TOKEN

Token White Paper #1:

Draft prepared by: Evan Krueger, Engineering Manager
June 27, 2022

HOW TO CHOOSE THE BEST MFA METHODS TO HELP STOP RANSOMWARE ATTACKS

By David Strom and Evan Krueger

Introduction

Interest in multi-factor authentication (MFA) has risen in the past few years, spurred by the increasing frequency and severity of data breaches and destructive attacks. When Covid-19 happened, ransomware actors proliferated. In May, BlackFog saw the largest number of ransomware attacks over the last three years. Many ransom demands leverage either simple login/password combinations, which had already been posted to the dark web or other accounts that had either no or weak MFA methods. Some analysts have brought up the point that trying to pay off many Russian ransom collector accounts could result in sanctions being applied. Enterprise adoption of MFA has become the best tool to fight present-day ransomware attacks by protecting administrative accounts and in interrupting the movement of attacker across your corporate network. MFA is no longer the sole province of the extremely security-conscious crowd — it has become generally accepted and a progressively necessary practice for any computer user. And increasing interest is being met with greater levels of support and industry adoption. MFA has recently received several major supporters: Last year, Google enabled MFA by default on all of its end user accounts. The US government proposed a more widespread adoption of MFA in a series of Biden Executive Orders last year as well. Then GitHub announced that it will require all users who contribute code to use MFA by the end of 2023. And in June, Microsoft announced it will encourage more of its customers to move towards MFA. Yet despite these victories, MFA still has a bad rap: it is inconvenient, it is costly to implement, it can be hacked anyway, and not every situation supports it. When evaluating the various MFA products and technologies on the market today, it's important to understand the tradeoffs in security, scalability and usability inherent in each option. Additionally, it can be helpful to understand your available choices in the context of how MFA has developed over time. Let's look briefly at MFA's history, its relevance to digital security, and how to choose the right MFA methods to stop these and other potential attacks.

Evolution of MFA

Back in the '90s, hardware "key fob" devices were pioneered by SecurID, which would display rotating one-time passcodes. Users of these devices would be prompted for these codes at the time of authentication, adding an additional layer of security beyond a username and password. These were groundbreaking at the time, because they provided iron-clad security if you didn't lose your fob or leave it in the office when you were working elsewhere. Without physical possession of the key fob device, an attacker with knowledge of the target's username and password would almost certainly be unable to guess the associated one-time passcode. While six-digit codes could eventually be brute-forced, each code was valid for only a short window, mitigating such an attack. Since then, various forms of time-based one-time passcode (TOTP) MFA have become available. In some

of these implementations, TOTP codes are delivered via SMS, while others require users to use an authenticator app. There are security tradeoffs in how these codes are delivered. SMS messages can be intercepted through SIM swapping attacks or by exploiting flaws in telecommunications protocols, like SS7. Authenticator apps and hardware authenticators utilizing TOTPs sidestep the risk of interception inherent in SMS-based systems, but users can be phished or otherwise tricked into sharing their one-time passcode with a threat actor.

While far from perfect, it's important to understand that the fundamental goal of a TOTP system is to provide a level of assurance that the person making an authentication attempt is in possession of some device such that an attacker would need two factors of authentication: something the valid user would know (i.e., a password) and something a valid user would have (i.e., access to the phone that has been authorized to receive TOTPs, a key-fob, etc.). This approach has become a popular and relatively low-effort approach to adding MFA to various services and applications.

As MFA evolves, so too do the efforts of threat actors. SMS-based TOTP codes are still commonly used today, but the promise of security they offer is diminishing with time. Many consider such methods to be useless as an authentication method. In 2013, LifeHacker posted this article that spoke about how mobile malware could exploit these SMS codes, and a few years later Brian Krebs described an entire ecosystem of criminal workers who can be bribed to defeat the process. Today, potential avenues for MFA compromises such as these should be considered when choosing a service or technology for administering MFA, and for most operations, SMS-based TOTP isn't a satisfactory MFA solution. This is especially true for enterprise deployments, as the payoff for compromising the credentials of an employee may be worth the level of effort involved in phishing or intercepting SMS messages in a way that it might not be for an attacker to target an individual person.

An alternative option used by some vendors who have tried to eliminate the effort of typing in the codes by having special hardware or software to send push notifications to your phone that just require acknowledgment. In some ways, this idea is an improvement over insecure TOTP services, as there is no code or passphrase to phish. In addition to a username and password, the push notification serves as a second factor of authentication, as it is delivered only to pre-registered devices associated with the user's account. For an attacker to exploit this system, he or she would need to be in possession of both the knowledge of the user's password and have physical access to one of the user's devices. However, in many cases, it's possible for the user to become accustomed to approving notifications without understanding the connection between the intended action (the authentication attempt) and the request for approval. Furthermore, in some enterprise settings, these systems can be set up such that the user is not the one to whom the notification is delivered, and instead a manager or some individual with a greater level of privileged access is tasked with approving requests for access, which only further disconnects the action from the request for approval. In these cases, the expected protection of push-based MFA is undermined by habituation or misunderstanding, nullifying the promised security.

About ten years ago, the Fast Identity Online (FIDO) Alliance began its operations, eventually pulling together Google, Microsoft, Apple and several hundred vendors and major end-users around a series of authentication standards. Today, the products that carry FIDO certification are the most secure mechanisms to protect users' logins. Ironically, FIDO has brought about a return to the hardware fob, albeit in a somewhat different form factor. What makes FIDO security keys more secure than other forms of MFA is that no user secret information is stored outside the key or transmitted anywhere. Instead, authentication data is processed by software on the end user's device. FIDO also gets rid of the need for custom programming an authentication solution using proprietary or insecure methods and replaces them with an open standards-based approach. Additionally, use of Fido devices also divorces MFA methods from the actual apps that have to depend on them. It has taken FIDO several years to

get to this point, but there are now more products that can deliver better authentication experiences. YubiKey, SoloKeys, or Google's Titan Security keys all support various aspects of the Fido protocol and cost around $50 apiece, as shown in the photo below.

