DUO | cisco SECURE

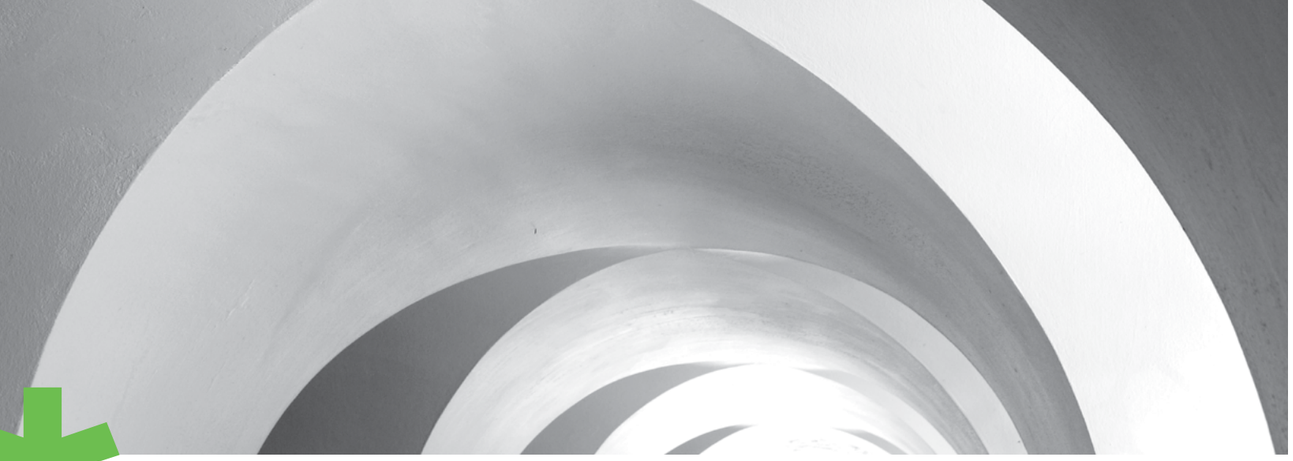
ADMIN'S GUIDE TO PASSWORDLESS

Busting Passwordless Myths

ADMIN'S GUIDE TO PASSWORDLESS

Busting Passwordless Myths

Table of Contents



MYTH 1

Passwordless is Less Secure than Multi-Factor Authentication

If you go by just the name, “Passwordless” could refer to any login experience that doesn’t require a password. An absurd example would be one that simply logs you in using a username, and nothing else. In considering a passwordless solution, we want to raise the security bar, not lower it.

> Part of ensuring that passwordless is just as secure as multi-factor is ensuring that it *is* multi-factor.

During account registration, the authenticator generates a credential and passes the corresponding public key to the website for association with the user account. Later, during login, the authenticator uses the private key associated with that credential to sign a message known as an assertion, and passes it to the website. The website uses the credential public key, from the registration step, to verify the signature on the assertion. This verification proves control over the credential, which, if properly protected, strongly identifies the authenticator device (and, by extension, the user).

But how do we know that it’s really our user that holds the credential and not an imposter? For instance, someone who stole the authenticator device.

For that, WebAuthn and CTAP2 support a User Verification (UV) flag, wherein the authenticator device must first locally verify the identity of the user before it can unlock the credential to sign messages. This often takes the form of a biometric check, such as a fingerprint or face scan. Alternatively, users can unlock the credential using a local PIN. Notably, the biometric or PIN never gets sent to a server or otherwise leaves the device.

Since User Verification generally can only be performed locally, attacks against this user verification process become very labor-intensive and must be targeted at specific users, greatly increasing the difficulty of attacks.

MYTH 2

PINs Are Just Passwords

We already talked about how passwordless authentication is still multi-factor:

- Possession of a private key, ideally stored on a piece of secure hardware
- A biometric or PIN the authenticator uses to locally verify the user's identity

Reasoning about a PIN being used as a factor is simpler than a biometric. A PIN is simply a password, with a few key differences. The most critical difference is the context in which it is used for authentication in WebAuthn.

