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.

Creating a new enterprise standard with mobile biometric authentication

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 images can often be captured simultaneously with voice or keystroke, for example.

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.

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

www.aware.com

Using mobile biometric authentication to elevate enterprise security

Sources:
https://usa.visa.com/visa-everywhere/security/how-fingerprint-authentication-works.html
Biometric authentication is necessitated, not by trendiness or consumer demand, but by a fundamental transformation in the shape of the modern enterprise. Enterprises are already adopting phone-as-a-token authentication for the enterprise look less like a possibility and much more like an eventual certainty.

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 compute the biometric with the sensors. Now, more than 10 years ago these devices were the exception; now they’re the norm. No biometric authentication system can exist now without multi-factor authentication.

This involves taking the concept of phone-as-a-token authentication, using a personal device as a token that possesses the matching biometric. The result: enterprise applications are hardened against unauthorized access and can pass on biometric data to better diagnose issues and improve algorithm performance.

Architecting a biometric solution for the enterprise

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 link confirmation to a user’s employer’s mobile device. This is the traditional approach to authentication, using a personal device as a token that possesses the matching biometric. Using multiple modalities increases performance and options for users. However, the two main challenges are the trade-offs between usability and performance, and the security risks associated with storing biometric data on the device.

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 the biometric data to prove that a lost or stolen device cannot be used to illicit access.

Although biometric application developers are hardened against unauthorized access by multi-factor authentication, using a personal device as a token that possesses the matching biometric data to better diagnose issues and improve algorithm performance.

Architecting a biometric solution for the enterprise

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 link confirmation to a user’s employer’s mobile device. This is the traditional approach to authentication, using a personal device as a token that possesses the matching biometric. Using multiple modalities increases performance and options for users. However, the two main challenges are the trade-offs between usability and performance, and the security risks associated with storing biometric data on the device.

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 the biometric data to prove that a lost or stolen device cannot be used to illicit access.

Although biometric application developers are hardened against unauthorized access by multi-factor authentication, using a personal device as a token that possesses the matching biometric data to better diagnose issues and improve algorithm performance.

Architecting a biometric solution for the enterprise

The result: enterprise applications are hardened against unauthorized access and can pass on biometric data to better diagnose issues and improve algorithm performance.

Architecting a biometric solution for the enterprise

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 link confirmation to a user’s employer’s mobile device. This is the traditional approach to authentication, using a personal device as a token that possesses the matching biometric. Using multiple modalities increases performance and options for users. However, the two main challenges are the trade-offs between usability and performance, and the security risks associated with storing biometric data on the device.

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 the biometric data to prove that a lost or stolen device cannot be used to illicit access.

Although biometric application developers are hardened against unauthorized access by multi-factor authentication, using a personal device as a token that possesses the matching biometric data to better diagnose issues and improve algorithm performance.
Using Biometric Authentication to Elevate Enterprise Security

Passwords, PINs, and knowledge-based authentication are widely-outused across all industries, but are no longer secure. As network threats continue to evolve, enterprises are seeking new layers of authentication to bolster their security posture.

Enterprises are already adopting phone-as-a-token approaches to multifactor authentication; the basic functions and user experience are similar across all devices, and wield control over the functionality, user experience and performance.

Authentication mechanisms are out-of-step with enterprise evolution

In short, enterprises need to protect significantly larger and more critical data, and thus, there is a need for more advanced authentication methods. Biometric authentication is necessitated, not by trendiness or necessity, but rather because it offers a unique combination of convenience and security.

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

Why passwords fail

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 link confirmation to an employee’s smartphone. While better than the password-only approach, possession-based authentication is still inadequate as it can be lost or stolen.

To combat this challenge, many enterprises are adopting software-based token solutions, which provide an additional layer of security by requiring users to enter a password along with the token code. However, these solutions still suffer from several limitations. For example, if an employee loses a token or forgets their password, they may be locked out of their account.

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

New layers of access demand new layers of authentication

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; against unauthorized access by multifactor authentication, using a personal device as a token that phone, prompting them to biometrically authenticate, again with face and voice. Only the device owner can use the biometric data to log-in; 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.

Out-of-band, mobile biometrics:

Architecting a biometric solution for the enterprise

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 removing biometric data from the device. The adoption of FIDO Alliance specifications for device-based biometric 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 biometric templates 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 only factors to consider. Rather, enterprises must also focus on creating a high-performance biometric authentication framework uniquely suited to a given enterprise’s needs and capabilities.
Mobile biometric authentication is officially here to stay. Most of today’s leading devices come with native biometric sensors, and so do all these 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. Why? Passports, 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 device: the camera, microphone and touchscreen. This way, enterprises can apply biometric security across all devices, and avoid 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 like a possibility and much more like an eventual certainty.

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 invented in the 1950s before any of today’s threats existed.

Their most evident flaw is that they can be stolen through phishing schemes, keyloggers, malware, brute force attacks or password server breaches. Once compromised, passwords are easy to use 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.

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 capture those sensors. A new report by Verizon shows that 3 years ago these devices were nonexistent; now they’re the majority. Mobile biometric authentication is a real possibility.

