

# Webauthn Identitätsdiebstahl ade!



5. April 2019  
Jan Lühr

1. Motivation

4

2. Multifaktor-Authentisierung

8

3. WebAuthn im Detail

12

4. Angriffsform: Social Engineering

16

5. Zusammenfassung

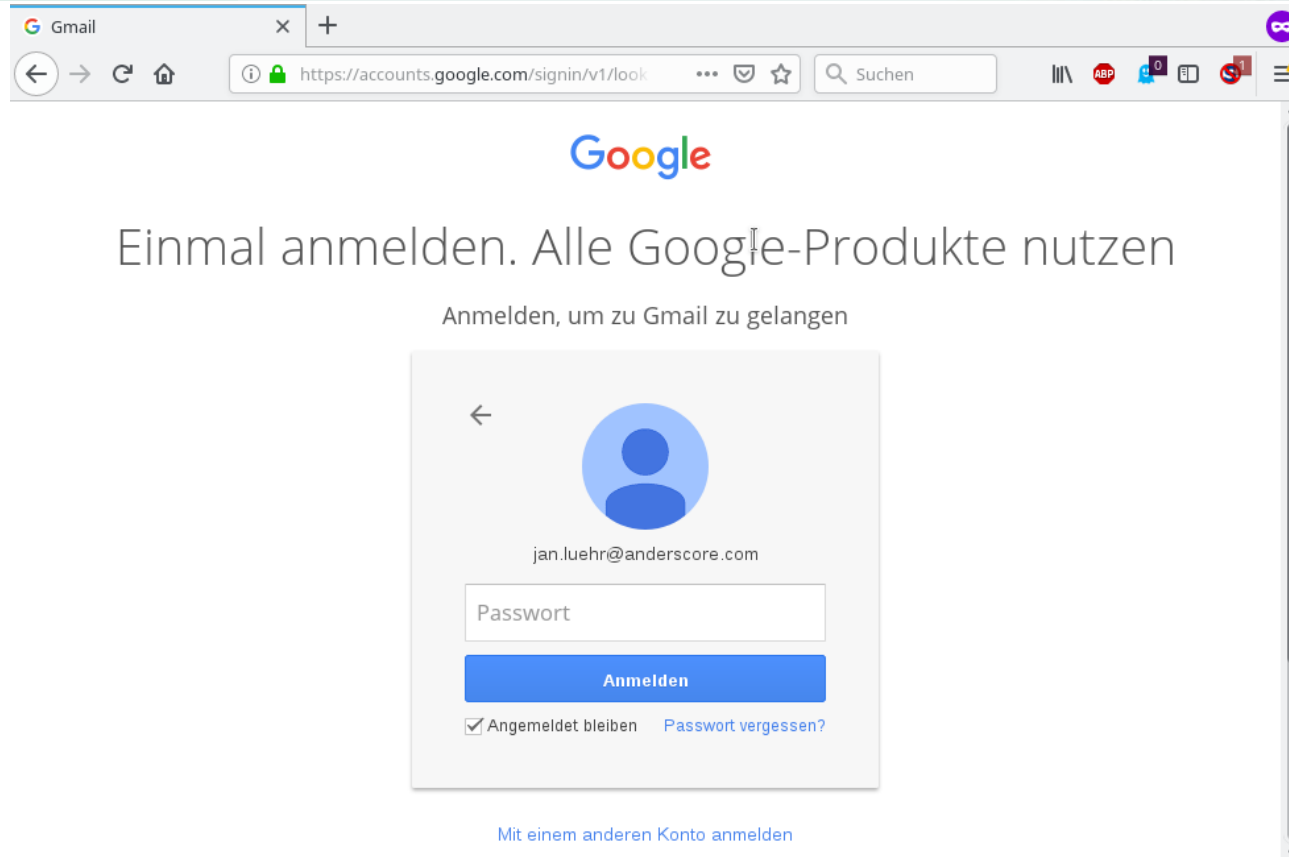
18

Jan Lühr

- B. Sc., Computer Science
- Senior Software Engineer & Architect
- anderScore seit 2007
- Fokus
  - Software Development
  - Pragmatic Architect
  - Network- and Security-Techniques
  - IT-Trainer
  - Java, JavaScript, Ruby



# 1. Motivation: Login



The screenshot shows a web browser window with the address bar displaying `https://accounts.google.com/signin/v1/look`. The page content includes the Google logo, the text "Einmal anmelden. Alle Google-Produkte nutzen", and "Anmelden, um zu Gmail zu gelangen". A login card is centered on the page, featuring a back arrow, a blue user icon, the email address `jan.luehr@anderscore.com`, a password input field labeled "Passwort", a blue "Anmelden" button, and a checkbox for "Angemeldet bleiben" with a link for "Passwort vergessen?". Below the login card is a link that says "Mit einem anderen Konto anmelden".

