The Truth about Passwordless Authentication

What it is and how it works

Passwordless authentication is a means to verify a user's identity, without using a password. Instead, passwordless uses more secure alternatives like possession factors (one-time passwords [OTP], registered smartphones), or biometrics (fingerprint, retina scans).

Passwords haven't been safe for a long time. They are hard to remember, and easy to misplace. They are also the number one target of cybercriminals. So much so that 81 percent of breaches involve weak or stolen passwords.

In the following article, let's explore passwordless authentication in more detail.

What are the Types of Passwordless Authentication?

Passwordless authentication can be achieved in many ways. Here are a few:

- **Biometrics:** Physical traits, like fingerprint or retina scans, and behavioral traits, like typing and touch screen dynamics, are used to uniquely identify a person. Even though modern AI has enabled hackers to spoof certain physical traits, behavioral characteristics still remain extremely hard to fake.
- **Possession factors:** Authentication via something that a user owns or carries with them. For example, the code generated by a smartphone authenticator app, OTPs received via SMS, or a hardware token.
- **Magic links:** The user enters their email address, and the system sends them an email. The email contains a link, which when clicked, grants access to the user.

How Does Passwordless Authentication Work?

Passwordless authentication works by replacing passwords with other authentication factors that are intrinsically safer. In password-based authentication, a user-provided password is matched against what is stored in the database.

In some passwordless systems, like biometrics, the comparison happens in a similar manner, but instead of passwords, a user's distinctive characteristics are compared. E.g., a system captures a user's face, extracts numerical data from it, and then compares it with verified data present in the database.

In other passwordless implementations, comparisons may happen differently. E.g,. a system sends a one-time passcode to a user's mobile, via an SMS. The user receives it and enters it into the login box. The system then compares the user-entered passcode to the one it had sent.

Passwordless authentication relies on the same principles as digital certificates: a cryptographic key pair with a private and a public key. Although they are both called keys, think of the public key as the padlock and the private key as the actual key that unlocks it.

Digital certificates work in a way in which there is only one key for the padlock and only one padlock for the key. A user wishing to create a secure account uses a tool (a mobile app, a browser

Is Passwordless Authentication Safe?

Whether or not passwordless authentication is safe depends on your definition of safe. If safe means harder to crack and less prone to the most common cyberattacks, then yes, passwordless authentication is safe.

If by safe you mean, it is impervious to hacking, then no, it's not safe. There's no authentication system out there which can't be hacked. Maybe there is no obvious way to hack it, but it doesn't mean that the most sophisticated hackers can't work their way around its defenses.

With that said, passwordless techniques are inherently safer than passwords. E.g., to hack a password-based system, a bad actor may use a dictionary attack, which is often considered the most rudimentary hacking technique (keep trying different passwords until you get a match).

Even the amateur hackers can perform a dictionary attack. Conversely, it takes a significantly higher level of hacking experience and sophistication to infiltrate a passwordless system. E.g., only the most advanced AI algorithms can enable a hacker to spoof a fingerprint.

MFA vs Passwordless Authentication

Passwordless authentication simply replaces passwords with a more suitable authentication factor. On the other hand, MFA (multi-factor authentication) uses more than one authentication factor to verify a user's identity.

For example, an MFA system may use fingerprint scanning as the primary authentication factor and SMS OTPs as the secondary.

People sometimes confuse passwordless with MFA or use the two interchangeably. That's because many traditional, password-based login systems have started using a passwordless technique as their secondary authentication factor.

How Do I Implement Passwordless Authentication?

Here's how you could approach implementing passwordless authentication:

1. **Pick your mode:** The first step is choosing your preferred authentication factor. Available options range from fingerprints and retina scans to magic links and hardware tokens.

based passwordless authentication. For other modes, like magic links or mobile OTPs, you may only have to procure software.

4. **Provision users:** Start registering people on your authentication system. E.g., for a face recognition system, you will need to scan the faces of all your employees.

Implementing passwordless authentication in-house can be time-consuming and complicated. This is why many businesses prefer outsourcing to third-party IAM providers (like OneLogin) instead. This speeds up the process and significantly reduces maintenance costs and worries.

Is the Future Passwordless?

Even though passwords are far less prevalent than ever before, they are still being used worldwide. The primary reason is that a password-based login system is the easiest and the cheapest to implement. However, we expect passwordless to take over soon.

In the last two years, we have had more cyberattacks than ever before. This is setting off alarm bells in many companies, with more and more investments being made into biometrics and adaptive authentication (more on this in the next section).

Moreover, many companies have now realized that passwords are the primary reason for data breaches. The cost of implementing passwordless is nothing compared to the fines and losses incurred due to a data breach.

Last but not least, passwords are a nuisance for users. Hard to remember and a pain to reset. On the other hand, passwordless techniques, like biometrics, are convenient and much more user-friendly.

Combine Passwordless Authentication with Adaptive (Behavioral) Authentication

Even though passwordless authentication is a major improvement over using passwords, it's still not infallible. Biometrics can be spoofed, OTPs can be intercepted, and hardware tokens can be stolen. This is why you need a system that goes beyond just authentication factors to verify identity, i.e. adaptive authentication.

Adaptive authentication uses machine learning to develop patterns of typical user behavior. Any time the system notices a deviation from the pattern, it regards the login attempt as risky and takes appropriate actions.

For example, let's suppose a user logs in to the system, via their laptop, early in the morning, every weekday. Over time, the system establishes that this is their typical login behavior. Then one day, the user logs in to the system on a Saturday.

They still used the same laptop, it was still early in the morning, and their geographical location was the same as well. The system calculates a relatively higher risk score for this behavior, which warrants the use of a secondary authentication factor, like an SMS OTP.

A few days later, the system notices a login attempt from the same user, originating from a different country, and from a different device. It calculates an exponentially higher risk score, and blocks the user. It's later found out that it was a login attempt from a cybercriminal who had spoofed the user's identity.

Combining passwordless with adaptive authentication can make your system much more resilient. It's harder to hack passwordless factors, but not impossible; adaptive authentication helps you add another, AI-powered layer of protection.

Related Resources

5 Reasons Relying on Passwords is a Recipe For Disaster

Passwords alone are not enough to protect your corporate data. Here are five reasons why.

Read the Blog →

How MFA Helps Prevent Common Cyberattacks

See how Multi-Factor Authentication (MFA) helps to prevent some of the most common and successful types of cyber...

Learn More →

SmartFactor Authentication

See how SmartFactor Authentication uses machine learning to automatically adjust authentication behavioral patte...

Read More →