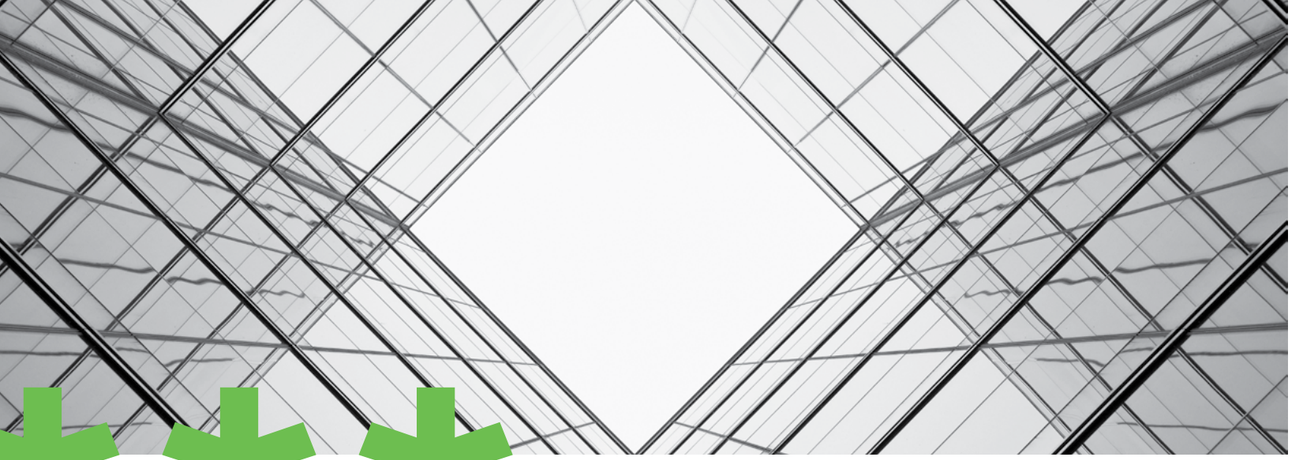
Unlike a password, which is transmitted to the website and checked against the website's record (hopefully, a salted hash, and not a copy of the password itself), a PIN is used only to unlock the credential stored on the local authenticator device. There is no central repository of user PINs for an attacker to breach and steal, no remote access to the authenticator for an attacker to brute-force over the network. The only way to unlock the credential is for the user to locally, often physically, interact with the authenticator device and enter the PIN.

By way of analogy, let's consider the teleporting burglar problem. Why a teleporting burglar? Because remote attacks on the internet are similar in nature – an attacker can instantly "travel" to any "door" in order to attempt a theft. To reduce the risk of a burglar who can teleport, we can (a) make our keys harder to forge and our locks harder to pick, or (b) stop the burglar from being able to teleport.

Burglars who have to walk from house to house are much less of a threat. By enforcing local authentication via PIN, we effectively force remote attackers to "walk" to each account they want to hack. Even weak local authentication stops most remote attacks cold. Switching to local evaluation of a user's identity eliminates several entire categories of attacks that impact organizations and individuals today.

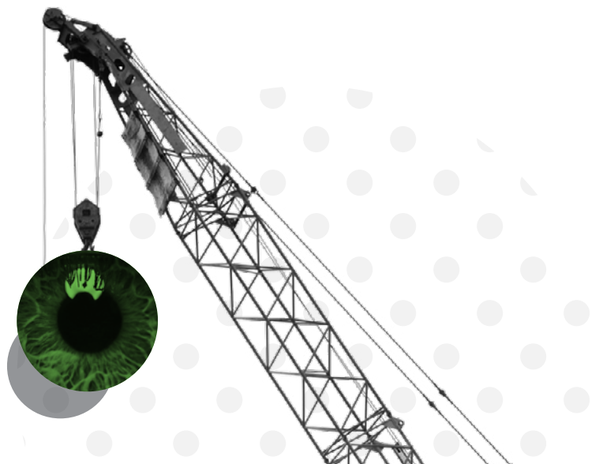
Because a user must be able to locally access the authenticator to enter the PIN, and authenticators often lock after a small number of incorrect attempts, the complexity requirements we associate with "good" passwords may not be necessary. Using numbers, symbols, capital and lowercase letters, with a minimum character count, all aim to deter attackers who can brute-force guess trillions of passwords per second. When an attacker gets 10 guesses total and has to enter them all by hand, a random six-digit numerical PIN (search space of one million) becomes sufficient to block bad actors, and is substantially more practical to enter on some devices than a complex password.

Nevertheless, it can be hard to shake off a vague sense of uneasiness around using such a weak "password" as an authentication factor. Is this because we're worried about remote attacks? Hopefully not. But what about local attacks? Shoulder surfing? Someone recording us unlocking our devices? Fingerprints on the glass that reveal which digits were pressed? Hollywood and its abundance of spy movies give us some great ideas for how a local PIN might be attacked. So if local attacks are part of your threat model, let's consider biometrics.



MYTH 3

Passwords Are Safer Than Biometrics



Biometrics get a bad rap. They're basically magic. And by magic, we mean difficult to reason about. There are many different kinds of biometric sensors, and even two sensors that measure the same biometric feature, such as a fingerprint, may do so in completely different ways, and be subject to completely different attacks.

