered due to human predictability. For example, if a password requires an uppercase letter most users will only

capitalize the first letter of their password. Non-secret information about a person, such as a pet's name, storage of a password in another application, or the password written near a login station, increases vulnerability of an account. Malicious actors can use phishing scams to learn account information, with users having no idea they have been compromised until long after their data are stolen. If users have a second factor on their account that is required to complete a login request, they will either be notified when a login attempt is initiated, or the malicious actor will not be able to proceed due to lack of the second factor. Unless a password is compromised along with the user's phone, token generator device, or self (if biometrics are used to authenticate), there is little chance the account can be compromised. Not all second factors are perfect, but common second factor implementation options are robust and secure. Even simple, common implementations of multi-factor authentication dramatically make a difference in an organization's information security.

Implementation Options

The three types of factors are knowledge factors (something the user knows), ownership factors (something the user has), and biometric factors (something the user is). Most single-factor authentication systems only require a password, a type of knowledge factor. Increased security is obtained when two types of factors are used together to access a resource, such as using a knowledge factor and a biometric factor.

Knowledge factors

Nearly every online account employs the knowledge factor of a unique username and password. For many websites and accounts, usernames are fairly public as they are typically the user's email or the name they are known by on the service. A user's password is more difficult to obtain, but not impossible. If a service has a data breach, all accounts where that password is used are vulnerable to unauthorized logins. Another common type of knowledge factor is a security question, which can easily be obtained by looking for information on public social media accounts, making this a weak factor, especially when used with another knowledge factor.

Ownership factors

One-time passcodes are the most versatile ownership factor option. One-time passcodes can be obtained through a text message, a physical code generator, a phone app that sends a push notification, or a USB or card that can be inserted into a computer. Implementation plans can include any combination of these generators to best tailor towards subsets or individual users. Depending on the infrastructure of an organization, adding an ownership factor can be a costly solution. Employees must have smartphones available to use for work purposes or separate devices must be purchased and registered for each employee. If employees already have company cell phones, ownership factor implementation can be fairly cost effective.

Biometric factors

The only widely used biometric factors are fingerprint and face recognition. These are built in authentication factors for many off-the-shelf model laptops and phones. Although these

factors also require infrastructure, they can be incorporated during routine hardware upgrades for work-issued phones and laptops. If upgrading equipment is not possible but biometric is the preferred form of multi-factor authentication, fingerprint scanners can be attached via input jacks in laptops.

Conclusion

Multi-factor authentication is an effective way to prevent information security attacks. Therefore, it is imperative that all federal agencies deploy multi-factor authentication for all users and systems. There are a variety of methods to implement multi-factor authentication through ownership or biometric factors. A department's multi-factor authentication solution can be targeted towards its employee population to increase usability and adoption.

Recommendations

Individual departments should decide how to implement multi-factor authentication for their employees to increase adoption and minimize issues that will arise upon roll out. Major information security incidents are very costly, so funding for the implementation of multi-factor authentication should be prioritized in budgeting for new equipment. For departments where every employee has a government-issued work phone, a one-time password generator or phone-supported biometric factor would be cost effective and simple for employees to adapt to.

There are multiple ways to roll out a multi-factor authentication solution in an organization. A phased role-based approach that implements multi-factor authentication for privileged accounts before non-privileged accounts ensures that those with the highest access have a higher level of protection covering their information. It also minimizes the risk of issues arising when a whole organization makes a change at once. Not every attack is targeted towards privileged users however, so it is essential that non-privileged users adopt the multi-factor authentication solution as soon as the process is perfected by those in the privileged user phase. Once the entire organization is covered by multi-factor authentication, administrators will see fewer information security incidents, further protecting government data from malicious actors.