The Low-Down on Multi-Factor Authentication

Multi-Factor Authentication, Strong Authentication, 2FA, MFA, Token-Based, Out-of-Band Authentication; what does it all mean? Many more people are familiar with these terms than just a few years ago. But, not all multi-factor authentication (MFA) types are created equal. MFA solutions are designed to protect their users' accounts in the event of credential theft. With more advances in software technology and features, comes more vulnerabilities and potential ways for attackers to gain your password. However, just how effective are the various MFA types? Many MFA solutions have recently flooded the market, and that raises the question: Are all MFA methods created equal?

The short answer is most certainly: No. Let's briefly analyze some of the most common MFA methods and explore which factors of verification are more or less effective than others.

SMS or One-Time-Passwords (OTP): SMS based text messages to your mobile phone, often referred to as one-time-passwords or out-of-band authentication, is a random (usually) six-digit number sent to the authenticators mobile phone using SMS. In theory, the only person with the right mobile phone number will be able to authenticate… right? Wrong. There are several proven ways to hack an SMS OTP, albeit generally unlikely unless you're a high-profile target from a persistent threat. For example, Reddit was breached in mid-June of 2018 via an SMS intercept. (https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/)

This shows that SMS authentication is not as secure as most assume. This can be done by taking advantage of mobile network vulnerabilities or malware that is installed on the victim's phone. Often, a social engineering attack is conducted on the carrier that lets the attacker get a new SIM card associated with the victim's number. The National Institute of Standards and Technology (NIST) deprecated SMS authentication in 2016, indicating that it is no longer an acceptable form of authentication; however, most companies, yes – even banks, continue to offer SMS OTPs. Again, unless you're a high-profile target, SMS is better than no MFA.

Hardware Tokens: Perhaps one of the oldest methods for MFA is the use of hardware authentication tokens. These are often in a key-fob format with a digital LED display showing random numbers that change every 30-60 seconds. The hardware itself protects the internal unique key, but there are a few disadvantages. The most obvious: you have to carry them around. Secondly, they are one of the most expensive types of authentication, require some logistics and must be changed out periodically. Some also require a USB connection, which may be tricky if you need to authenticate from your mobile phone or tablet.

Software or "Soft" Tokens: Perhaps the most popular currently is in the form of a software or "soft" token such as Google Authenticator. They perform just like hardware tokens, but in the form of a mobile application on your phone. You can have multiple "tokens" in one spot so the biggest advantage is that there is no extra hardware, and most people keep their phones within arm's reach.

Push-Based Authentication Tokens: As an evolution to the soft-token and SMS, the use of secure push technology to authenticate has gained popularity due to its improved usability and security. Unlike SMS, the push message doesn't carry the OTP. Instead, it carries an encrypted message that can be opened only by the specific app on the user's phone. The user then decides whether the login attempt is valid or not. If approved, the unique OTP should be generated internally by the token on the user's phone and sent back with the approval to verify it. Not ALL solutions do this, which can increase the risk of a push approval message being spoofed.

QR Code Based Authentication Tokens: Most push-based tokens require a data connection from the phone; however, QR code-based authentication works offline and provides the contextual information through the QR code itself. The

user scans the QR code on the screen with the authentication mobile app, then types the OTP that the mobile app generates based on the unique key, the time, and the contextual information. This process is quick and efficient, which has been gaining more popularity in recent years due to its simplicity.

Certificates: Many applications authenticate using digital certificates, essentially a permanent "digital ID" that resides on the user's computer. Once the user provides their username and password, the authentication process then checks for the presence of this "digital ID" to confirm if the computer the user is using is authorized to use the application. This essentially does not provide MFA for the user themselves, but only limits the use to a specific physical device. So, if this particular device were to become compromised, and the user's credentials were stolen – it is still very possible for an attacker to gain access to the application. While this method had its purposes, it is generally not acceptable for a true MFA implementation for user credentials.

Security Questions: This is not a form of MFA. MFA is often confused with the simple definition that an account must answer multiple questions or have multiple passwords in order to gain access to the application or device. To be defined as true MFA, the authentication process must consist of two (2) of the following: Something you know (i.e., username/password), something you have or given (i.e., token, OTP, QR code), and/or, something you are (i.e., biometrics).

As you can see, there are many different forms of authentication, but not all of them will provide the desired level of security. A push-based token can be more effective than a hardware token, but not all push-based tokens are developed the same way. If you're planning to roll out an MFA solution, make sure you address these items in a risk assessment and establish a clear understanding of what level of security and risk you're getting with the solutions you're considering.