At the lower end of the spectrum, biometric sensors like optical fingerprint sensors and single-lens cameras for facial recognition can be spoofed with photos printed by a $50 inkjet printer. On the higher end of the spectrum, facial recognition sensors like Apple's Face ID and Google's Face Unlock use multiple cameras and near-infrared dot emitters to capture a 3D facial map. Combined with 2D color imagery, and sometimes liveness detection, the bar is raised quite high.

While headlines like to broadcast doom and gloom for biometrics, such as the 2019 BlackHat USA demonstration against Face ID, the truth is these biometrics are really quite secure.

"The attack comes with obvious drawbacks — the victim must be unconscious, for one, and can't wake up when the glasses are placed on their face."

Lindsey O'Donnell, ThreatPost

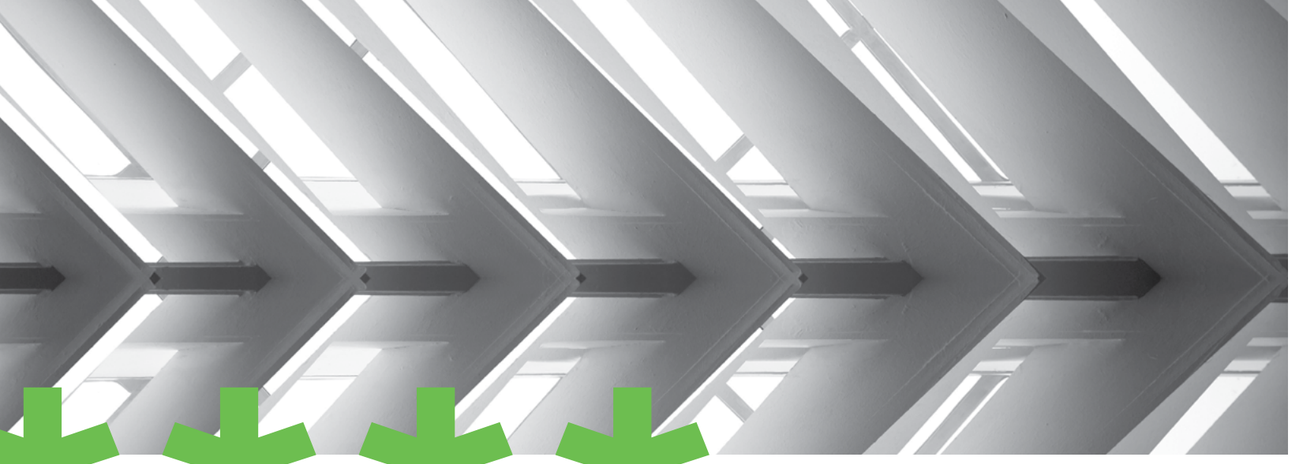
In 2020, Talos did an investigation of fingerprint sensors and their practical spoofability on a reasonable budget. Despite achieving great success rates spoofing most of the devices they tested, they ultimately felt it was a difficult process.

When evaluating the security of biometrics in the context of passwordless authentication, the bar we have to beat is to be stronger than a local (often 6-digit) PIN. A biometric, measured and analyzed locally, inherits the same game-changing properties as the PIN does. It unlocks the unguessable, private credential stored on the authenticator device itself, and avoids sharing a cloneable secret with the web server – so even if it becomes compromised someday, it cannot compromise credentials used on other sites. The biometric can only be attacked locally in analog space, eliminating much of the risk of remote attacks entirely.

"We defined the threat models starting from the collection methods. The creation process is time-consuming and complex. We had to create more than 50 molds and test it manually. It took months. Once we created an accurate mold, the fake fingerprint creation was easy. Today, by using our methodology and our budget it is not possible to create a fingerprint copy on-demand and quickly."

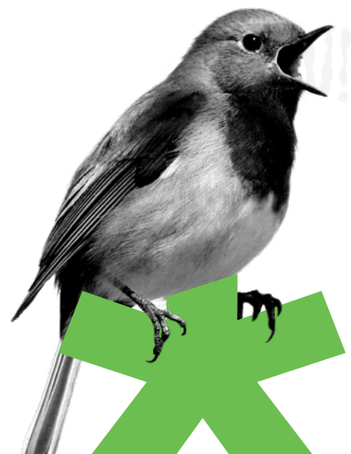
Paul Rascagneres
Security Researcher
Talos Security

Vitor Ventura
Technical Lead/Security Researcher,
Talos Security



MYTH 4

Biometrics Are Secrets



Another point that bears mentioning: Biometrics are also used in an entirely different context than we discuss here. That is, while biometrics can be used for authentication, they can also be used for surveillance.

Luckily, there's a fairly easy way to differentiate between these: whether your biometric information is stored in a centralized database with biometric information of many other people, or kept local to the one device that you used to generate your credential. For instance, biometrics used at border crossings, despite being used to identify users, are checked against a central database rather than a device you carry locally with you, and so fall under the surveillance category.

