Get Rid of Passwords With This One Weird Trick

An Introduction to Web Authentication

DUO LABS

Nick Steele

Senior R&D Engineer

@codekaiju

James Barclay

Senior R&D Engineer

@futureimperfect

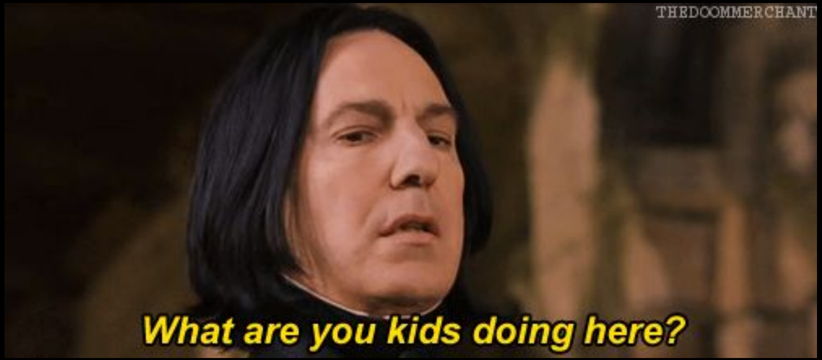
DUO LABS

What are we talking about?

- Moving past passwords
- Why it’s important
- Passwordless Authentication on the Web
- How we’re doing it

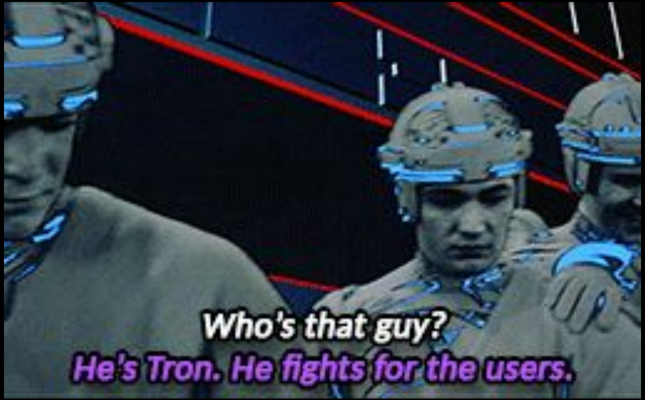
Why are we talking about this?

- We’re **Duo Labs**
  - We’re the research group at **Duo Security**, now part of **Cisco**
  - Strong authentication on the internet is a hard problem
  - We research hard problems!
- We believe that the WebAuthn spec is a good solution to passwordless authentication
- Solving this problem helps pretty much everyone



Democratization of Security Is Key

- A rising tide lifts all ships
- Solving big security issues together rather than apart
  - Strengthens our community
  - Keeps us honest
- Focus should always be on helping the most users
- Be like Tron



A Brief History

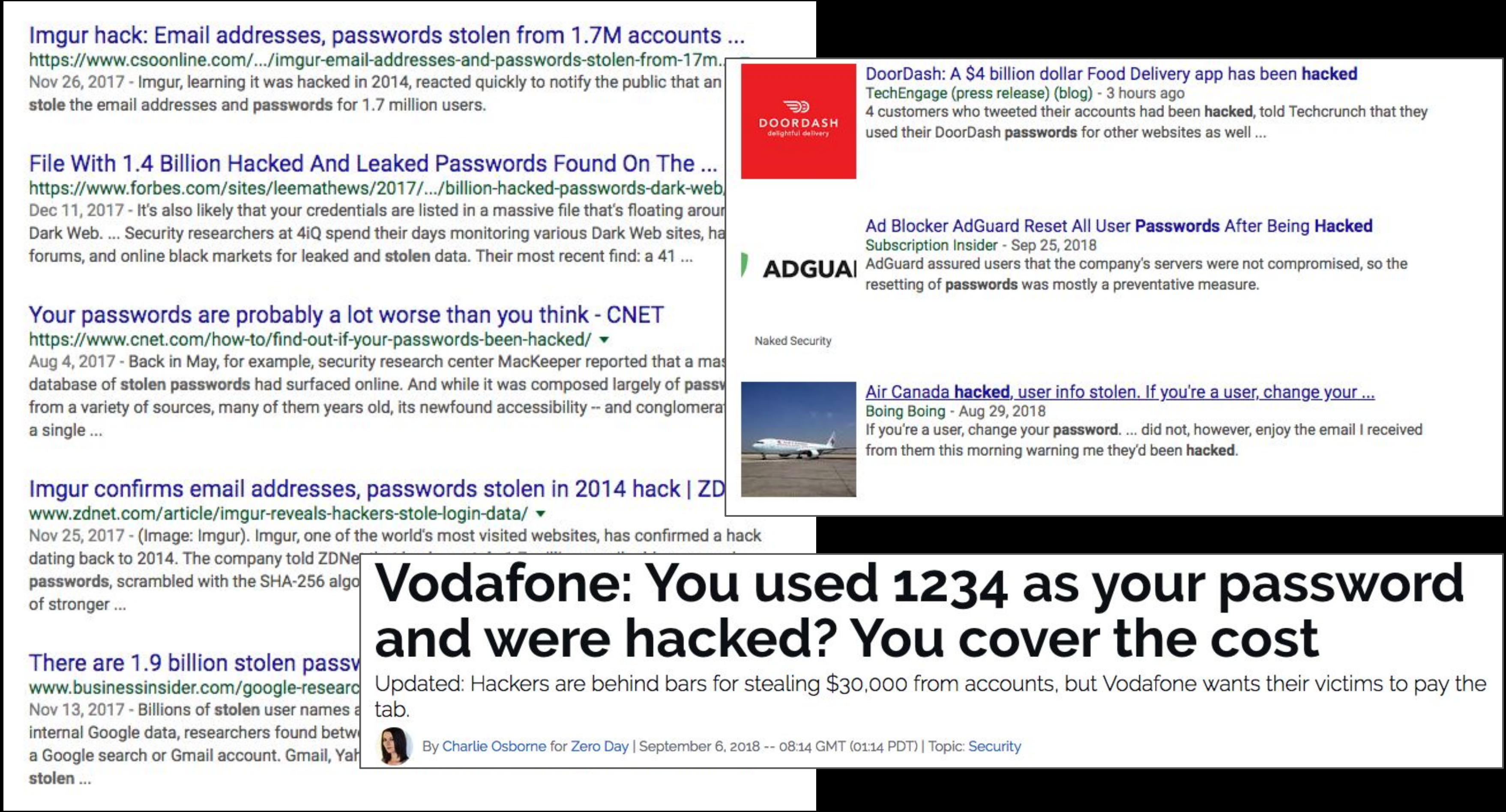
“In the beginning the password was created. This has made a lot of people very angry and been widely regarded as a bad move.”

- Douglas Adams, sorta

81% of breaches leverage either stolen and/or weak passwords.

Source: [2017 Verizon Data Breach Investigations Report]

DUO LABS



Imgur hack: Email addresses, passwords stolen from 1.7M accounts ...
https://www.csoonline.com/.../imgur-email-addresses-and-passwords-stolen-from-17m...
Nov 26, 2017 - Imgur, learning it was hacked in 2014, reacted quickly to notify the public that an
stole the email addresses and **passwords** for 1.7 million users.

File With 1.4 Billion Hacked And Leaked Passwords Found On The ...
https://www.forbes.com/sites/leemathews/2017/.../billion-hacked-passwords-dark-web/
Dec 11, 2017 - It's also likely that your credentials are listed in a massive file that's floating arour
Dark Web. ... Security researchers at 4iQ spend their days monitoring various Dark Web sites, ha
forums, and online black markets for leaked and **stolen** data. Their most recent find: a 41 ...

Your passwords are probably a lot worse than you think - CNET
https://www.cnet.com/how-to/find-out-if-your-passwords-been-hacked/ ▾
Aug 4, 2017 - Back in May, for example, security research center MacKeeper reported that a mas
database of **stolen passwords** had surfaced online. And while it was composed largely of **passw**
from a variety of sources, many of them years old, its newfound accessibility -- and conglomerat
a single ...

Imgur confirms email addresses, passwords stolen in 2014 hack | ZD
www.zdnet.com/article/imgur-reveals-hackers-stole-login-data/ ▾
Nov 25, 2017 - (Image: Imgur). Imgur, one of the world's most visited websites, has confirmed a hack
dating back to 2014. The company told ZDNe
passwords, scrambled with the SHA-256 algo
of stronger ...

There are 1.9 billion stolen passw
www.businessinsider.com/google-researc
Nov 13, 2017 - Billions of **stolen** user names a
internal Google data, researchers found betw
a Google search or Gmail account. Gmail, Yah
stolen ...

DoorDash: A $4 billion dollar Food Delivery app has been **hacked**
TechEngage (press release) (blog) - 3 hours ago
4 customers who tweeted their accounts had been **hacked**, told Techcrunch that they used their DoorDash **passwords** for other websites as well ...

Ad Blocker AdGuard Reset All User **Passwords** After Being **Hacked**
Subscription Insider - Sep 25, 2018
AdGuard assured users that the company's servers were not compromised, so the resetting of **passwords** was mostly a preventative measure.

Naked Security

Air Canada **hacked**, user info stolen. If you're a user, change your ...
Boing Boing - Aug 29, 2018
If you're a user, change your **password**. ... did not, however, enjoy the email I received from them this morning warning me they'd been **hacked**.

Vodafone: You used 1234 as your password and were hacked? You cover the cost

Updated: Hackers are behind bars for stealing $30,000 from accounts, but Vodafone wants their victims to pay the tab.

By Charlie Osborne for Zero Day | September 6, 2018 -- 08:14 GMT (01:14 PDT) | Topic: Security

ALL YOUR FAULT!

“Kind of a nightmare…”

- The guy who invented it

“Passwords Suck”

- Most People

“Pas uck”

- Most Peop

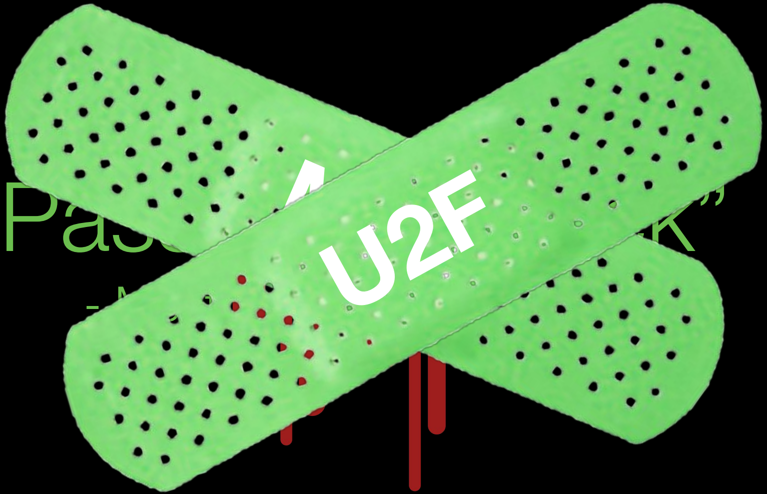
Multi Factor Authentication

- Better than only first factor, but…
  - User experience *can* be cumbersome (except Duo :)
  - SMS OTP codes can be intercepted
  - HOTP and TOTP seeds can be intercepted
  - Not phish-proof

“Pas [illegible] ck”

- Most Pe [illegible]

“Pas k”



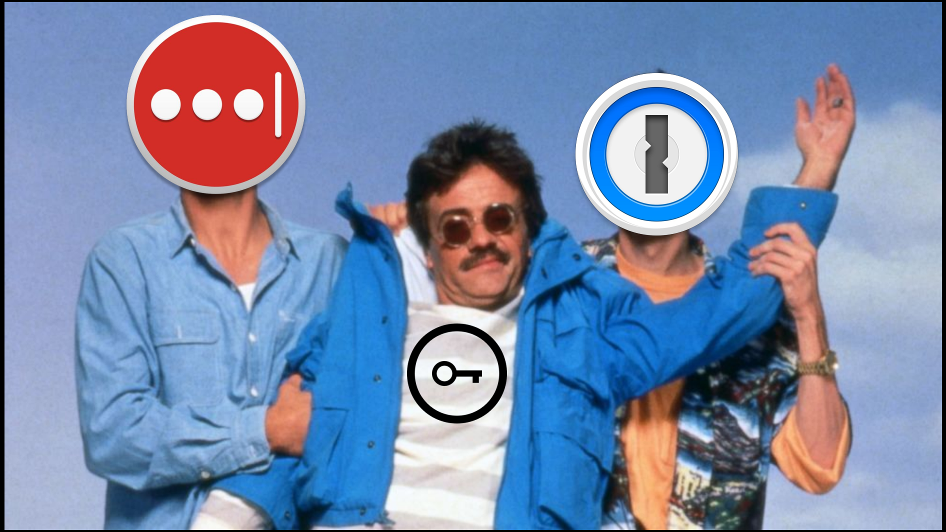
Universal Second Factor

- Better than only first factor and traditional MFA but…
  - Requires physical token (usually)
  - Tokens can be expensive ($19 and up)
  - Hard to use (if even possible) on mobile devices
  - Isn't supported natively in most browsers
    - Not really universal…
  - Hard to convince people to use it casually

“Pas
U2F
We did it Patrick! We saved
PASSWORDS

“The average… user has over 107 accounts registered to one email address… In 2020, the average number of accounts per internet user will be 207”

- Dashlane, 2015



Meanwhile… in the year 2015

- Phones are becoming smarter
    - Most have a built-in security module, like a TEE or SEP
    - Biometric authentication is common on these devices
    - 77% of Americans own a smartphone in 2017 (68% in 2015)
- FIDO drafts Universal Authentication Factor spec
    - Spec describes a method for authenticating users via client devices to online services using key pairs created by the client, (and authorized by the user via a biometric or PIN)
    - Not a lot of traction, but paved the way for…

Web Authentication

Web Authentication

WebAuthn

WebAuthn

- A W3C spec started in 2016
- Includes contributors from Google, Mozilla, Microsoft…
- Currently supported in Chrome, Edge, and Firefox
- But what is it?

WebAuthn is…

“...an API enabling the creation and use of strong, attested, scoped, public key-based **credentials** by web applications, for the purpose of strongly authenticating users.”

WebAuthn

“...[with WebAuthn] one or more public key credentials, each scoped to a given **Relying Party**, are created and stored on an **authenticator** by the user agent in conjunction with the web application.”

Credentials

Strong

Attested

Scoped

Credentials

Strong

Attested

Scoped

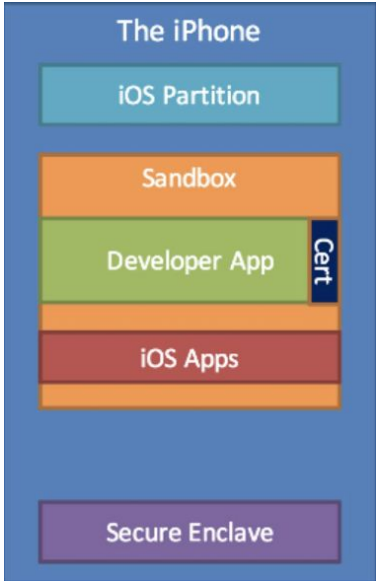
DUO LABS

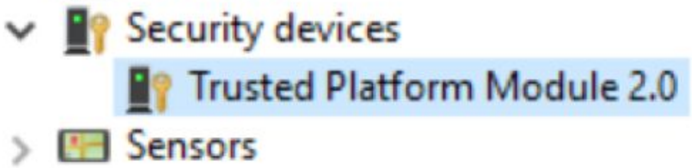
p@ssw0rd

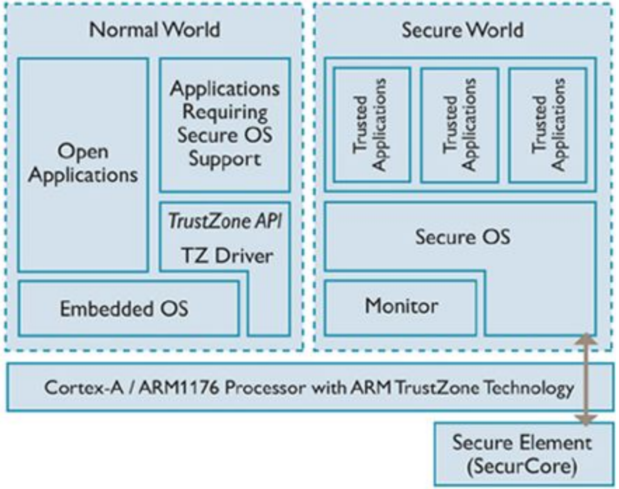
Passwords Have Problems

1. Passwords are **pre-shared keys**
2. Passwords are **difficult to remember**
3. Passwords can be **stolen**
4. Passwords can be (and are) **re-used**
5. Passwords are **difficult to secure** for developers

WebAuthn Credentials Are Strong




Security devices
Trusted Platform Module 2.0
Sensors

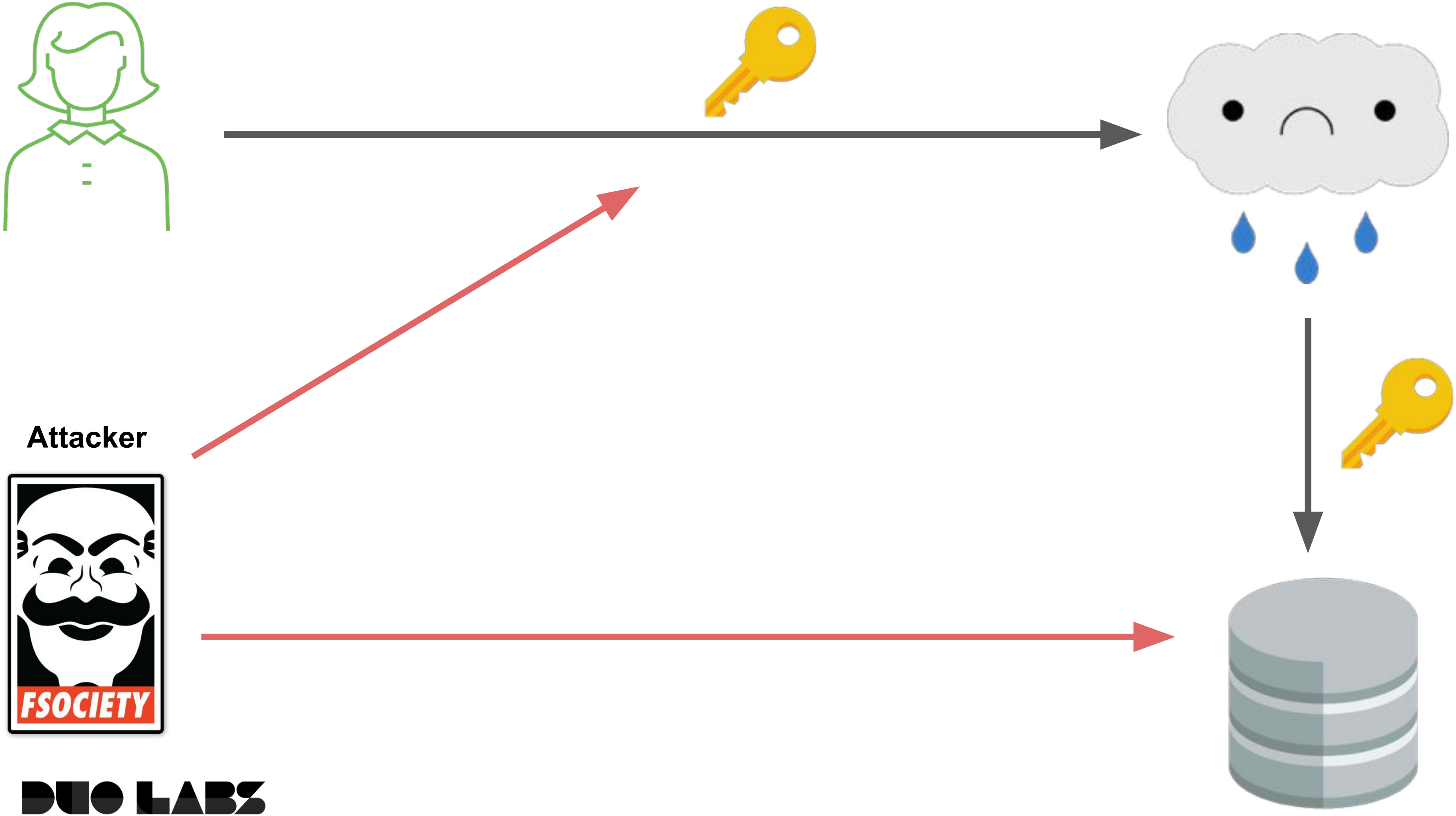


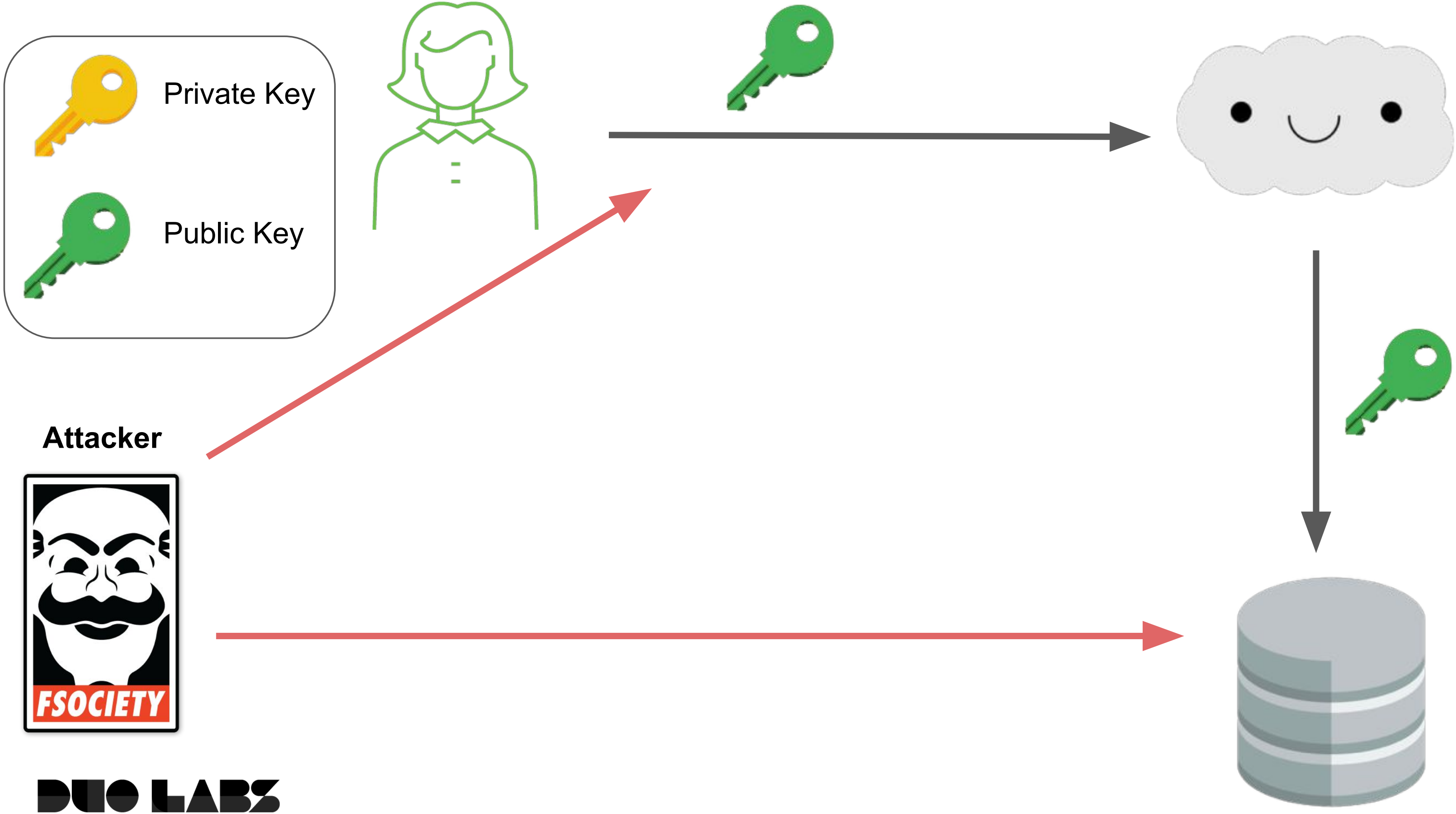
WebAuthn Credentials Are Strong

- Unlike passwords or passphrases, WebAuthn uses **public-key cryptography** rather than **pre-shared keys**

- With **user verifying** WebAuthn authenticators, signing operations are authorized by the user via something they know (PIN), or something they are (biometric)

- With **non-user verifying** WebAuthn authenticators, signing operations are authorized by proof of **user-presence**


Attacker
FSOCIETY
DUO LABS



Private Key

Public Key

Attacker

DUO LABS

Credentials

Strong

Attested

Scoped

DUO LABS

Attestation is a way to cryptographically **prove** that a key pair came from an authenticator we **trust**.

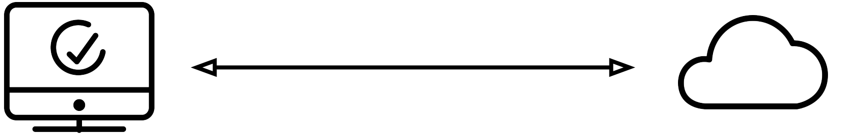
Credentials

Strong

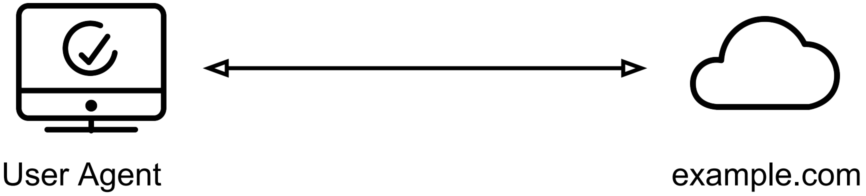
Attested

Scoped

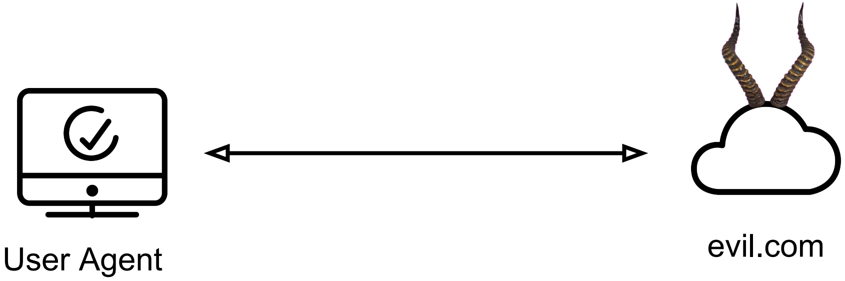
“Give me the credential for **example.com.**”



“I see you’re **example.com**, so here it is.”



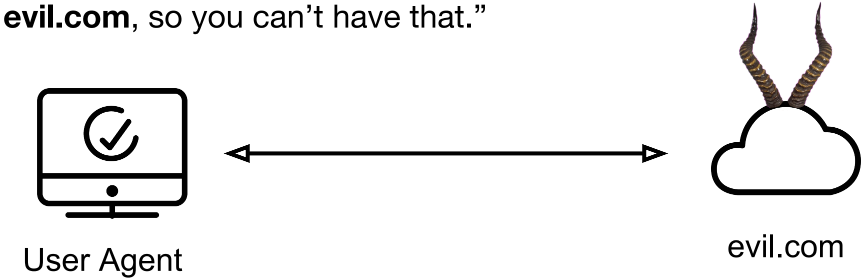
“Give me the credential for **example.com**”



User Agent

evil.com

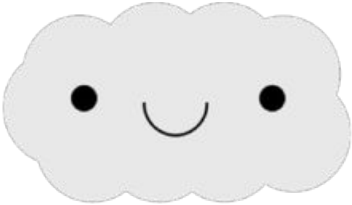
“I see you’re **evil.com**, so you can’t have that.”



Who Would Win?
A Password or One Credential Boi?

Credential Type	Strong?	Attested?	Scoped?
Password	**Maybe**	**No**	**Maybe**
WebAuthn	**Yes**	**Yes**	**Yes**

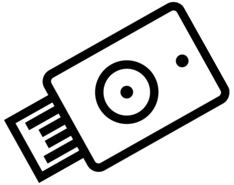
Relying Party



- AKA the website the user is authenticating to
- Credentials for the Relying Party are bound by origin (scoped)
  - Possible to use for subdomains (`sub.example.com)` when the credential is scoped to the domain (*example.com*)
    - The reverse is not true
- Cannot talk directly to the authenticator or (by default) identify the authenticator
  - This prevents tracking of the user via the authenticator
- A breach of the Relying Party's credential database would leak the **credential public key** and **credential ID**, not the **credential private key**

Authenticators

- Capable of creating and storing and strong credentials
- Authenticators can require biometric or PIN to use the credential
- U2F tokens can also be used, like Yubikeys and Feitian keys



- These devices require interaction by the user
- Communicates to the the User Agent, using Client to Authenticator Protocol
- Can provide proof that it created the credential, via authenticator attestation

Glossary

Credential Key Pair:
The private/public keys used for authenticating.

User Agent:
Software that acts on behalf of the user, (browser).

Other WebAuthn Terminology

- Credential ID (Public Key ID)
  - Can also be wrapped private key

- WebAuthn Ceremonies (or Functions)
  - Registration
  - Assertion (Login)

- Authorization and Authentication
  - Authentication - Identifying the user
  - Authorization - Access rights of the user

WebAuthn

- Allows websites and users to have a unique credential between them
- The authenticator can be a biometric device, identifying the user
- The user **must** interact with their authenticator to release the credential
- The authenticator gives us proof that it created the credential

Why Is WebAuthn Important?

- Eliminates the need for user created passwords
- Raises the bar for security on the internet
    - The weakest WebAuthn credential is stronger than the stronger password
    - A credential cannot be easily phished from the user
    - A public key stolen from the Relying Party is ineffective
- Lowers the barrier to entry
    - Uses hardware commonly available to users (a smartphone or laptop)
    - Means users don’t need to buy any extra hardware

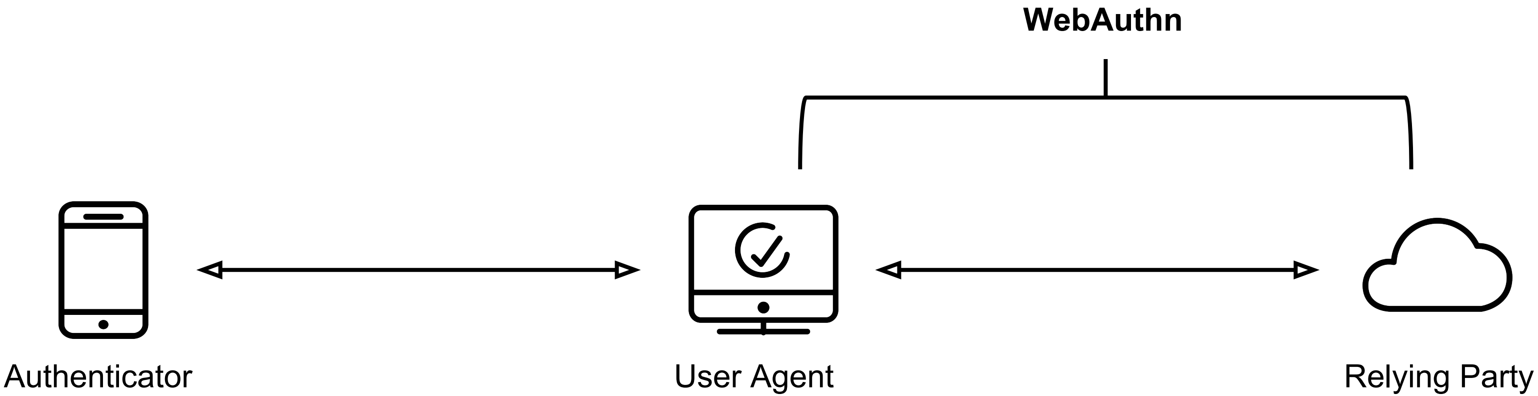
QUICK DEMO HERE

FIDO2

- In March the FIDO Alliance introduced “**The FIDO2 Framework**”
  - **WebAuthn** + **CTAP2** together

- FIDO2 covers the full spectrum
  - Client (User Agent) <--> Authenticator
  - Client (User Agent) <--> Relying Party

- Can be confusing, so when you hear **FIDO2** just remember that it encompasses **WebAuthn** as well

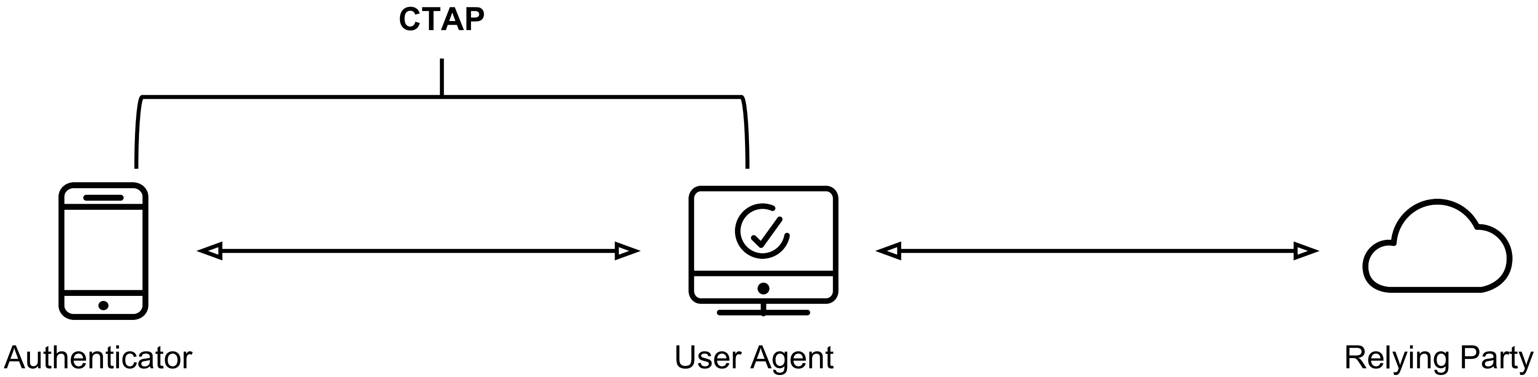


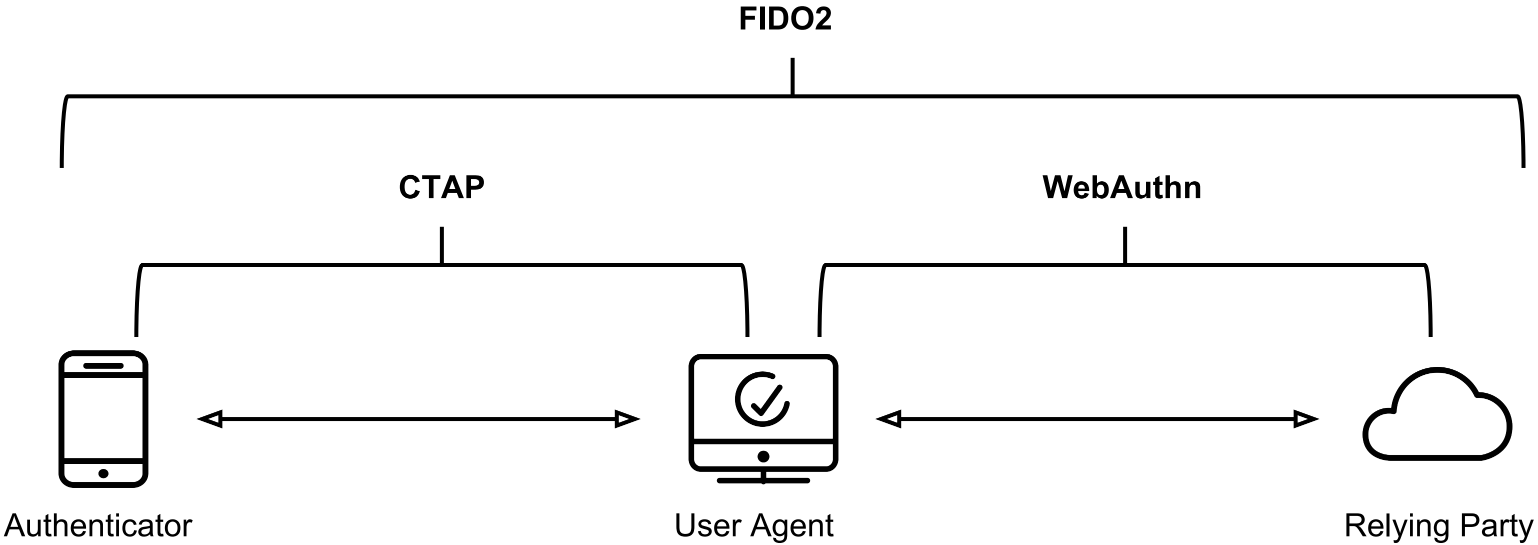
WebAuthn

Authenticator

User Agent

Relying Party


CTAP
Authenticator
User Agent
Relying Party



FIDO2

CTAP

WebAuthn

Authenticator

User Agent

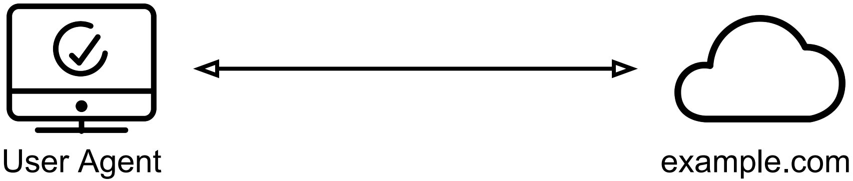
Relying Party

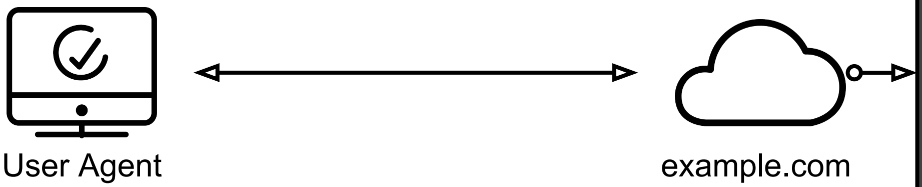
The Technical Bits

- WebAuthn uses native JavaScript code in the browser.
- The Relying Party gives the client JSON to be handled by the Authenticator.
- The CTAP responses are returned using in CBOR
  - Concise Binary Object Representation (skinny JSON)
- Easy to request a credential, but validation is a bit tricky.
- Let’s look at creating a WebAuthn credential...

Creating a WebAuthn Credential

“Hi, I’d like to make an account for `username@example.com`”

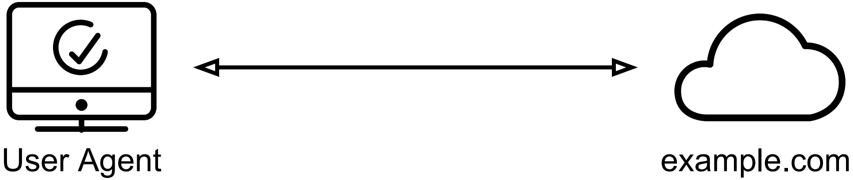




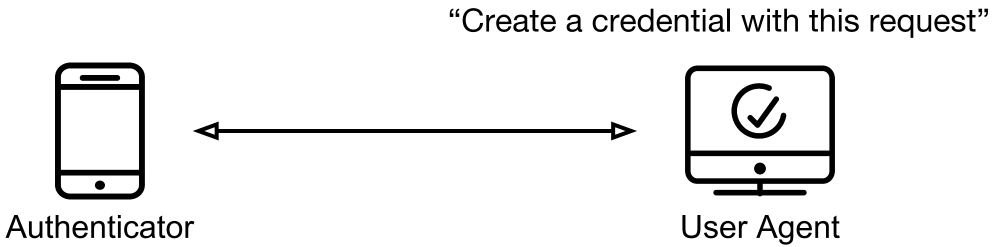
```
createRequest = {
 challenge: “kB_iazmlpT6vV3mGrukC_g”,
 // Relying Party
 rp: {
   name: "Example"
 },

 // User
 user: {
   id: the_user_id_as_buffer,
   name: "username@whatever.com",
   displayName: "User P. Name",
   icon: "https://pics.image.com/ava.png"
 },
//
 pubKeyCredParams: [
   {
     alg: -7, //“ECDSA with SHA256”
     type: "public-key",
   }
 ],
 authenticatorSelection: {
   authenticatorAttachment:"cross-platform",
   requireResidentKey: false,
   userVerification: "preferred"
 },
};
```

Creating a WebAuthn Credential

```
navigator.credentials.create({publicKey: createRequest})
```



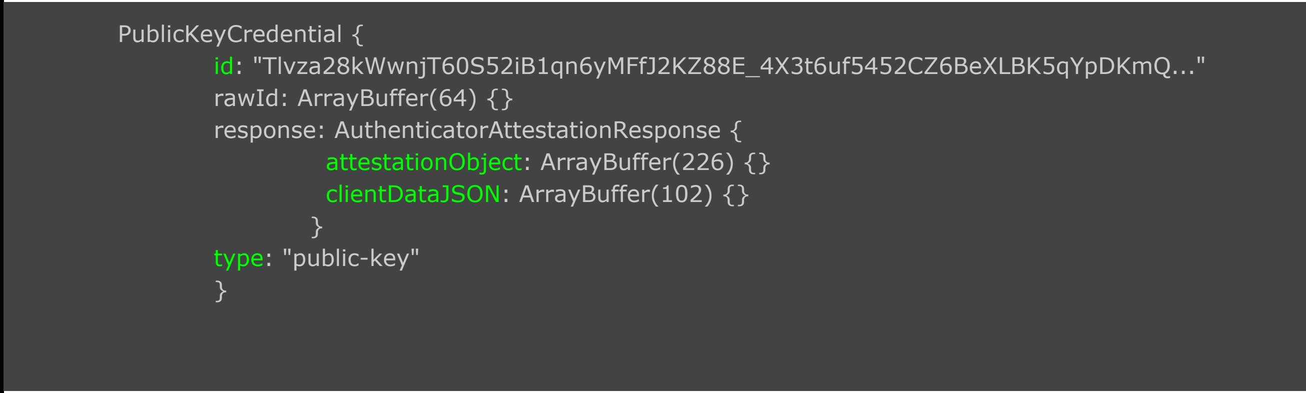
Creating a WebAuthn Credential



Create

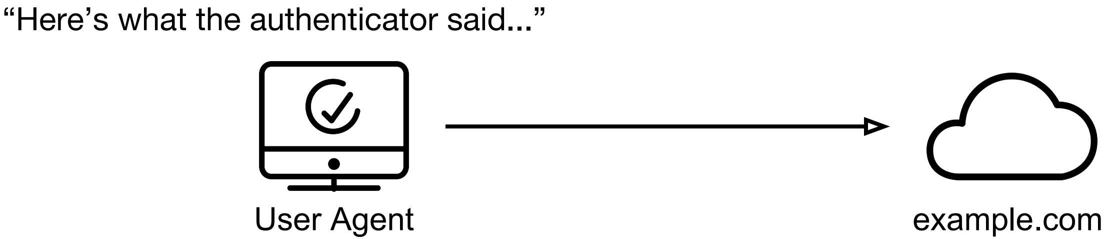
Authenticator returns:

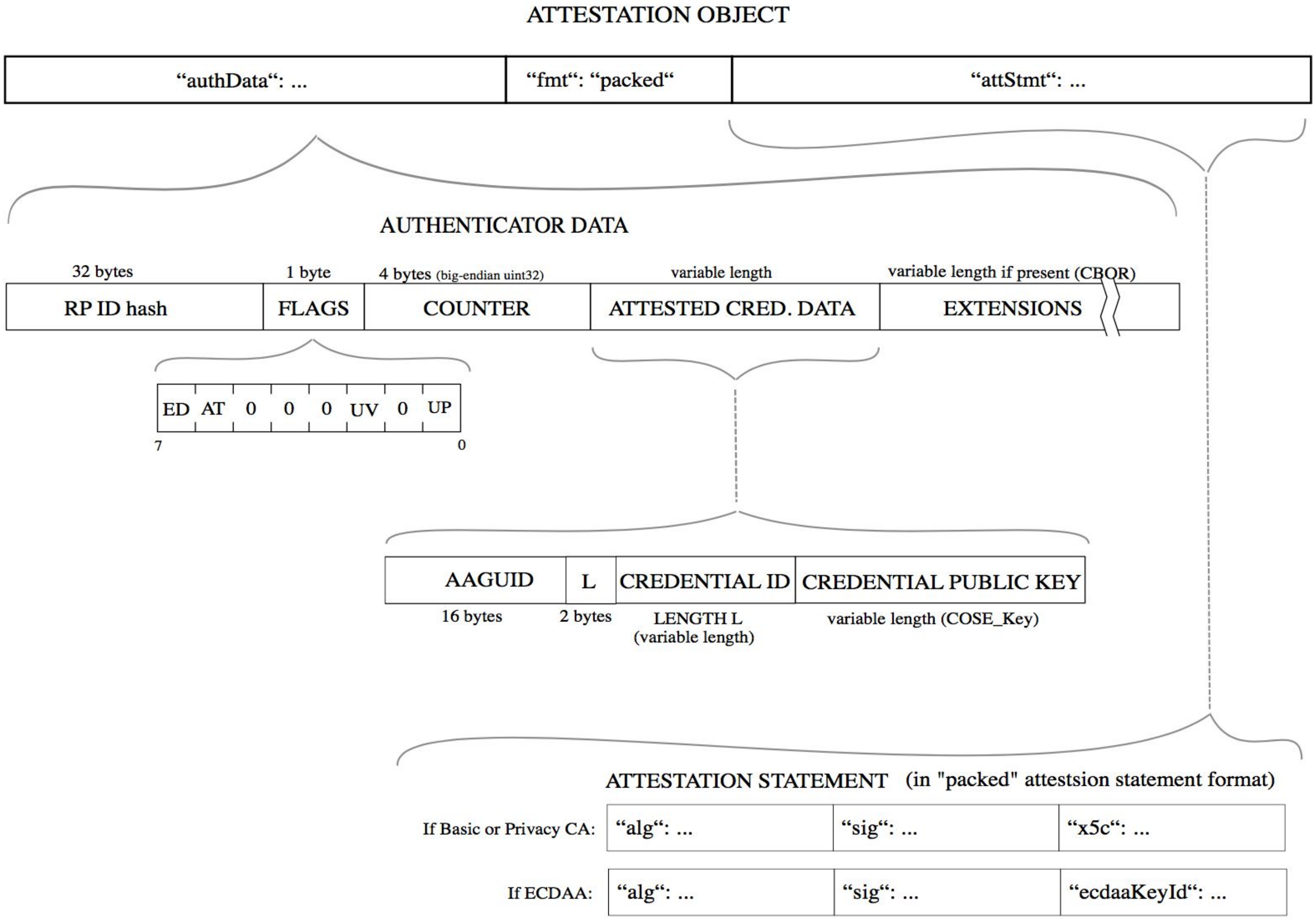
- ID
- Attestation Object
  - Attestation Data
  - Auth Data
- Client Data
- Type



```
PublicKeyCredential {
          id: "Tlvza28kWwnjT60S52iB1qn6yMFfJ2KZ88E_4X3t6uf5452CZ6BeXLBK5qYpDKmQ..."
          rawId: ArrayBuffer(64) {}
          response: AuthenticatorAttestationResponse {
                      attestationObject: ArrayBuffer(226) {}
                      clientDataJSON: ArrayBuffer(102) {}
                    }
          type: "public-key"
          }
```

Creating a WebAuthn Credential





ATTESTATION OBJECT

"authData": ...	"fmt": "packed"	"attStmt": ...

AUTHENTICATOR DATA

32 bytes	1 byte	4 bytes (big-endian uint32)	variable length	variable length if present (CBOR)
RP ID hash	FLAGS	COUNTER	ATTESTED CRED. DATA	EXTENSIONS

7							0
ED	AT	0	0	0	UV	0	UP

AAGUID	L	CREDENTIAL ID	CREDENTIAL PUBLIC KEY
16 bytes	2 bytes	LENGTH L (variable length)	variable length (COSE_Key)

ATTESTATION STATEMENT (in "packed" attestsion statement format)

If Basic or Privacy CA:	"alg": ...	"sig": ...	"x5c": ...
If ECDAA:	"alg": ...	"sig": ...	"ecdaaKeyId": ...

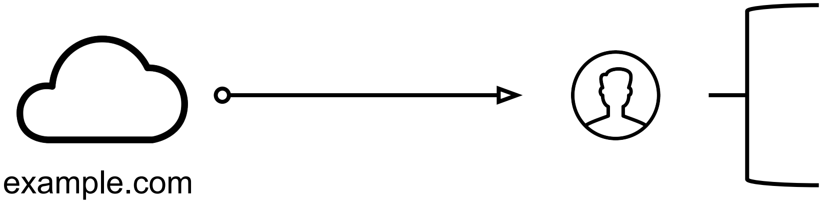
Attestation Data (abridged)

- Contains the Attestation Statement and Auth Data
- Attestation Statement
    - The private key signature over the client data
    - x509 certificate from the authenticator device
- Authenticator Data
    - Hash of the relying party ID (“example.com”)
    - Credential Public Key
    - Byte Flags with other info (user present, verified, etc)

Verifying the Data

- Is the client data properly signed/hashed?
- Are the challenge and origin correct?
- Is the credential ID in use already?
- Is this a create request or a get request?
- Was the flag for user presence set to true?
- 19 verification steps in total...

Creating a WebAuthn Credential

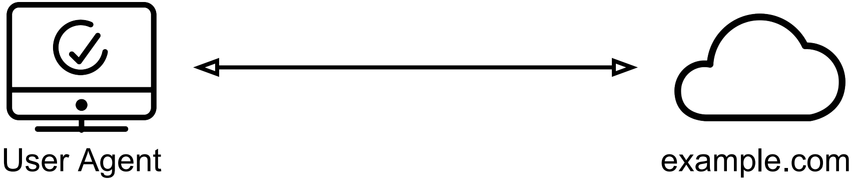


Credential ID

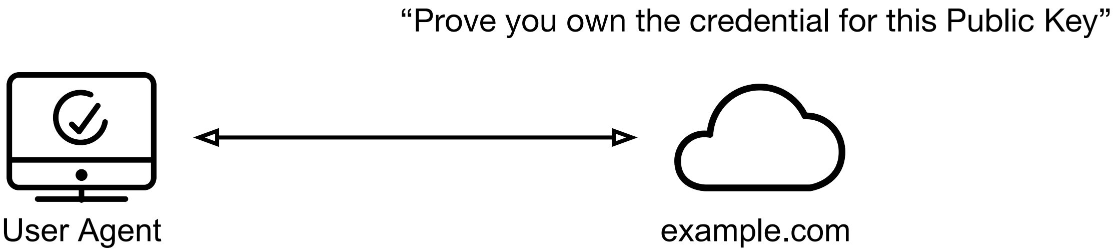
Credential Public Key

Logging in with a WebAuthn Credential

“Hi, I’d like to login as `username@example.com`”



Logging in with a WebAuthn Credential

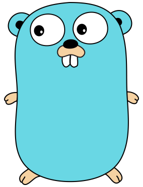


What we did

🐍🕸️Authn

github.com/duo-labs/py_webauthn

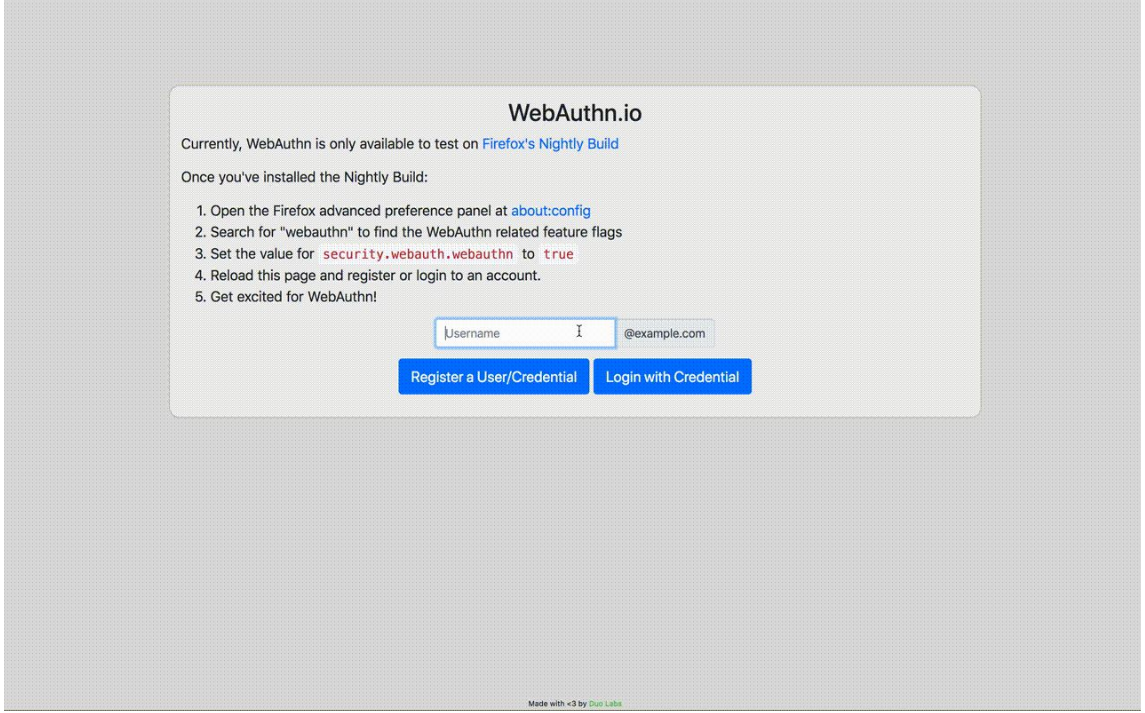
DUO LABS



🕸️ Authn

github.com/duo-labs/webauthn

DUO LABS



WebAuthn.io

Currently, WebAuthn is only available to test on Firefox's Nightly Build

Once you've installed the Nightly Build:

1. Open the Firefox advanced preference panel at about:config
2. Search for "webauthn" to find the WebAuthn related feature flags
3. Set the value for `security.webauth.webauthn` to `true`
4. Reload this page and register or login to an account.
5. Get excited for WebAuthn!

webauthn.io

DUO LABS

WebAuthn – Open-Source

Author	GitHub Repository	Language
Google	google/webauthndemo	Java
FIDO	fido-alliance/webauthn-demo	Node (JavaScript)
Duo Labs	duo-labs/webauthn	Go
Duo Labs (New!)	duo-labs/PyWebAuthn	Python
Mastercard	Mastercard/fido2-rp-spring	Java

What’s next?

- Native support of mobile cross-platform authenticators
    - i.e. Supporting Laptop to Mobile authentication
- More support of on-platform authenticators
    - Touch ID supported in Chrome only
    - Windows Hello supported in Edge
- More support for NFC and Bluetooth authenticators
- More details around how to handle account recovery

Account Recovery

- FIDO has a working group discussing best practices
- Practices include…
    - Email based account recovery
    - Backup authenticators
    - Wrapping and storing key material

Current Implementation on Browsers

Chrome Desktop

U2F API 🟩			WebAuthn API 🟩			
CTAP1/U2F 🟩			CTAP2 🟩			
USB 🟩	NFC 🟧	BLE 🟨	USB 🟩	NFC 🟧	BLE 🟨	Win10 🟧

Edge

U2F API 🟧			WebAuthn API 🟩			
CTAP1/U2F 🟩			CTAP2 🟩			
USB 🟩	NFC 🟩	BLE 🟨	USB 🟩	NFC 🟩	BLE 🟨	Win10 🟩

Chrome Android

U2F API 🟩			WebAuthn API 🟩			
CTAP1/U2F 🟩			CTAP2 🟩			
USB 🟩	NFC 🟩	BLE 🟩	USB 🟩	NFC 🟨	BLE 🟨	Android 🟩

Safari

U2F API 🟧			WebAuthn API 🟩			
CTAP1/U2F 🟧			CTAP2 🟧			
USB 🟧	NFC 🟧	BLE 🟧	USB 🟧	NFC 🟧	BLE 🟧	06 🟧

Firefox

Windows, MacOS & Linux

U2F API 🟧			WebAuthn API 🟩			
CTAP1/U2F 🟩			CTAP2 🟧			
USB 🟩	NFC 🟧	BLE 🟧	USB 🟧	NFC 🟧	BLE 🟧	Win10 🟧

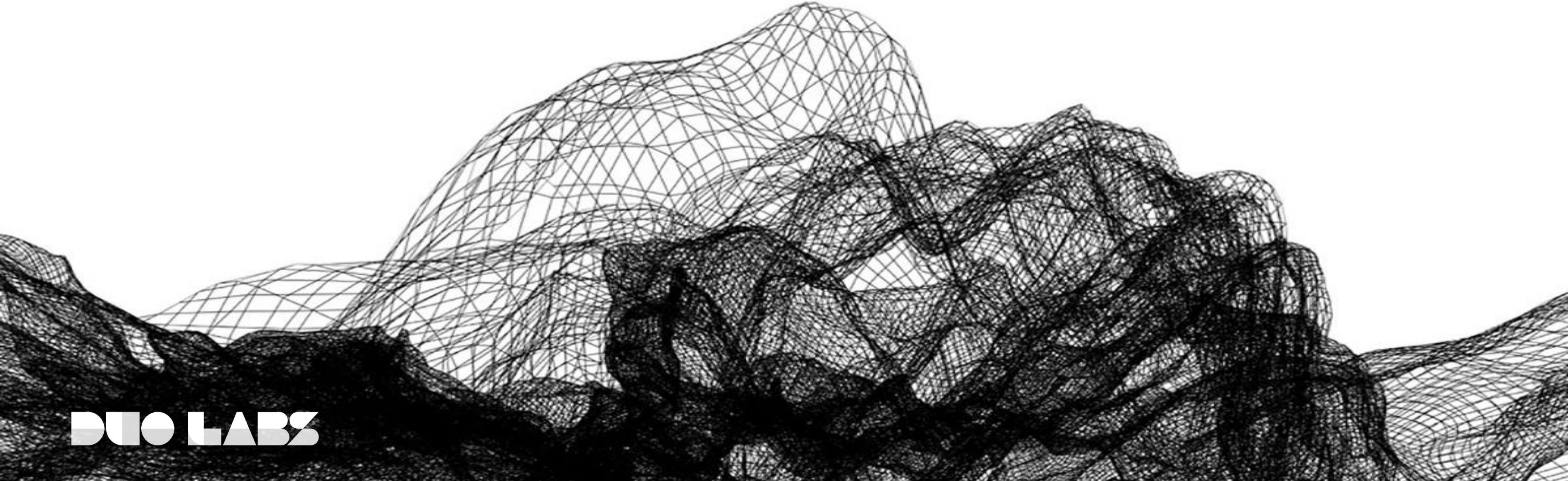
🟩 Implemented/Stable
🟨 In Development
🟧 Not Supported/No ETA

Takeaways

- **Passwords have problems**, but we don’t have to settle for them
- **WebAuthn is a new standard** for managing public-key credentials on the web, for the purpose of **strongly authenticating users.**
- WebAuthn development still has some areas needing work, but you can begin to **implement it on your site today**.
- **Major platform, hardware, and software vendors are investing resources** into WebAuthn, so expect to hear more in the coming months and years.

Questions?

@codekaiju && @futureimperfect



DUO LABS