Various hardware keys used for MFA, including the latest FIDO-support keys along the right side and RSA's latest SecurID. (credit: D.Strom)

But these hardware keys have issues, just like any other piece of hardware that you carry around. First, you'll want to have at least two keys and keep them stored in two separate places, just in case you lose one. Second, the keys fit into your devices via a variety of connection methods or transports, such as USB-A, USB-C, Bluetooth, or NFC. That means managing a key collection and matching it with the appropriate endpoint device and connector. And you have to remember which key is used to authenticate you to a particular account, which can be annoying even for the most fervent FIDO supporters. While Google has deployed them for all of its employees, they haven't caught on elsewhere.

Some vendors have tried to combine FIDO keys with other security factors to make an easier and more usable solution. These so-called "passwordless" products are really adaptive authentication routines that adjust how much MFA is needed to complete a particular operation. Some products, for example, consider biometric factors such as finger gestures, typing cadence, geo-location, or leverage the phone's secure enclave to store their keys. That is a step in the right direction, although they are still difficult to implement across the enterprise.

The next evolution of the Fido protocol will arrive soon in the form of Passkeys. These will be cross-platform, syncable credentials built atop the Fido protocol, and they overcome many of the usability challenges associated with Fido hardware security keys. Passkeys will work in much the same way that operating systems and major browsers offer to recall passwords and sync them across devices for users. This solves for issues such as needing to enroll multiple security keys and keep one or more as backups. Passkeys will leverage hardware that supports user verification through biometrics to provide assurance to the application or service that a user is not only in possession of some device but matches the enrolled identity of the authorized user. Passkeys are shaping up to be a realistic password replacement scheme for individuals, but enterprises my be slow to adopt them or may avoid them entirely, as the private keys associated with each Passkey are stored on and synced across all devices into which a user is signed in. For an individual, the hurdle for an attacker to compromise the security of that person's operating system and Passkey-syncing mechanism is likely too high. However, an attacker my find the effort worthwhile if it results in compromising the private keys associated with all of an employee's logins, allowing him or her leverage those credentials to gain further access to the enterprise.

Choosing the Right MFA

So which MFA method should you choose? If you're looking to integrate MFA into an application or service, the fastest to implement is often SMS-based TOTP, but it isn't considered secure and shouldn't be used as a primary MFA method. For users of existing services and application that offer multiple MFA options, authenticator apps are far better than SMS-based options. They are more secure and support almost every SaaS app, but you still have to type in the one-time codes, meaning these can be shared or phished. FIDO hardware keys are a great option for anyone interested in preventing credential theft and phishing attacks, but use of the security key is in no way tied to the identity of the user, meaning anyone can avail oneself of the security key — not just its intended user.

What is needed to make MFA completely successful is to have a marriage of security, usability and privacy that doesn't compromise any one particular aspect. The ideal MFA method must be easy to administer, easy to apply to a user's login, and it needs to work across all modern endpoint OSs and web browsers. The best approach is to have something that you carry on your person, which makes wearable devices, such as the Token ring, an attractive option. This is helpful in that you don't have to worry about losing it or leaving it at home when you travel. It also can tie the person to the use of the authenticator device and avoids having to remember and type in the one-time passcodes generated by a smartphone authenticator app. Most importantly, it must provide assurances beyond a user having some knowledge factor and being in possession of a trusted device. Only those MFA solutions that can verify that the individual attempting to authenticate matches the enrolled identify of the valid user will be able to offer the level of security assurances necessary for enterprise and support future passwordless login standards built atop the Fido protocol.

Multi-factor Authentication methods comparison

MFA Method	Pros	Cons
SMS	Easiest to implement	Easiest to compromise
Authenticator phone app (Google, Authy)	Wide app support	Tied to your phone in most cases, still have to type in the one-time code manually
Hardware keys (Yubico, Titan)	More secure than software tokens, Fido support	Need multiple keys in multiple locations, easy to forget, multiple connector form factors
Passwordless tools	Support for adaptive authentication	Complex to setup and manage at scale
Passkeys	Convenient, Fido Support, Support for passwordless Logins	Private keys are synced and stored across devices and potentially remote servers
Integrated biometric hardware	Key is tied to your identity, Fido support, Support for passwordless Logins	Users must enroll to the device and then enroll the device with each app or service

For developers, supporting Fido/WebAuthn in your applications and services is paramount. Arguably the best MFA options for individuals and enterprises alike are being built atop this standard. Individual users who value convenience, TOTP apps are a good option for now, but consider using Passkeys when support for them becomes available in early 2023. For enterprises, hardware security keys are ideal, especially those that can biometrical verify the identity of the user. These devices offer tremendous security benefits against credential theft, reuse, and misuse. Tying the use of the authenticator to the user's identity will only become more important as true passwordless security becomes available.

It is fortunate that so many MFA methods exist to choose from today. While using any of them is better than just using a simple login/password pair that can be quickly compromised, the best choice for today and into the future is something that you carry with you, that understands your biometrics, and can be married to your identity without any operator intervention. Ransomeware and data theft are only increasing in severity. It's time for the defenders to up their game as well.

BIO: David Strom is a well-known author who writes frequently about security and B2B IT topics and can be found on Twitter @strom or at http://strominator.com.