Multi-Factor Authentication Guide

Background

Digital security is critical for organizations because software systems store sensitive information. A common point of failure in digital security is the password. Passwords are frequently forgotten, shared, and stolen for malevolent reasons. Many organizations deploy multi-factor authentication (MFA) for identity and access management as an additional layer of security. That additional layer of security creates a unique challenge when building automations.

Overview

The organization which owns the application is responsible for security and the MFA approach. There is no one-size fits all approach to automating because each application the automation touches may have a different MFA methodology. This is the challenge and constraint for automation developers.

MFA requires additional verification information (beyond a password) which comes in various forms, such as:

- One-time passwords (OTP)
    - Codes that come via email, text, or app
- Time-based one-time passwords (TOTP)
    - Codes that constantly update (e.g. every 30 seconds) and must be retrieved from an app
- Security questions
    - A system prompts the user to answer security questions that were required during account creation (e.g. Name of your first pet)
- Biometrics
    - Software systems may require you to use fingerprints, voice recognition, etc.
- Other
    - Other types may include your physical location or a physical token, such as a smart card or USB

Avoiding MFA

The best way to manage MFA in automation is to avoid it where possible. Below are tactics that should be explored when developing an automation.

- **Service accounts**
    - A service account is a special type of account for applications, not people. They often have extensive access to an organization's underlying applications or

databases. Service accounts should be used wherever possible. Often MFA is a security feature that can be disabled when setting up a service account. Typically, external applications cannot be managed with service accounts which means many automations will still require an approach to getting around MFA.

- **Single Sign On (SSO)**
    - SSO is a method that allows users to log in once and access multiple applications without having to enter their credentials for each one separately. SSO uses a central identity provider (IDP) to authenticate users and provide them with access to the applications they are authorized to use. Once the user is authenticated, they can access multiple applications without having to re-enter their credentials. For example, logging into google gives you access to related google applications like youtube, gmail, and other google applications. Using SSO with automation typically requires additional IT involvement, but it comes with the benefit of reducing the amount (or need) of authentication.
- **Open-Authentication (OAuth)**
    - OAuth can only be used if your automation platform is 'On Premise' (not cloud based). OAuth provides an application with secure delegated access to server resources without providing credentials. OAuth allows access tokens to be issued to third-party clients by an authorization server. The third party then uses the access token to access the protected resources hosted by the resource server.
- **MFA alternatives**
    - Similar to disabling MFA altogether, some applications offer an MFA alternative. Commonly, this is an advanced password scheme such as a password that has 72 characters. Selecting this security feature is preferable to MFA because the automation can store the username and password in its credentialing management system. Similarly, some applications will allow you to choose to use backup security questions, such as the name of your first pet. Both of which are preferable to MFA.

Our recommendation

When choosing an MFA approach, minimizing the steps required to access an application while maintaining security is the goal. Tarpon Health recommends desktop applications and/or browser extensions that use TOTP. The automation can obtain the code/pin by opening the application, copying the code, and entering into the requesting application. Integrating MFA in this manner is most effective because it contains the least steps, there are no send/receive delays, and no manual intervention is needed.

Recommended TOTP applications:

- Authy
- Google Authenticator

Viable approaches

Tarpon Health recommends using desktop-based applications and or browser extensions that generate OTP if a TOTP application cannot be used. These MFA solutions typically generate codes/pins from an application and/or send them to an email address/virtual phone accessible to the automation. The automation initiates a request, waits for the receipt, scrapes the information, and inserts the code/pin into the requesting application. This method is not as efficient as our recommended TOTP solution because there are more steps and a send/receive delay that can cause issues. That said, it remains effective because the automation can integrate and monitor the success of these steps easily.

Recommended OTP applications:

- Email (Outlook/Gmail/etc.)
- Dialpad (paid service)

Not recommended

Any MFA solution that requires an external device (e.g. not a desktop application) or manual action to satisfy the authentication requirement should be avoided. Common approaches include a push notification, call, or text to a phone. For example, a service will call a designated number and instruct users to press “1” on a dialpad to authenticate. Since the automation relies upon two devices, it makes it nearly impossible for an automation to authenticate on a schedule or without manual intervention.

Least preferred applications:

- LastPass (Push Notification - IOS/Android)
- Microsoft authenticator (TOTP - IOS/Android)
- DUO (Push Notification - IOS/Android)