Attestation is essentially a certificate that verifies that the authenticator being used is from a trusted source.

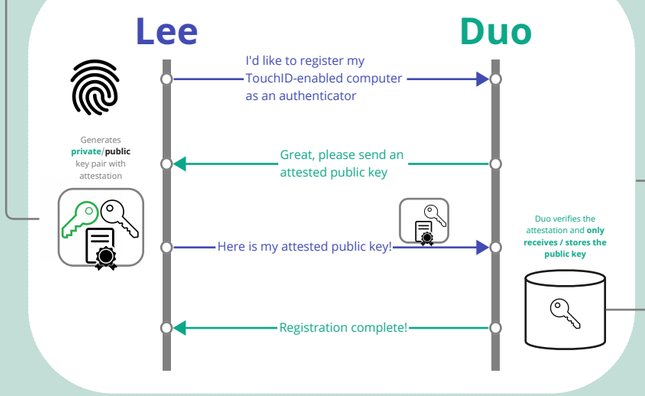
This means that the authenticator says "I am using TouchID by Apple, and here is a certificate to prove it". Duo then verifies this certificate.

Attestation requires trust of the parties implementing the authenticator, and limits the user to only "trusted" authenticator implementations, such as Apple TouchID/FaceID, Windows Hello, and Yubico

WebAuthn and Why it Works

Three things must be true for an authentication method to be "unphishable". It must have **no shared secrets**, and it must enforce both **origin binding and channel binding.**

Registration



Lee first will need to register their device as a WebAuthn Authenticator.

This involves generating a public/private key pair and providing the public key to Duo.

"No shared secrets" is inherent to the design of WebAuthn.

The authenticator generates a keypair per-service, and Duo only stores the public key.

If Duo were breached, the public keys wouldn't provide any use to an attacker.

Origin Binding is achieved because the *browser*, not the site, sends the origin to the authenticator.

The authenticator will only sign the payload if the origin matches the origin to which that authenticator was initially registered.

Channel Binding is achieved because the authenticator is generally tied to Lee's physical device.

It would require significant privileges on Lee's device for an attacker to invoke the authenticator, which prevents push "phishing" in this case

Note that **origin binding** is only maintained if the customer is protecting applications with Universal Prompt. This is because the old prompt is an iframe, which is essentially an embedded webpage of Duo's actual login.

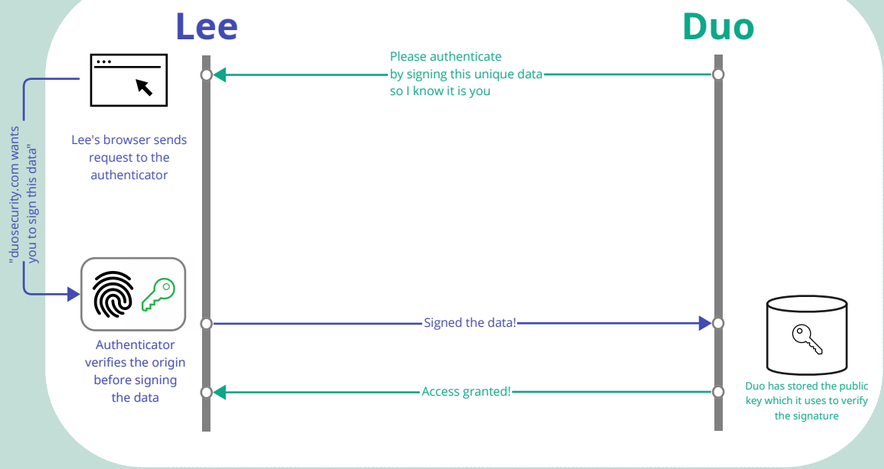
This means that any request from the iframe, proxied through the attacker, will still appear to the authenticator as being Duo, not the attacker.

Aside - **WebAuthn alone is still technically MFA** in most cases.

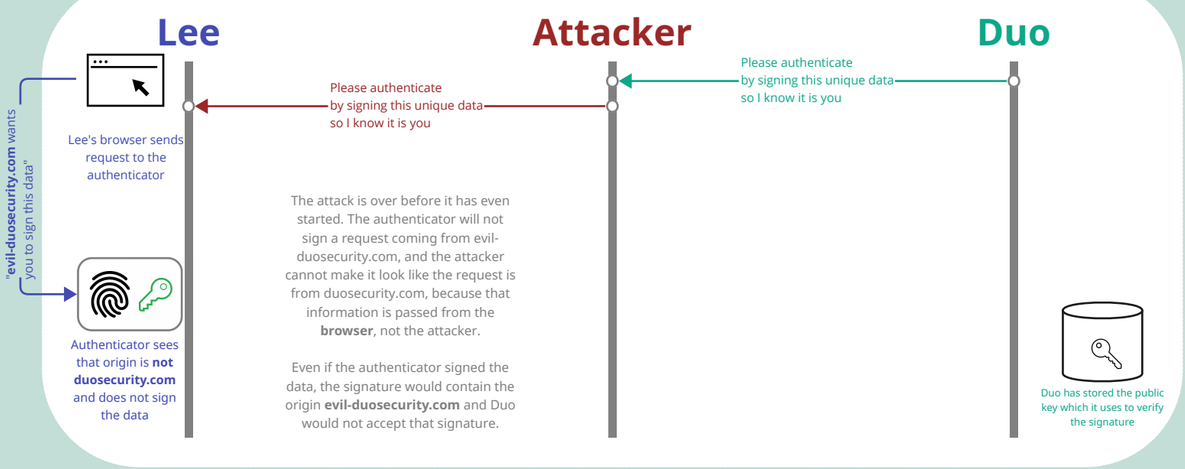
The two factors are

1. Something you have - your private key, which is used to sign the challenge sent from Duo
2. Something you are / know - your biometric or PIN which "unlocks" the authenticator. The validity of this factor is ensured via attestation.

In a normal auth...



In an attack...



Aside: Properties of "Unphishable" Authentication in WebAuthn

No shared secrets means that the secret used to authenticate is unique to the authenticator, and is registered to only one application.

It is shared with no one - not even the verifying service (Duo)!

Duo only maintains the public key, which cannot be used to impersonate a user.

Origin binding means that an authenticator will only verify a user if the origin of the request to authenticate *matches* the origin of the service for which the authenticator was set up.

In other words, if an authenticator is registered with duosecurity.com, evil-duosecurity.com cannot tell that authenticator to verify a user.

Channel binding means that an attacker is unable to prompt a user's authenticator, because the authenticator is strongly tied to the channel, being the user's browser.

Only the browser on the user's machine can prompt the authenticator to verify a user, making the authenticator resistant to "push phishing"

In an attack with the *old Duo Prompt*...