WebAuthn: How passwordless authentication works

Casaba  |  Slater Weinstock
What is WebAuthn?

- Known as the Web Authentication API
- Spec written by W3C and FIDO Alliance
- Allows integration into authentication mechanisms available in devices, bypassing the need for a password
  - Public/private key pair
Brief overview of public/private key cryptography

• Relies on a public/private keypair
• Data encrypted with a public key can only be decrypted with the corresponding private key
• Relies on very long numbers which have a mathematical relationship
How does password-based authentication work?

• The common flow when using password-based authentication
  1. Create a password
  2. The password is hashed and salted and then sent up to the server
  3. If the same value is ever produced in the future, you're authenticated into the system
Why is this a problem?

• Ultimately, the server is responsible for storing this password derivation
  – This makes the server a target for attackers
• In addition to the server being a target, other issues include:
  – Password reuse
  – Weak passwords
  – Credential leaks
  – Phishing
How does WebAuthn address this?

- In the case of WebAuthn, the server only holds the public keys.
- As an attacker, this makes it an uninteresting target, as public keys are meant to be public.
- Without the need to enter a password directly, phishing is also less likely.
WebAuthn Registration Ceremony

Figure 1 Registration Flow

https://w3c.github.io/webauthn/
WebAuthn Authentication Ceremony

**Figure 2 Authentication Flow**

https://w3c.github.io/webauthn/
Potential Attack Vector

- Let's say there's attacker.com and example.com and the attacker knows the ID of a key for example.com
- Could you request a signature with the key from example.com over the attacker.com domain?
  - No, because during the WebAuthn request, you must set the relying party ID, which is essentially a domain name. You couldn't claim example.com if you're attacker.com
  - Essentially, the credential ID is useless if you can't assert the exact relying party ID that it was registered with
  - In addition, the exact origin is also returned, which means we know what actual origin was used and this can be validated against the expected origin
Example

- https://demo.yubico.com/webauthn-technical/registration
Connection between authenticator and client

- Relying Party (RP)
- Client/Browser
- Authenticator

Connections:
- From Relying Party (RP) to Client/Browser: WebAuthn
- From Client/Browser to Authenticator:
  - U2F/CTAP1
  - Or
  - CTAP2
Passkeys

- Passkeys are an extension of this, and it's enabling a phone to be an authenticator.
- So effectively, we are replacing security keys with the phones.
- This solves the need of people having to buy loads of security keys.
- Basically, passkeys are WebAuthn credentials that are backed up.
• Start with scanning a QR code
• Begins talking to the cloud
• Phone broadcasts BLE advertisement
• Noise handshake
Noise handshake in the context of Passkeys

- Based on Diffie-Hellman
- Parties exchange DH public keys and perform a series of operations, resulting in a shared secret key
- This handshake pattern may either be NK or KN.
- The handshake pattern consists of:
  - A pre-message pattern for the initiator
  - A pre-message pattern for the responder
  - A sequence of message patterns
- First letter is the initiator's static key, second letter is responder's static key
- In the context of NK
  - N means NO static key for the initiator
  - K means the static key for the responder is known to the initiator
• NKpsk0

← s

...

→ psk,e,es

← e,ee
What is the goal of this?

• The laptop has to prove that it has knowledge of the private key whose public key was in the QR code.
• It also has to prove the PSK.
• Ultimately, this is proving proximity.
Summary of authenticator to client communication

- Phone communicates with the cloud
- Laptop communicates with the cloud
- A tunnel is established between them
Passkeys vs Passwords

- Passkeys allow you to avoid using a typable string
- Passkeys are generated securely on the device
- Storage of the public key on the server in place of passwords makes the server not a target
- Passkeys provide a strong claim that the devices are in close physical proximity to each other
  - This means that a QR code sent via a phishing email or a QR code on a fake website, the attacker can't receive the BLE advert
- Additionally, this process occurs only between the client/browser and the authenticator. The website is never involved during the communication
Careers in Cybersecurity
Thank You

Slater Weinstock
slater@casaba.com
Slide 2:
• https://webauthn.io/
• https://webauthn.guide/#about-webauthn
• https://demo.yubico.com/webauthn-technical/registration

Slide 3:

Slide 4:

Slide 5:
• https://webauthn.guide/

Slide 6:
• "Security. Cryptography. Whatever." is hosted by Deirdre Connolly, Thomas Ptacek, and David Adrian. - Passkeys episode
References

Slide 7:
- https://curity.io/resources/learn/webauthn-overview/
- https://w3c.github.io/webauthn/
- https://www.w3.org/TR/webauthn/#registering-a-new-credential

Slide 8:
- https://curity.io/resources/learn/webauthn-overview/
- https://w3c.github.io/webauthn/
- https://www.w3.org/TR/webauthn/#registering-a-new-credential
- "Security. Cryptography. Whatever." is hosted by Deirdre Connolly, Thomas Ptacek, and David Adrian. - Passkeys episode

Slide 9:
"Security. Cryptography. Whatever." is hosted by Deirdre Connolly, Thomas Ptacek, and David Adrian. - Passkeys episode

Slide 10:
- https://demo.yubico.com/webauthn-technical/registration
References

Slide 11:
• [https://developers.yubico.com/WebAuthn/](https://developers.yubico.com/WebAuthn/)
• "Security. Cryptography. Whatever." is hosted by Deirdre Connolly, Thomas Ptacek, and David Adrian. - Passkeys episode

Slide 12:
• "Security. Cryptography. Whatever." is hosted by Deirdre Connolly, Thomas Ptacek, and David Adrian. - Passkeys episode
• [https://www.imperialviolet.org/2022/07/04/passkeys.html](https://www.imperialviolet.org/2022/07/04/passkeys.html)

Slide 13:
• "Security. Cryptography. Whatever." is hosted by Deirdre Connolly, Thomas Ptacek, and David Adrian. - Passkeys episode
• [https://www.imperialviolet.org/2022/07/04/passkeys.html](https://www.imperialviolet.org/2022/07/04/passkeys.html)
References

Slide 14:
- [https://noiseprotocol.org/noise.html](https://noiseprotocol.org/noise.html)
- [https://www.imperialviolet.org/2022/07/04/passkeys.html](https://www.imperialviolet.org/2022/07/04/passkeys.html)

Slide 15:
- [https://noiseprotocol.org/noise.html](https://noiseprotocol.org/noise.html)
- [https://www.imperialviolet.org/2022/07/04/passkeys.html](https://www.imperialviolet.org/2022/07/04/passkeys.html)
- [https://noiseprotocol.org/noise.html#interactive-handshake-patterns-fundamental](https://noiseprotocol.org/noise.html#interactive-handshake-patterns-fundamental)

Slide 16:
- "Security. Cryptography. Whatever." is hosted by Deirdre Connolly, Thomas Ptacek, and David Adrian. - Passkeys episode
- [https://www.imperialviolet.org/2022/07/04/passkeys.html](https://www.imperialviolet.org/2022/07/04/passkeys.html)
References

Slide 17:
• "Security. Cryptography. Whatever." is hosted by Deirdre Connolly, Thomas Ptacek, and David Adrian. - Passkeys episode
• https://www.imperialviolet.org/2022/07/04/passkeys.html

Slide 18:
• "Security. Cryptography. Whatever." is hosted by Deirdre Connolly, Thomas Ptacek, and David Adrian. - Passkeys episode