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 asset.

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 the biometric data to sign on or to unlock the device.

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.

Authentication mechanisms are out-of-step with enterprise evolution

Cloud computing has enabled anyone, 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 obviates 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 more complex, and inconvenient.

In short, enterprises need to protect significantly larger and more elusive network perimeters. All too often, the main barrier to enterprise security is the same: passwords.

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 transformed. 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 forecloses remote access to enterprise applications: anyone who has possession is inadequate and the latter is inconvenient.

Security and convenience converge in a third factor of authentication: the device. 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. 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 leveraging 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 architectures can address these challenges.

FIDO® Alliance specifications for device-based authentication have resulted in a large marketplace of FIDO® Certified authentications.

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 anti-fraud performance.

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 leveraging biometric data on the device. The adoption of FIDO® Alliance specifications for device-based authentication has resulted in a large marketplace of FIDO® Certified authentications.

Architecting a biometric solution for the enterprise

Using Biometric Authentication to Enhance Enterprise Security

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

Authentication is not just a matter of time.

With so many industries -- including finance, healthcare, government, and retail -- facing an increasing number of cyber threats, it’s no wonder that enterprises have their work cut out for them. The challenge is to implement biometric authentication solutions that are effective, secure, and user-friendly.

Why is biometric authentication essential for enterprises?

Biometric authentication provides a layer of security that is unique to each individual, making it difficult for hackers to replicate. This is especially important in industries where data breaches can have severe consequences.

One of the primary reasons for this is that biometric authentication is based on physical characteristics, such as fingerprints, facial recognition, or voice biometrics. These characteristics are unique to each person and cannot be easily replicated by a hacker.

Out-of-band authentication, where the biometric data is collected and processed on the device, is becoming increasingly popular in the enterprise space. This approach helps to address the issue of data breaches by ensuring that the biometric data never leaves the device.

Out-of-band authentication also offers several advantages.

First, it is more secure than out-of-band authentication because the biometric data is never transmitted over the network. This reduces the risk of interception and theft.

Second, it is more convenient for users because they can perform biometric authentication anywhere and anytime, even when they are not connected to the network.

Finally, it is more efficient because it eliminates the need to store biometric data on the server, which can be a significant advantage in terms of both performance and cost.

In conclusion, biometric authentication is essential for enterprises because it provides a layer of security that is unique to each individual and cannot be easily replicated by a hacker. Out-of-band authentication offers a secure, convenient, and efficient approach to biometric authentication that is becoming increasingly popular in the enterprise space. Unternehmen und andere Organisationen sollten eine biometrische Authentifizierung in Betracht ziehen, um eine höhere Sicherheit bei der Benutzeridentifizierung zu gewährleisten.

Die biometrische Authentifizierung wird inzwischen in vielen Branchen üblich, da sie eine höhere Sicherheit bietet als traditionelle Verfahren wie PINs oder Passwörter. Mit der biometrischen Authentifizierung können Unternehmen sicherstellen, dass nur diejenigen, die die biometrische Identifikationsmethode kennen, Zugriff auf ihre Systeme erhalten.


Die biometrische Authentifizierung kann auch in Kombination mit anderen Sicherheitsverfahren eingesetzt werden, um eine zusätzliche Schicht der Sicherheit zu schaffen. Dies kann beispielsweise durch die Kombination von biometrischer Authentifizierung und einem One-Time-Password (OTP) erreicht werden.

Bei der Planung einer biometrischen Authentifizierung sollte man darauf achten, dass das System für die Benutzer so intuitiv wie möglich ist und dass es auch die notwendige Flexibilität bietet, um unterschiedliche Anforderungen zu erfüllen.

Insgesamt bietet die biometrische Authentifizierung Unternehmen und Organisationen eine sichere und effiziente Methode, um ihre Daten zu sichern und sicherzustellen, dass nur die berechtigten Benutzer Zugriff auf sie haben.

Die biometrische Authentifizierung wird in Zukunft sicherlich eine zunehmende Rolle in der digitalen Welt spielen, da sie eine höhere Sicherheit bietet und den Nutzern eine höhere Benutzerfreundlichkeit ermöglicht.

Therefore, it is important for enterprises to consider biometric authentication as a way to ensure secure and efficient access to their systems.

In conclusion, biometric authentication is essential for enterprises because it provides an additional layer of security that cannot be replicated by hackers. Out-of-band authentication offers a secure, convenient, and efficient approach to biometric authentication that is becoming increasingly popular in the enterprise space. Unternehmen und andere Organisationen sollten eine biometrische Authentifizierung in Betracht ziehen, um eine höhere Sicherheit bei der Benutzeridentifizierung zu gewährleisten.
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.

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.

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 enterprise even 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

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 features can often be captured simultaneously with voice or keystroke, for example.

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

Multimodal biometrics and liveness detection enhance performance and security

Using mobile biometric authentication to elevate enterprise security

Sources:
https://usa.visa.com/visa-everywhere/security/how-fingerprint-authentication-works.html
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.

www.aware.com