This distinction is significant for several reasons, both technical and non-technical. Surveillance itself is a thorny topic with both legitimate and illegitimate uses, and the ethical boundaries of surveillance and privacy are an area of significant public debate. This clouds the discussion around the use of biometrics for authentication, which is highly privacy-preserving.

Additionally, the use of central databases risks large-scale biometric leaks, as occurred in the CBP biometric leak (2019), Biostar Leak (2019), OPM Hack (2015), SenseNet (2019), and was feared during ClearView AI's account breach (2020). Biometric data is often considered sensitive or personal information under laws and regulations such as HIPAA, CPRA, and BIPA, with harsh penalties for data leakage, creating even further risk for storing it centrally.

> However, the single most significant distinction between authentication and surveillance is that surveillance relies upon a remote representation of a user's biometric.

To fool a remote biometric check, I must simply submit a digital equivalent to the remote verification engine. A digital representation of a biometric is trivial to replicate and distribute, and is therefore an incredibly weak proof of identity. The original, physical, biometric is very difficult to replicate with sufficient fidelity to pass as the original. By verifying a biometric locally, you gain a high level of assurance in the user's identity. By verifying a biometric remotely, you verify that the user is in possession of a shared secret that is the user's digital biometric.

Biometrics may be sensitive and personally identifiable, but they aren't secrets.

Evaluating a biometric digitally, remotely, turns the biometric into a password that can never be changed and that you wear around on your face all day. In short, remote biometric matching should be considered distinct, separate and vastly inferior to local biometric authentication.

Today, there are really good, easy to use, biometric-based authenticators that achieve the right security properties – and best of all, you may already have many of these in your environment:

- Windows Hello
- Apple Face ID and Touch ID
- Google Face and Fingerprint Unlock
- Yubico Yubikey 5 Bio

This isn't meant to be an all-inclusive list, or to advertise or advocate for any particular product or vendor. Instead, it's meant to illustrate that your users probably already have a FIDO2-capable and secure authenticator in their pocket, and even if they don't have one today, your organization's equipment refresh cycle may supply your users with one or even multiple secure authenticators, simply as a side effect.

MYTH 5

Passwordless is Vulnerable to Phishing

In some ways, the term “passwordless” is a misnomer. Yes, it’s a password-less authentication method, greatly streamlining the login experience, and while that’s a great incentive to use passwordless for logging in, it’s not an improvement in authentication security in and of itself.

> Passwordless uses multiple factors in one step.

Unlocking authenticator devices locally removes the threats of credential reuse and shared secrets. But on top of all of that, passwordless should also raise the bar by substantially reducing or even eliminating the risk of phishing attacks.

Any “passwordless” solution that cannot meet this bar is simply inferior.

That isn’t to say that every password-less solution needs to be phish-proof. There may be other properties of an authentication solution you’re considering that make it a better fit for your environment, and you may be able to mitigate the risk of phishing using additional authentication factors. While not every solution will use the same mechanisms to prevent phishing, there are some properties that will be common to every solution that is truly phish-proof.

To prevent phishing, there are a few general properties that your authentication solution needs:

No Shared Secrets is the property that secrets are never shared and are always kept local to the authenticator device. The authenticator will use these secrets to sign messages, which can be verified by the other party to only have been able to come from the authenticator device. Unlike passwords or other shared secret-based approaches, the solution should guarantee that the secret used for one website is distinct and separate from any secrets used for other websites.

Origin Binding is the property that the site you (as a user) are attempting to log in to must match the domain, or origin, of the site you’re actually on. The history of active phishing has taught us that this is not something that the user can be relied upon to do, so any solution must avoid being dependent on the user checking the domain before authenticating.

Secrets, or credentials, should be linked to the domain upon which they were registered, and should not be unlockable without an automated check that the user is actually on that page. From our first No Shared Secrets property, we should be guaranteed to have different credentials for different sites, and so while a phishing site should be able to gain access to credentials for its own domain, it must never be able to access credentials for another site.

Channel Binding is the property that the communication channel from the authenticator to the website must be strongly tied to the browser session attempting to authenticate. Put another way, an attacker attempting to log in as the victim should be unable to reach the user’s authenticator to prompt the user to log in. Doing anything else would make push phishing attacks viable. There must be a guarantee that only the user’s browser (or other legitimate software) can activate the authenticator device. The channel between the browser and authenticator must be bound.

Learn More

Read the full *Administrator’s Guide to Passwordless*

DUO.SC/ADMINSGUIDE

Want to test it out before you buy? Try Duo for free using our 30-day trial and get used to being secure from anywhere at any time.

SIGNUP.DUO.COM


:"false"
=(n||"fx"
&&(i=n.sh
Passwor
DUO
cisco SECURE