Using mobile biometric authentication to elevate enterprise security

AWARE

eBook

Biometric authentication in the enterprise? It's just a matter of time

Mobile biometric authentication is officially here to stay. Most of today's leading devices come with native biometric sensors, and virtually all have cameras, microphones and touchscreens that can be used for biometric authentication.

Consumers have embraced this transformation; **86 percent have shown interest in biometric authentication according to research by Visa.** Passwords, PINs, and knowledge-based authentication are steadily losing ground to biometrics as a primary means of authentication among personal users.

Biometric adoption among enterprise users has moved more slowly, in large part because the biometric functionality and user experience offered natively on devices varies by vendor and model and can't be controlled; it's a black box. This makes using them for high-security applications more difficult.

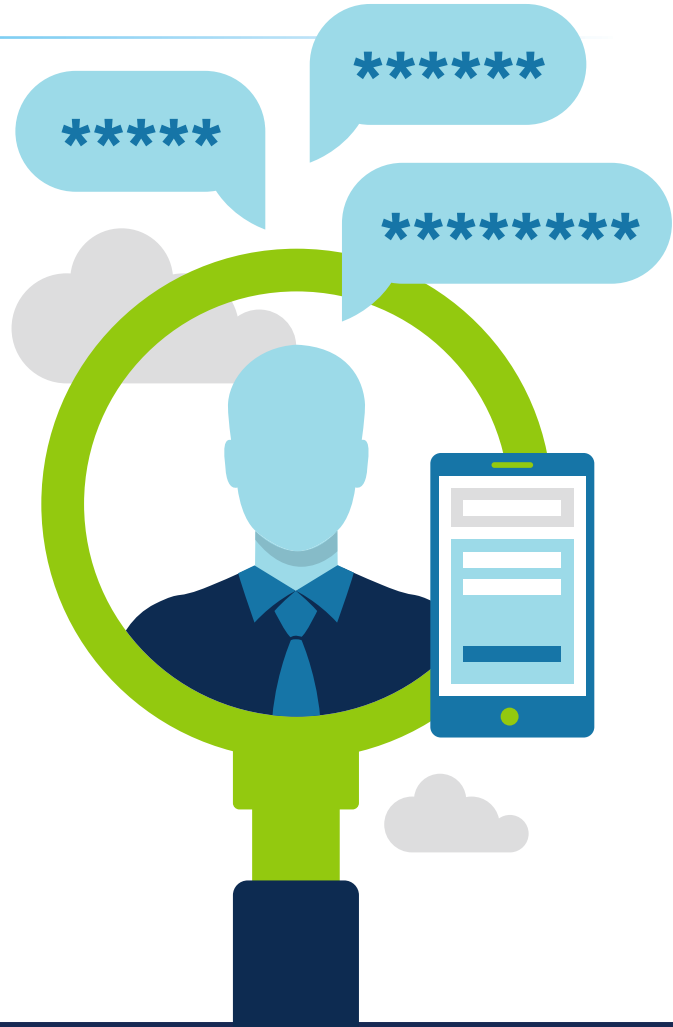
This challenge can be addressed by implementing biometrics that utilize the generic sensors of the devices: the camera, microphone and touchscreen. This way, an enterprise can apply biometric security across all devices, and wield control over the functionality, user experience and performance.

Enterprises are already adopting phone-as-a-token approaches to multifactor authentication; the basic infrastructure for enterprise biometrics already exists. The convenience and security benefits make biometric authentication for the enterprise look less like a possibility and much more like an eventual certainty.

Authentication mechanisms are out-of-step with enterprise evolution

Biometric authentication is necessitated, not by trendiness or consumer demand, but by a fundamental transformation in the shape of the modern enterprise.

- **Cloud computing** has enabled anytime, anywhere access to digital productivity resources, spurring the prevalence of remote workforces and bring-your-own-device policies.
- In that same vein, **employees are no longer bound to local networks** or to a fixed number of enterprise endpoints, a dynamic that obscures attempts to spot suspicious network activity.
- The growth of **microservices** has increased the number of sign-ons and authentications among enterprise users, making password management riskier, more complex, and inconvenient.



In short, enterprises need to protect significantly larger and more elusive network perimeters. All too often, the main barrier preventing fraudulent access to information systems is passwords.

This may have worked 10 years ago, but not today.

Why passwords fail

Passwords may exist into the future as a secondary authentication factor, but they're inadequate as a primary authentication measure in today's complex computing and networking environment. After all, they were conceived in the 1960s before any of today's threats existed.

Their most evident flaw is that they can be stolen through phishing schemes, keylogger malware, brute-force attacks or password server breaches. Once compromised, passwords are easy to leverage for further malicious activity. Case in point, **lost or stolen credentials were directly involved in approximately 80 percent of all data breaches in 2017**, according to Verizon's Data Breach Investigations Report. Enterprises are generally aware of this, which is why so many businesses spend an inordinate amount of time managing passwords.

Plus, passwords are notoriously inconvenient. The number of services we use requiring passwords is growing exponentially, and the security levels are increasing, with longer, more complex strings and more frequent changes. Some organizations have leveraged single sign-on (SSO) applications or password managers to limit the number of passwords that users need to remember, let alone replace every few months, but this has the effect of reducing security.