Google

Einmal anmelden. Alle Google-Produkte nutzen

Anmelden, um zu Gmail zu gelangen

←

jan.luehr@anderscore.com

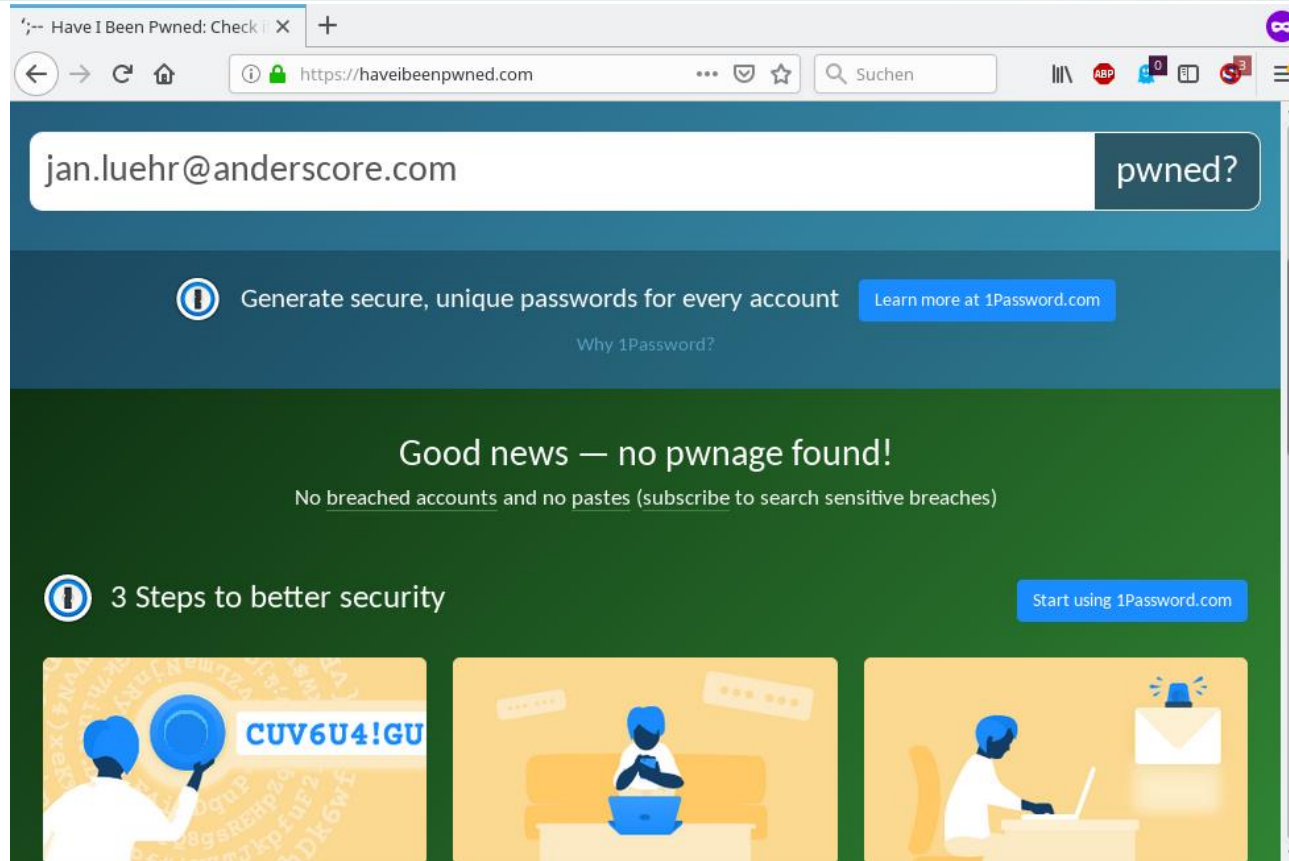
Passwort

Anmelden

☒ Angemeldet bleiben [Passwort vergessen?](#)

[Mit einem anderen Konto anmelden](#)

# 1. Motivation: Problemfall Passwort



# 1. Motivation: Angriff auf Web-Angebot

1. Angriff auf Web-Angebot: Nutzernamen & Kennwort gestohlen:
  - Einbruch in Server (**Datenreichtum**, p0wned, hack)
  - Gefälschte Version der Login-Seite im WWW (**phishing**)
2. Angreifer nutzt Zugangsdaten:
  - Zur Anmeldung am System des Opfers
  - Zur Anmeldung an **anderen Systemen** (identische Zugangsdaten)
3. Abwehr:
  - Phishing erschweren (z.T. schwer möglich)
  - Identity-Federation / Dienstleister nutzen (Datenweitergabe)
  - Ungewöhnliche Login-Versuche erkennen und sperren (sperrt z.T. legitime Nutzer)
  - Neben Kennwort **weitere Merkmale** fordern (z.B. Online-Banking: TAN-Nummer)



Weitere Merkmale fordern

Mehrfaktor-Authentisierung (MFA), Zwei-Faktor-Authentisierung (2FA)

## 2. MEHRFAKTOR-AUTHENTISIERUNG



## 2. Mehrfaktor-Authentisierung (MFA)

- Mehrere Merkmale zur Anmeldung – Kombination aus:

1. Was jmd. **kennt** – **Wissen**
2. Was jmd. **hat** – **Besitz**
3. Was jmd. **ist** – **Biometrie**



- BSI IT-Grundschutz: M 4.441 Multifaktor-Authentisierung für den Cloud-Benutzerzugriff:

*„Eine sichere Lösung stellt hierbei eine Multifaktor-Authentisierung dar.  
Dabei sind mindestens zwei Faktoren für eine erfolgreiche Authentisierung erforderlich.“*



## 2. Mehrfaktor-Authentisierung: Besitz

### Was erfährt der Benutzer – User-Experience verbreiteter Verfahren:

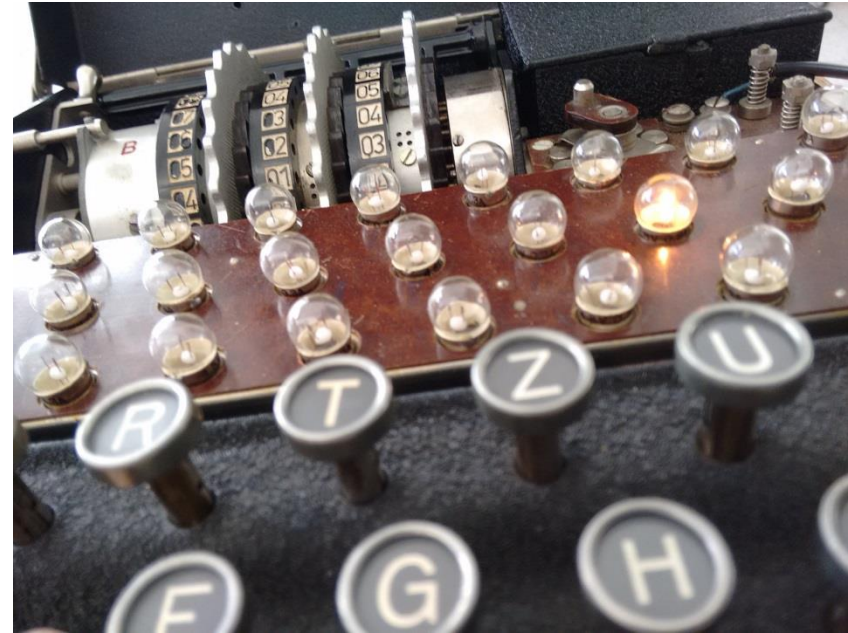
- Typisch: Einmal-Passwörter (One-Time-Password – OTP)
  1. Papier-Liste (TAN)
  2. Challenge-Response-Verfahren / Event (iTan, Chip-Tan, HOTP)
  3. Zeitbasiert (TOTP)
  4. Push-Nachricht (mTan)
- Alternativ:
  1. Smartphone-App (z.B. Google Push)
  2. USB-Dongle (U2F, Smartcard)
  3. Smartcard
  4. Client-Zertifikate (TLS)



Keine schnelle & zuverlässige Zustellung!

## 2. MFA: Problematische Eigenschaften

1. Schlechte User-Experience (UX):
  - Umständliches Handling
  - Token-Verlust: Kompliziertes Recovery
2. Unzureichender Schutz
  - Eingabe von TAN / OTP auf Phishing-Seite
  - Z.T. unsichere Plattform (SMS; RCE Android Media Subsystem)
3. Höhere Kosten
  - Zusatzhardware kostet Geld
  - Aufwendiges Deployment
4. Kein einheitlicher Standard
  - Proprietär: Software / Plug-Ins nötig
  - Meist Kaum Verbreitung im WWW



Ein neuer Standard für das World-Wide-Web

## 3. WEBAUTHN IM DETAIL

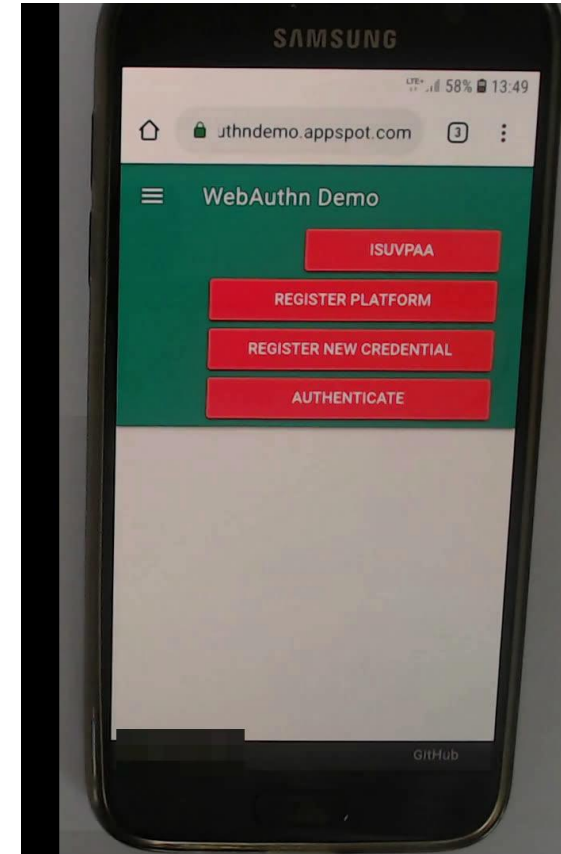
# 3. Web Authentication (WebAuthn)

- “Web Authentication: An API for accessing Public Key Credentials Level 1”
  - **W3C-Standard**, Status: W3C Recommendation (4 March 2019)
  - Umgesetzt in Chrome, Firefox, MS Edge
  - Audit: Paragon Initiative Enterprises (08/2018)
    - Kryptographische Konventionen z.T. nicht befolgt (→ Schwächung)
    - Kein praktischer Angriff, **Nutzung empfohlen** (gegenüber 1-Faktor Kennwort)
- Technisch: Erweiterung / Standardisierung FIDO JavaScript U2F API (erweitert W3C Credential API)
  - Public- / Private Key basierte Signatur: **Schutz vor Phishing; privater Key lokal gespeichert**
  - Erweiterung
    - Neue Verfahren (z.B. Fingerabdruck-Lesegeräte, **keine serverseitige Speicherung biometrischer Daten**)
    - Bestimmten Benutzer verifizieren (vorher: lediglich Präsenz eines Nutzers)

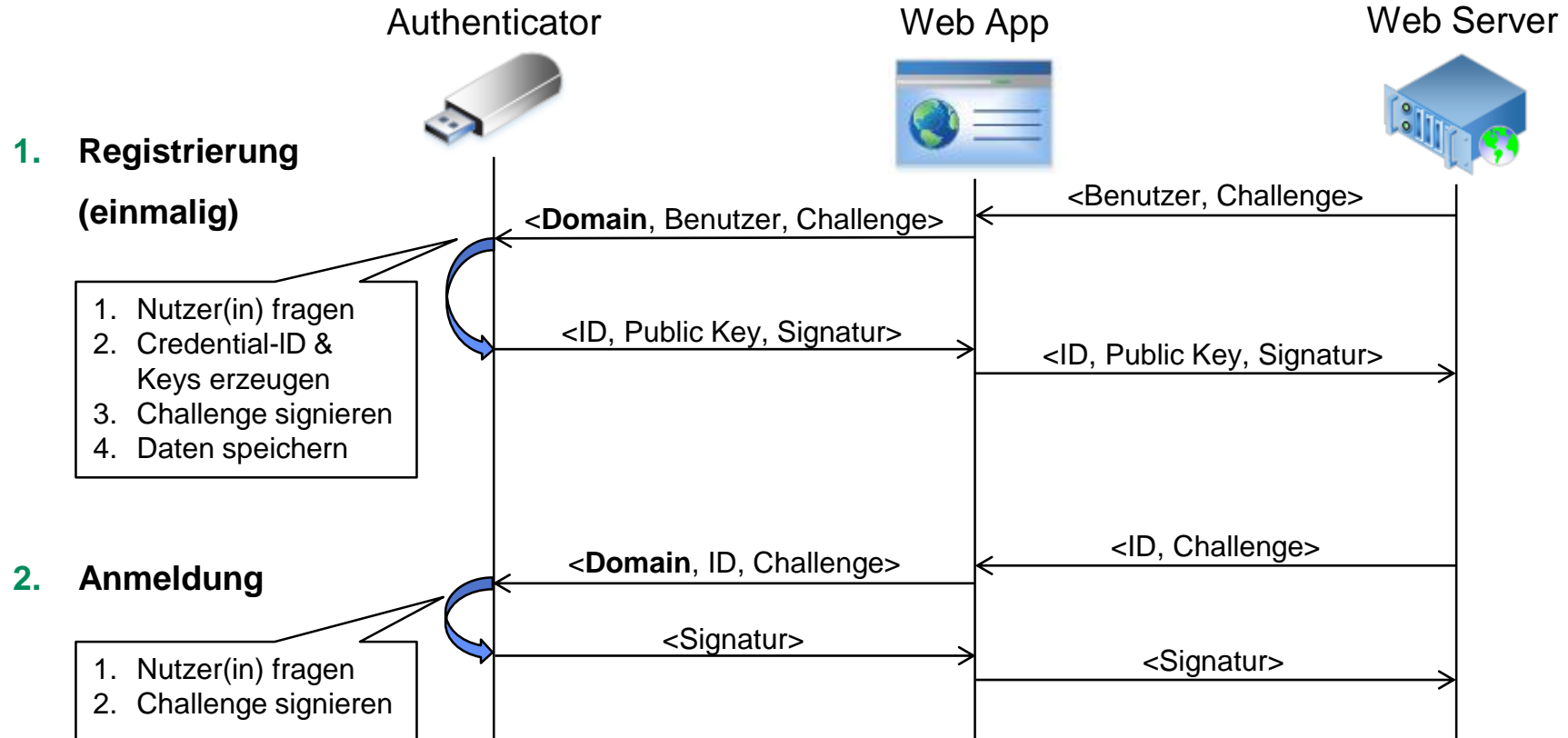


# 3. WebAuthn: User Experience (UX)

1. **Einmalige Registrierung des Geräts („Authenticator“)**
2. **Anmeldung**
  - **Ohne Kennwort**
  - (als weiterer Faktor)



### 3. WebAuthn: Technischer Ablauf (vereinfacht)



<https://www.youtube.com/watch?v=lc7scxvKQOo>

## 3. ANGRIFFSFORM: SOCIAL ENGINEERING



# 3. Angriffsform: Social Engineering

- **Identitätsdiebstahl – Mehrfaktor-Authentisierung umgangen:**

„Ich kann keine Text-Nachrichten empfangen, während ich telefoniere.“

- **Mensch wird zur Kooperation überzeugt**

Stress, Hilfsbereitschaft, Erpressung, Rhetorik  
(Ethos, Pathos, Logos) ...

- **Abwehr: Schwierig**

- Widerstandsfähige Software
- Schulung der Mitarbeiter
- Härtung der Geschäftsprozesse



# 5. Zusammenfassung

## 1. Multifaktor-Authentisierung:

- Wesentlicher Sicherheitsgewinn
- Teil des BSI-Grundsatz Katalogs

## 2. WebAuthn

- Offener Standard für Web-Apps, Fokus: End-Nutzer
- Schutz vor Phishing
- Stand: Candidate Recommendation

## 3. Sicherheit

- Multifaktor-Authentisierung ist ein Teil
- Angriffe z.B. via Social Engineering möglich
- Abwehr im Geschäftsprozesse



- Java Demo (Servlet / GAE): <https://github.com/google/webauthndemo>
- JavaScript Client Howto:  
<http://slides.com/herrjemand/jan-2018-fido-seminar-webauthn-tutorial>
- Client API Documentation:  
[https://developer.mozilla.org/en-US/docs/Web/API/Web\\_Authentication\\_API](https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API)
- Android Safety Net Client Attestation API  
<https://developer.android.com/training/safetynet/attestation>
- Yubico Webauthn Server (Java)  
<https://github.com/Yubico/java-webauthn-server>
- Weitere Sprachen / Ressourcen:  
<https://webauthn.io/>

**Vielen Dank für Eure Aufmerksamkeit!**

**Fragen?**