FIDO2 & WEBAUTHN

PASSWORDLESS LOGINS AND 2FA

Benjamin Schmid, @bentolor

PASSWORDS ARE BEYOND REPAIR!

Retention

Complexity

Reuse

Stealing & Phishing

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address pwned?

457	10,093,204,490	113,729	194,661,914
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991 Collection #1 accounts

Recently added breaches

268,765,495 Wattpad accounts

Password Memes: Length restrictions, Weird complexity rules, Expiration

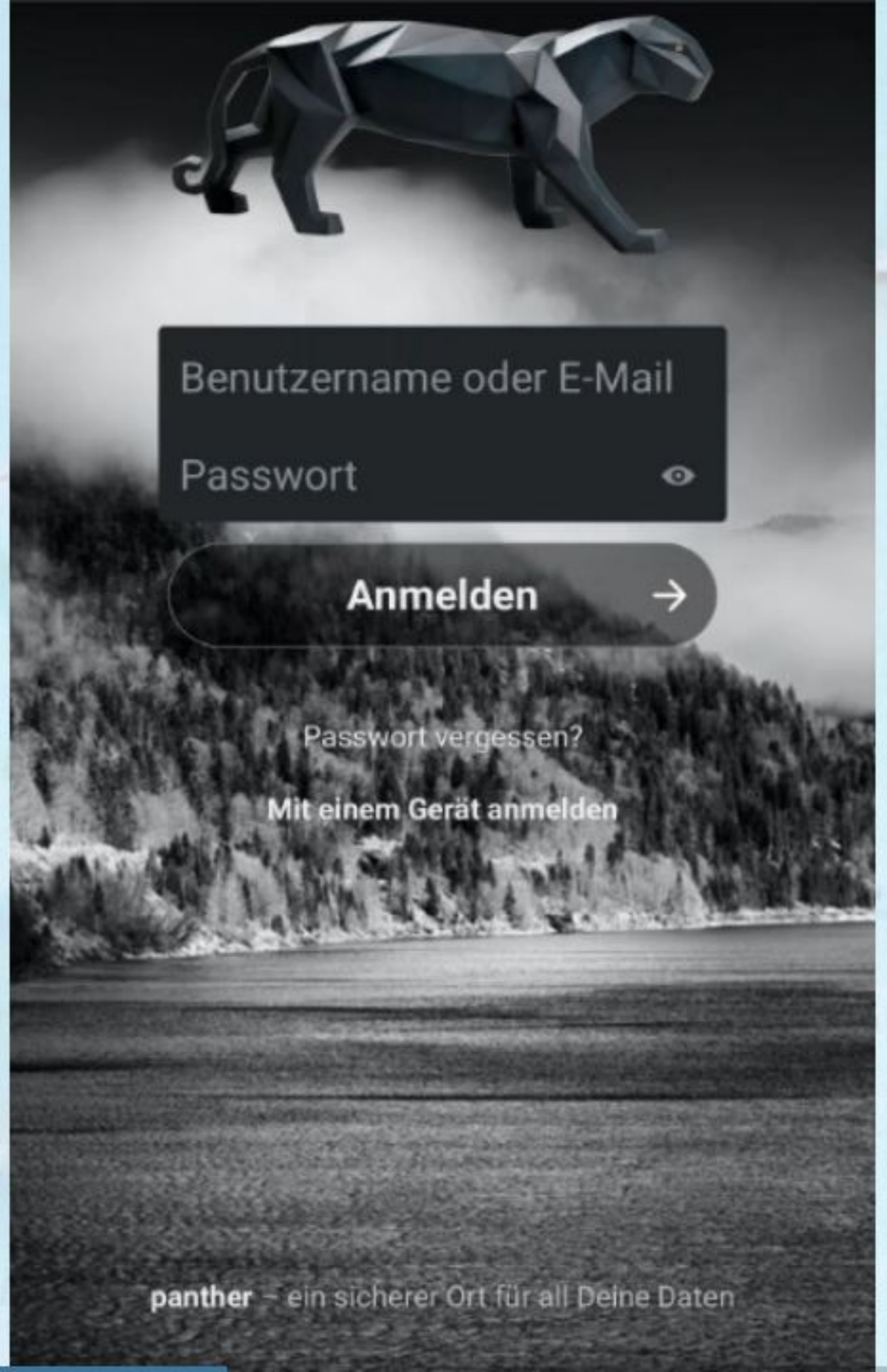
2-FACTOR / MFA FOR THE RESCUE?

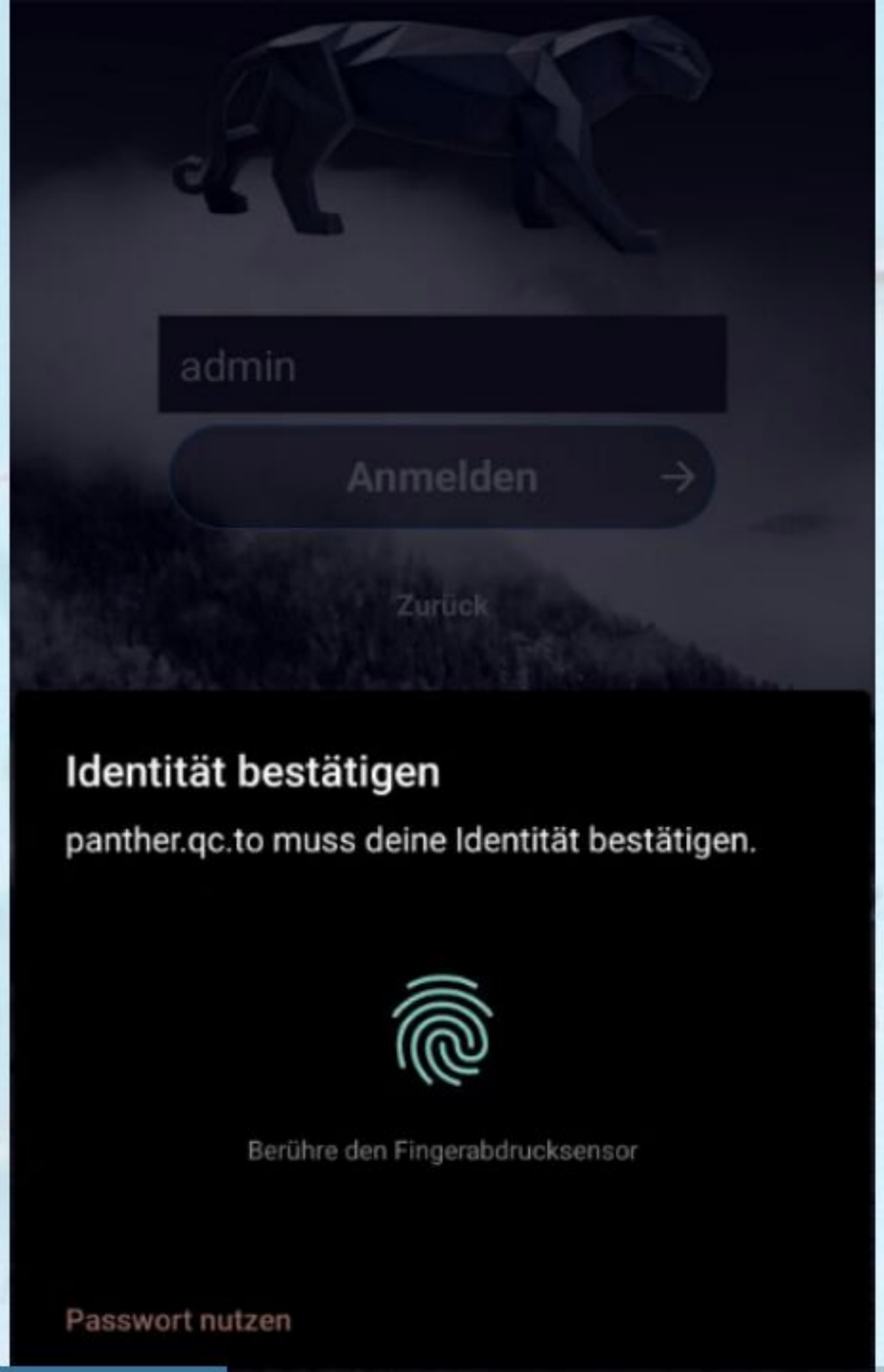
Grant access only after presenting 2+ pieces of evidence out of:
knowledge, **possession** or **inherence**.

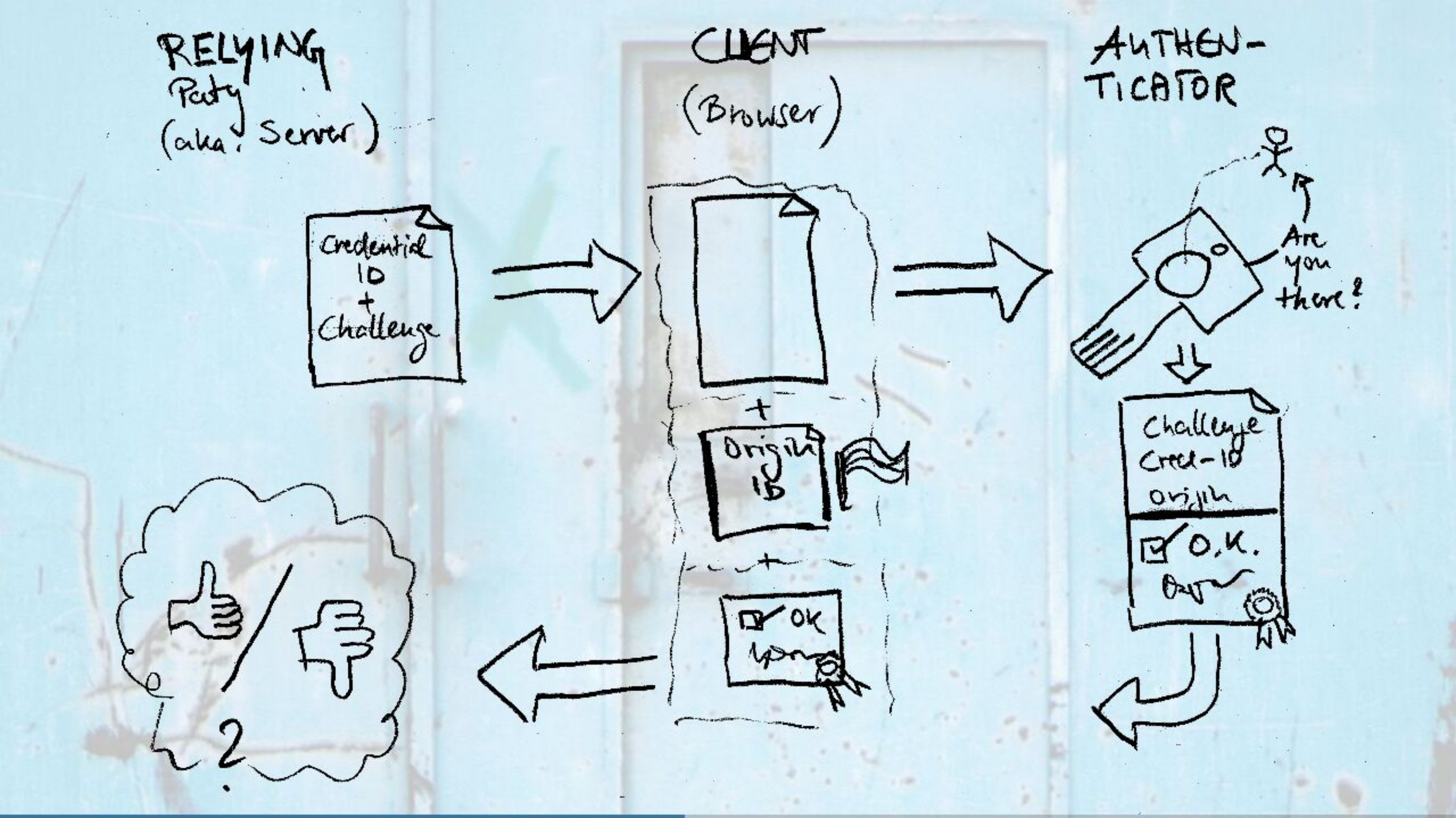
- *One-time passwords:* Mobile App, SMS, Email
- *Tokens:* OTP Token, Security Key
- *Biometrics:* Fingerprint, Iris

Issues: UX, Privacy, Phishing, Costs, Portability

FIDO2 & WEBAUTHN


Benutzername oder E-Mail
Passwort
Anmelden
Passwort vergessen?
Mit einem Gerät anmelden
panther – ein sicherer Ort für all Deine Daten


admin
Anmelden
Zurück
Identität bestätigen
panther.qc.to muss deine Identität bestätigen.
Berühre den Fingerabdrucksensor
Passwort nutzen


RELYING Party (aka: Server)
CLIENT (Browser)
AUTHEN-TICATOR
Credential ID + Challenge
Origin ID
OK
Are you there?
Challenge
Cred-ID
origin
O.K.
2

SOLVING THE CONFUSION

FIDO	FIDO Alliance; author of protocols UAF, U2F, FIDO2
FIDO2	Joint Project by FIDO Alliance & W3C. Bascially: **WebAuthn + CTAP**
WebAuthn	Browser JS API to talk to *Authenticators* and manage *Credentials*
CTAP	Client to Authenticator Protocol *CTAP1: U2F, CTAP2: FIDO2*

AUTHENTICATOR TYPES

Platform (TPM)

Verification via Biometrics: Fingerprint, Iris, ...
Platforms: Android, Windows 10

Portable: Security Keys (USB, NFC, Bluetooth)

Verification via Presence
Platforms: all

EXAMPLE CLIENT CODE

```
const credentialCreationOpts = {
    challenge: Uint8Array.from( serverRandomValue, c => c.charCodeAt(0)),
    rp: { name: "eXXcellent solutions Web", id: "exxcellent.de" },
    user: {
        id: Uint8Array.from("EXXL85T9AFC", c => c.charCodeAt(0)),
        name: "alice@exxcellent.de",
        displayName: "Alice Lee",
    },
    pubKeyCredParams: [{alg: -7, type: "public-key"}],
    timeout: 60000
};

const credential = await navigator.credentials.create(
     { publicKey: credentialCreationOpts }
);
```

FIDO2/WEBAUTHN SCENARIOS

Convenient & Secure 2FA

Just use WebAuthn to register/verify an additional credential. *No more OTPs – Yeah!*

Passwordless Logins (no MFA)

Just use WebAuthn *instead* of passwords

Passwordless Logins (with 2FA)

Request *User Verification (UV)* from Authenticator → Additional PIN, Biometrics, …

"I'm a bank!"

Trusting for only selected authenticators? → request device attestation

"What is my username?"

Use *Resident Credentials (RK)*: Can be acquired without Credential ID.
But: 1. Incomplete browser support 2. UV must be setup 3. Limited storage

WebAuthn.io

A demo of the WebAuthn specification

example_username

Attestation Type | None

Authenticator Type | Unspecified

Register | Login

Advanced Settings

FIDO2, WEBAUTHN & JAVA

`webauthn4j`

A portable Java library for WebAuthn server side verification

`webauthn4j/webauthn4j-spring-security`

Spring Boot / Angular sample application

Keycloak 8.0+

Built-in support using `webauthn4j`

RESOURCES

Introductions

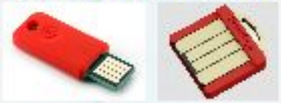
- FIDO2 Developer Primer: `webauthn.guide`
- FIDO2 Demo: `webauthn.io`

In-depth materials

- Links: `github.com/herrjemand/awesome-webauthn`
- Articles: `medium.com/@herrjemand/`

Standard Hardware Security Keys

$20-$35 Open-source key: Solo Keys



Indestructible, #1 brand, $20-$70: Yubico

Special Hardware Keys

Biometrics (no PIN for UV!):

Wearables:

Software-only Key (Android)

wiokey.de (Free)