New layers of access demand new layers of authentication

Many organizations leverage a possession-based token when verifying a remote access request, such as sending a message containing a one-time password (OTP) or a login-confirmation link to an employee's smartphone.

While better than the password-only approach, possession, like knowledge, can be transferred. A hacker can use a stolen smartphone, for example, to request a password reset. Meanwhile, an employee who loses a "security dongle" or accidentally leaves it at the office effectively forfeits remote access to enterprise applications. The former approach to possession is inadequate and the latter is inconvenient.

Security and convenience converge in a third factor of authentication enabled by modern mobile devices: inherence, or something the user is.

This involves taking the concept of phone-as-a-token authentication, and adding biometrics to the equation.

Out-of-band, mobile biometrics: The next step in enterprise security

Mobile biometric authentication requires smartphones with high-quality sensors and the processing power to perform biometric authentication. Only a few years ago these devices were the exception; now they're the rule. Mobile network coverage is no longer a factor. So today, mobile biometric authentication goes wherever it is needed, and the performance is well-suited for enterprise security.

A user starts the enrollment process by registering their mobile device with their employer, either in person or remotely. They also register their biometrics to their device (e.g. by taking a selfie and speaking a passphrase) as part of that process. In this way, the user's identity is biometrically bound to the device and to the identity server.

When a user logs into an enterprise application from their PC or laptop, a message is sent to the registered phone, prompting them to biometrically authenticate; again with face and voice. Only the device owner can use it to authenticate, so a lost or stolen device cannot be used for illicit access.

The result: enterprise applications are hardened against unauthorized access by multifactor authentication, using a personal device as a token that cannot be used fraudulently if lost or stolen.

Architecting a biometric solution for the enterprise

Smartphone apps with biometrics enable anytime, anywhere multifactor authentication, so that enterprise users can access the applications they need, when they need them. Enterprises, meanwhile, can be confident in their ability to prevent unauthorized access despite their expanding perimeters.

Mobile biometrics are an extension to well-established authentication measures that use tokens and out-of-band mechanisms to make breaches more difficult while preserving convenience. So while implementing biometric authentication does not require forklift upgrades, some decisions do need to be made.

The first is what biometric modalities are to be used. Each has its pros and cons for a given use case. Using multiple modalities increases performance and options for users. Some modalities that use the ubiquitous sensors on devices are face, voice and keystroke dynamics.

Another choice is between a device- or server-centric approach. Both are compatible with an out-of-band implementation. A device-centric approach enhances privacy and reduces risk of breach by keeping biometric data on the device. The adoption of FIDO® Alliance specifications for device-based authentication has resulted in a large marketplace of FIDO® Certified authenticators.

A server-based approach stores the matching engine and biometric templates on the server. An advantage here is the ability to use these same biometrics for other purposes, and also to be able to use the biometric data to better diagnose issues and improve algorithm performance.

Infrastructure and integration considerations are not the burdens they once were. Rather, they're opportunities to create a high-performance biometric authentication framework uniquely suited to a given enterprise's needs and capabilities.

Multimodal biometrics and liveness detection enhance performance and security

Enterprises can further enhance the performance and security of mobile biometric authentication with liveness detection and multiple biometric modalities.

For example, the availability of facial images and videos on social media and elsewhere introduces the possibility of fraudsters attempting to use a digital image of a person to "spoof" facial recognition-based authentication. Adding liveness detection helps protect against such an attack. Adding a modality serves to further complicate the efforts of a fraudster while also improving biometric performance.

For example, adding voice as a second modality for facial recognition improves matching performance by an order of magnitude. It also requires a fraudster to acquire much more data to launch a spoofing attack.

These measures are particularly important where users are enrolling remotely without third-party supervision, to ensure the validity of the reference biometric samples. Ideally, the addition of a modality does not result in less convenience for the user. The face image can often be captured simultaneously with voice or keystroke, for example.

Creating a new enterprise standard with mobile biometric authentication

The proliferation of powerful mobile devices has changed our lives in many ways; one of them is the introduction of a more convenient and secure approach to authentication across enterprises' ever-expanding digital ecosystem.

With the recent improvements in mobile biometrics, enterprises can finally look forward to ending their reliance on passwords and dongles for securing their assets. The combination of "something-you-have" with "something-you-are" authentication factors is more secure and more convenient than using secrets. Biometrics are not secrets; they can't be "stolen," and spoofing is preventable. Passwords will likely play a supporting role in the future of enterprise authentication. But today's businesses have too much to lose from overreliance on antiquated security measures that can be compromised by novice hackers with a malware kit and an email address. The standards for enterprises have changed because the enterprise itself has changed.

A convergence of game-changing technology advancements—smartphones and sensors, biometric algorithms, cloud computing, machine learning and others—have brought biometrics to the forefront of authentication solutions, and enterprises likely have the most to gain as they use them to secure their most valuable digital assets from theft and fraud.

Visit Aware's website to learn more about how mobile biometrics can make authentication more secure and convenient for your employees.

AWARE

Sources:
https://usa.visa.com/visa-everywhere/security/how-fingerprint-authentication-works.html
https://www.biometricupdate.com/201808/biometrics-catching-up-to-passwords-as-preferred-method-of-online-identification-for-consumers
https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf