https://duo.com/blog/the-multi-factor-factor-or-how-to-manage-authentication-risk

**The Multi-Factor Factor (or How to Manage Authentication Risk)**

As we debate the necessity of various authentication factors, particularly for passwordless projects, it’s good to take a step back and remember how we got here. There are key three types of authentication:

**The 3 Key Types of Authentication**

**1. “Something you know,”**otherwise known as a **“shared secret.”**This used to be something you memorized, but it turns out that fallible organic storage is not that great for storing complex character strings that now number in the hundreds (you ARE using unique passwords for every account, right? … Right?).

**2. “Something you have,”**meaning something that can’t be possessed by more than one entity at a time. This could be something that is too difficult to copy or generate independently, that is tied to storage and can’t be removed, or that exists as a unique physical item (such as a hard token or a key).

**3. “Something you are,”** referring to an attribute that is physically unique to an individual, such as a fingerprint, a palmprint, a retinal pattern, a gait, a typing pattern, or even a heartbeat.

**Each of these factors comes with a downside:**

***“Something you know” = “Something you forgot,” or “Something that someone beat out of you.”***

**A shared secret that is guessed or derived  … is not a secret any more.** Worse yet, it can be silently stolen without anyone noticing. But it’s also the cheapest factor, in the sense that it can be created, changed, expanded, distributed and used without having to buy any extra technology.

If you need to identify someone more definitively, you ask them for information they’re not likely to forget, such as the name of the street they grew up on. But any of that historical information is increasingly available on the Internet, or can be tricked out of the user through phishing or social media “quizzes.”

**Another downside to “something you know”**is that it may appear to be cheap in terms of technology, but in terms of support cost — help desk time when someone forgets a username or password, or can’t log in for another reason — it can be more expensive than a better-designed factor that is harder to get wrong.

**This is why we’re working on the journey to a [passwordless future.](https://duo.com/resources/ebooks/passwordless-the-future-of-authentication" \t "_blank)**

***“Something you have” = “Something you lost,” or “Something you broke.”***

One of the biggest threats today is SIM theft, in which an attacker manages to steal an assigned mobile phone number so that they can receive SMS authentication codes. This is nefarious because once again, it can be stolen silently; the victim still has the physical phone but may not realize that the number has been assigned to someone else until it’s too late.

Hard tokens that generate codes can run out their batteries in a few years; they’re also unwieldy to carry around if you have several of them for different accounts. Generally speaking, if a user loses the “something you have,” the fallback is “something you know,” which we’ve just discussed above.

***“Something you are” = “Something that aged”***

At least in my case; [gait analysis](https://en.wikipedia.org/wiki/Gait_analysis) for me would lose its baseline every time I had an arthritis flare-up. The other problem with biometrics is that you can’t change your retinal patterns or fingerprints if the records of them are stolen.

Covid has revealed some problems with [biometrics](https://duo.com/blog/new-duo-labs-security-report-on-passwordless-biometrics-and-sensors). For example: If you’re wearing a mask, FaceID doesn’t work; shared fingerprint readers aren’t sanitary these days. But biometrics are extremely convenient as a factor because you can’t forget them, you can’t leave them behind in the taxi, and chances are good that nobody can steal the originals without you noticing (water glasses in spy movies aside).

**But what risks are these authentication factors actually trying to address? Let’s list some out.**

**Risks of Authentication**

1. **Someone is trying to log in at the user’s machine with the real user’s username and password.**
2. **The real user walked away from their unlocked machine and now an attacker is trying to use it.**
3. **Someone is remotely connected to the user’s machine and is trying to pretend to be the user sitting at that machine.**
4. **Someone is trying to log in with the real user’s username and password from a different system (such as a compromised machine in a botnet).**
5. **The real user is trying to log in, but the machine is compromised and could be used to steal the username and password, or plant malware.**
6. **The real user is trying to log in from one location, but someone else is also trying to log in as that user from a different location.**
7. **Someone has gained access to the real user’s username, password, and second factor (such as a hard token or phone number for receiving SMS texts), and is trying to log in from a different device.**
8. **Someone is listening in on the network stream and trying to hijack the user’s session in progress.**

When we do threat modeling, we come up with these sorts of attacks and more. CISOs often run through a whole laundry list of possible attacks in their head whenever they’re looking at a new proposal. Then they have to pick the controls that address as many of the risks as possible. For example:

**Controls to Authentication Risks**

[A 2FA factor](https://www.duo.com/) that is physically separate from a user’s laptop would protect against 1), 2), 3), 4), and 6 listed in the previous section) — assuming that the user has that factor with them and doesn’t leave it near the laptop.

A session timeout, requiring reauthentication, is often used to protect against 2), 3), and to some extent 8).

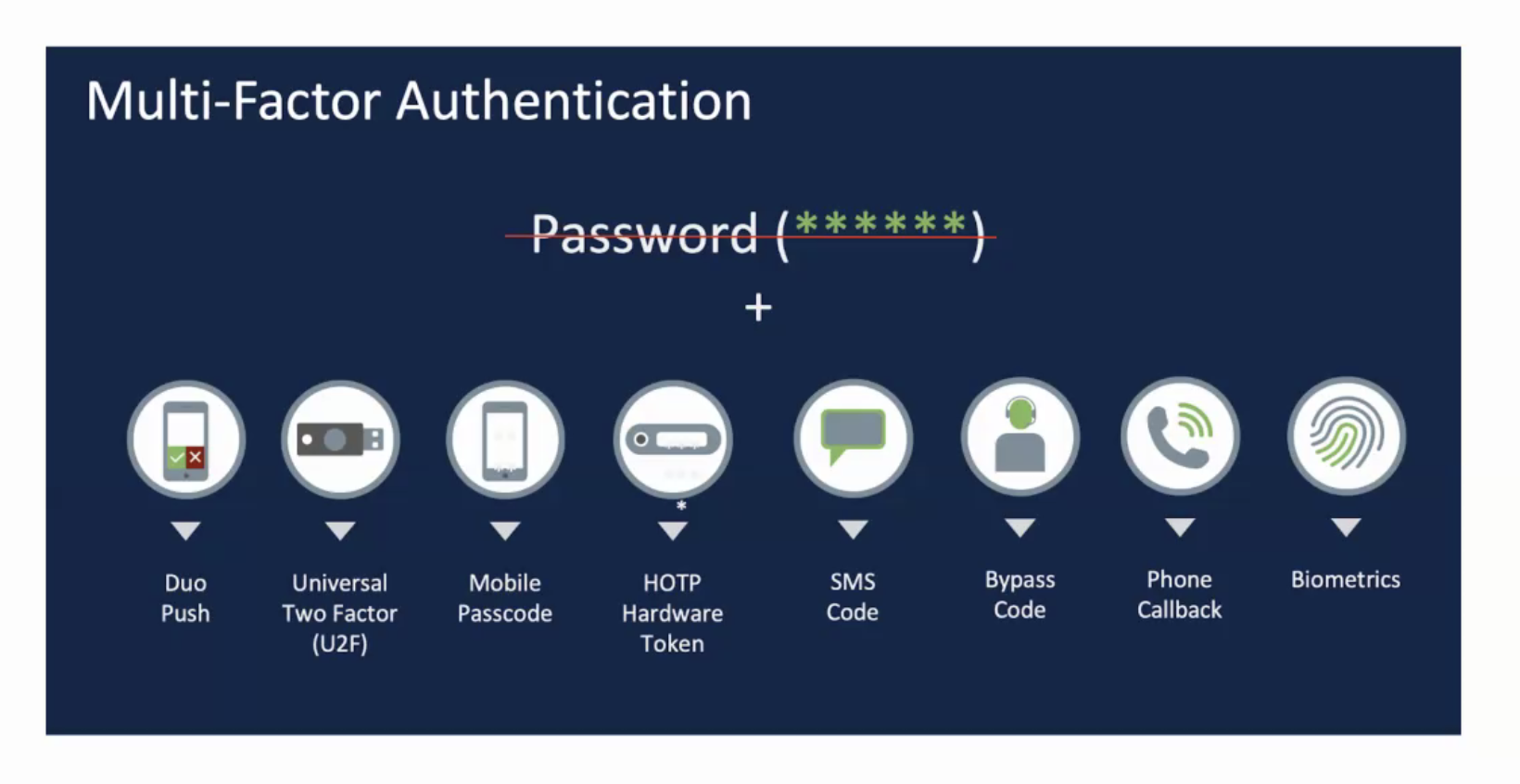
Marking a [laptop as trusted](https://duo.com/product/device-trust), bound specifically to the user, is used to prevent 4), 6), and 7).

Ensuring that the network connection is encrypted all the way between the user and the application protects against 8).

Using a [biometric for authentication](https://duo.com/product/device-trust) is intended to protect against 1), 2), 3), 4), 6), and 7), but that’s assuming that the user isn’t under duress (being forced by an attacker to supply it).

Checking the user’s [device for security state](https://duo.com/product/adaptive-access-policies)and any evidence of compromise is meant to protect against 2), 3), and 5).

Using a second factor such as a [U2F key](https://duo.com/product/multi-factor-authentication-mfa/authentication-methods/u2f-and-biometrics), that requires a physical response from the user to activate, also protects against 3) and 5) -- it proves that the user is actually present and intends to authenticate.



**Set Policy Controls As Guardrails**

For added protection [set policy controls](https://duo.com/product/adaptive-access-policies), using other factors, as guardrails. Factors such as location (either by GPS or IP address) can help to narrow down the vectors of attack if, for example, you never expect a user to try to authenticate from anyplace other than a certain network or geographic region. But we know that IP addresses aren’t foolproof — all you have to do is gain access to a system on the “right” network.  So these can’t be the sole authentication factors to rely on. Think of these more as a narrowing function: you are blocking more attacks right from the outset, leaving fewer to sift through and validate.

**Conclusion**

As you can see, there are layers upon layers of defense that you can build to try to address the most common risk scenarios. But you also have to take into account the downsides of each factor when designing the solution.

If you have an endlessly changing roster of 30 people using the same point of sale system, you can’t register a biometric or phone app for each of them, make each of them log in and out of accounts if they are rushing to serve a line of customers, or make them all share a hard token. The modern enterprise ends up with a portfolio of factors, deployed where they work the best and where they address the right risks.

We’ve learned a lot this year about assumptions we made when choosing the original authentication factors for an organization — factors that stopped working so well when we became physically separated from other people. As we make plans for the future state of authentication, it helps to go back to first principles and update the above lists for a flexible outcome.