TechTarget | SearchSecurity

E-guide

PRO+ Content

Authentication Compared: Biometrics vs. 2FA vs. MFA

In this e-guide

In this e-guide:

Authentication is an important piece in any security strategy, but there are a number of frameworks to choose from. What method is better for securing enterprise devices and systems?

In this guide, experts Craig Mathias, Michael Cobb, and Randall Gamby weigh in on the advantages and disadvantages of 3 different strategies: biometrics, 2FA and MFA.

You'll uncover answers to top questions, such as:

- **Is mobile 2FA is better than biometrics?**
- **What are the pros and cons of behavioral biometric technology for enterprises?**
- **What's the difference between 2FA and MFA?**

In this e-guide

Why mobile two-factor authentication is better than biometrics

Craig Mathias, Principal - Farpoint Group

Teamed with physical security, integrity management, encryption and authorization, authentication is one of the key elements in any good security strategy.

Traditional authentication methods are based on a single element or factor. For example, I can say "my name is Craig." Yes, my name really is Craig, but how does someone know it's true? Because I say so? Obviously enterprise mobile security can't run on the honor system.

Everyday billions of transactions take place based on a single authentication factor -- typically, a password. Because IT often uses authentication to derive encryption keys and so many users work with mobile devices that are easily lost or stolen, one-factor authentication doesn't really make sense. Instead, mobile two-factor authentication is key.

Biometrics authentication uses biological information for authentication purposes. Fingerprint scanners have been in use for decades, and new smartphones such as the Samsung Galaxy Note7 utilize iris scanners. Because each of these factors is unique to a given individual, biometrics should be the perfect authentication factor.

In this e-guide

Unfortunately, it is not. Despite the likelihood that these features differ on an individual basis, and the fact that they are more difficult to duplicate than other factors used in authentication such as passwords, biometrics is still not enough on its own.

It's possible for someone to fake a fingerprint, because people leave fingerprints everywhere. And facial recognition is great until a user grows a beard, shaves or otherwise changes his appearance. DNA would likely be the ideal biometric marker, but DNA scanners are complicated, expensive and time-consuming.

If biometrics isn't perfect, is anything?

Absolute security does not exist, and it likely never will. But two-factor or multifactor authentication, which requires users to identify themselves with something they have, plus something they know -- a physical device plus information stored in their biological memory, for example -- can improve security immensely.

The something the user has could indeed be biometric, or it could be a hardware token such as a personal handset. If the handset serves as a sufficient form of authentication, biometrics isn't necessary. Biometric data could serve as a third or even fourth factor in high-security situations, but it is certainly not required.

IT shops must remember that biometrics authentication systems alone are inadequate as the sole basis for authentication. In fact, every single-factor

In this e-guide

authentication mechanism is similarly vulnerable. Ideally, vendors will realize two-factor authentication is the minimum, no matter how sophisticated each factor might be. As a result, it is best not to rely on fingerprint scanners alone. The same goes for the iris scanner in the Galaxy 7.

Even with mobile two-factor authentication, bugs, operational errors and new threats appear with alarming regularity. IT must evaluate each element of any security strategy in terms of its effectiveness and potential vulnerabilities. The time is now to make two-factor authentication a priority.

Next article

In this e-guide

The enterprise potential of behavioral biometrics

Michael Cobb, CISSP-ISSAP and IT security author

The convenience of frictionless user authentication that biometric verification offers is one of the main reasons so many OEMs are beginning to incorporate various biometric authentication options into their devices. People are becoming quite familiar using their fingerprints or faces to unlock their computers and mobile devises, and it's a lot more user-friendly than having to remember and type in a password or PIN

Physiological characteristics like fingerprints, face, hand and retina represent just one type of biometric identifier, though. The other is behavioral characteristics, which are related to the pattern of behavior of a person, such as typing rhythm, gait, gestures and voice. It's nearly impossible to copy or imitate somebody else's behavior well enough to fool behavioral biometrics verification, as everyone's mannerisms and body language traits are shaped by social and psychological factors, which make them unique.

The advantages of behavioral biometrics

A big advantage of behavioral biometrics is that the identifiers can be discreetly monitored in real time to provide continuous authentication, instead of a single one off authentication check during login. For example, a

In this e-guide

user's keystroke length, typing speed, error patterns and mouse movements can all be used to create a unique template that distinguishes their typing from some else's. This can be used to continuously authenticate users in real time based on their mouse movements and keystrokes.

Enterprises with many users who regularly access sensitive data, such as customer support staff, can certainly benefit from this additional type of authentication to help detect when the correct person is not operating a device. A banking app could lock access to an account or prompt for a second factor of authentication if it detects irregular keyboard, mouse or touch interactions.

Analyzing body movements such as gait can be used to identify people from a distance; gait is hard to disguise because a person's build and muscles essentially limit their variation of motion, and could be used to ensure only authorized people, such as security guards, are present in a restricted area.

Behavioral biometrics: Disadvantages

While behavioral characteristics can provide continuous verification of a user, they are not so practical when it comes to the actual login process. A fingerprint reader only needs to take one reading to allow or deny access, whereas a user would have to type for a period of time before enough data had been captured to make a check. This delay in logging on is not what vendors or users are looking for.

In this e-guide

There are also concerns over stolen biometric data, such as what occurred in the Office of Personnel Management data breach, though it's a threat that the security industry doesn't yet fully understand. However, it should prove difficult for an attacker to automate the abuse of stolen biometric data in the same way they can passwords, and behavioral biometric data more so than physiological data like fingerprints.

One disadvantage with all forms of biometric identification is there is an element of interpretation. It is easy for a computer system to check whether the password submitted is the same as the password stored in its database, but the check in biometrics is more "like" than "equal to." The matching algorithm has to make a decision based on an acceptance threshold that determines how close to a template the input needs to be for it to be considered a match. This can lead to false negatives, which would prevent valid users from authenticating successfully, while false positives would allow unauthorized users to authenticate successfully -- the last thing purchasers want in an authentication product. The threshold needs to be set to ensure the right level of protection for the classification of the assets being safeguarded; some systems allow different thresholds for different types of users.

Behavioral biometrics can provide an additional layer of security and further strengthen defenses around highly sensitive data by monitoring in real time the way users interact with their devices. There are online fraud detection solutions coming onto the market that use behavioral biometrics to stop account takeover fraud and other fraudulent transactions, as well as malware such as RAT-in-the-browser. BehavioSec's product authenticates individuals in real time through behaviors like keystroke dynamics, touch and

In this e-guide

mouse motion, and compares those behaviors to previous interactions from the same user. It creates a session ticket and a confidence score so risk engines can add additional security steps if required. The system continually redefines a user's behavior profile by learning from every interaction to reduce false positives. Other products include NuData Security's NuDetect and BioCatch's Behavioral Authentication. SecureAuth Corporation in partnership with BehavioSec is releasing an API platform that will allow enterprises to develop custom continuous, passive authentication capabilities for their own IT infrastructures.

Next article

In this e-guide

Which authentication method is better: 2FA or MFA?

Randall Gamby, Master Security Architecture Consultant – HP

What's the difference between two-factor authentication and multifactor authentication? I've seen both terms used, but the specifics are still a bit unclear. What's the better option in terms of securing devices and systems?

Each of these authentication frameworks uses more than a simple username/password scheme to identify an individual, but they go about it in different ways. Two-factor authentication (2FA) uses a single authentication step where the individual authenticates with something he knows, for example a login name, and something he has, such as a biometric component -- like retinal scans, fingerprints or voice recognition -- or an assigned 2FA token issued by the organization. For example, when I log onto my workstation it first prompts me for my login name, then prompts for the number showing on my hard token that I have on my person. If both match my login data, then I can then access my files.

Multifactor authentication (MFA) can include both 2FA and non-2FA credentials, but its major distinguishing factor is that it is a multi-authentication process. Using the same example from above, when I log onto my workstation it prompts me for my login name, and then prompts for the number showing on my hard token. I am then prompted to enter a

In this e-guide

number that is texted to my mobile phone. If the information entered matches my login data I can then access my files. In reality, instead of working in conjunction with a 2FA credential, more often than not MFA is used with a simple username and password, and the number from a text message to a mobile phone, or some other non-2FA information such as secret question responses, typing in text garbled on an image, picking an image that the user previously selected in another session, or entering additional account information.

MFA and 2FA require something you know and something you have to authenticate, and are considered even when it comes to security. However, information like answers to a secret question, is easier for attackers to discover or guess, thanks to the Internet of Things, social media and other potential sources of data leaks, so 2FA is considered more secure. But the bigger question to ask when deciding whether to use 2FA or MFA is which is more easily supported by your applications and infrastructure? If the applications you wish to protect only support one or the other then the answer is quite clear: use the one supported. If the applications can support both, 2FA would be the preferred method since the user only has to perform one authentication event. If the applications support neither, then it might be necessary to recode the application. Regardless of which method you choose, both will require some level of registration process changes, and of course the end users will need to be trained on how to use the new authentication method and how to seek help should they run into an issue logging in.

Next article

In this e-guide

About SearchSecurity

IT security pros turn to SearchSecurity.com for the information they require to keep their corporate data, systems and assets secure.

We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security certification training resources, security standard compliance, webcasts, white papers, podcasts, Security Schools, a selection of highly focused security newsletters and more -- all at no cost.

For further reading, visit us at http://SearchSecurity.com/

Images; Fotalia