

# Usable Authentication: Was ist noch besser als ein sicheres Passwort?

15. BDCS, Bonn, 29. Oktober 2020

# Motivation

**WIR GESTALTEN DAS INTERNET.**  
**GESTERN. HEUTE. ÜBER MORGEN.**

# Historische Einordnung

- Passwörter (“Wachtwort”) gab es schon bei den Römern
- In der IT gilt Fernando Corbató als “Urvater” (1960, MIT)
- Einfache User/Passwort Kombinationen sind bis heute üblich
- Erster “Hack” und “Paste” schon 1962, ebenfalls MIT
- Motivation: Mehr Anwender sollten die Computer nutzen können

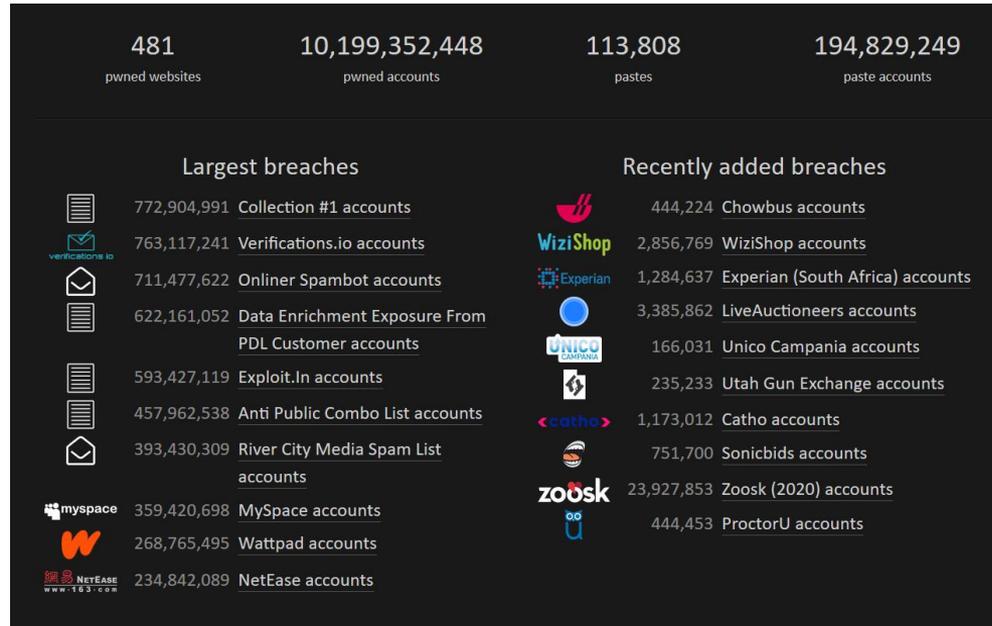
# Länge bedeutend wichtiger als Komplexität

Zeichensatz	Chars	Länge des Passworts						
		8	12	16	20	24	28	32
Alphanumeric + Specials	94	6.10E+15	4.76E+23	3.72E+31	2.90E+39	2.27E+47	1.77E+55	1.38E+63
Base64	64	2.81E+14	4.72E+21	7.92E+28	1.33E+36	2.23E+43	3.74E+50	6.28E+57
Alphanumeric	62	2.18E+14	3.23E+21	4.77E+28	7.04E+35	1.04E+43	1.54E+50	2.27E+57
Upper and Lower Alphabet	52	5.35E+13	3.91E+20	2.86E+27	2.09E+34	1.53E+41	1.12E+48	8.17E+54
Upper or Lower Alphabet	26	2.09E+11	9.54E+16	4.36E+22	1.99E+28	9.11E+33	4.16E+39	1.90E+45
Numbers	10	1.00E+08	1.00E+12	1.00E+16	1.00E+20	1.00E+24	1.00E+28	1.00E+32
		Mögliche Passwörter						

# Problemkreis

- Passwörter skalieren nicht für den Einsatz bei vielen Diensten und über viele Geräte hinweg (z.B. Workstation, Notebook, Handy, Pad, Fernseher...)
- Nutzer verwenden das identische Passwort bei vielen Diensten/Geräten
- Technische Entwicklung macht Passwörter impraktikabel, 12, 16 oder gar 32 Zeichen lassen sich in der Praxis nur mit einem Passwort-Manger handhaben (“Keychain”).
- Passwort “leaks” aus hacks gefährden die Sicherheit
- Leaks sind nur die “Spitze des Eisbergs”
- Unternehmen wollen keine Passwörter mehr speichern (GDPR-Betriebsrisiko)

# Aktueller Stand “haveibeenpwned” Leak Database



# Der Weg zu mehr Sicherheit

**WIR GESTALTEN DAS INTERNET.**  
**GESTERN. HEUTE. ÜBER MORGEN.**

# Single Sign on

- Kerberos (1980er), RADIUS (1991), TACACS (1984), TACACS Plus (1993)
- Roaming-Dienste (z.B. iPass 1996, EDUROAM 2002)
  
- OAuth 2006 (Amazon, Google, Facebook, Microsoft, Twitter)
- OpenID 2007 (Multiple, ca. 1.2 Mrd. User, 1.1 Mio Websites)
- “Sign in with Apple” 2019
  
- Vorteil: Nur noch ein zentraler Login, abgeleitete Authentication
- Nachteil: Erfordert ein etabliertes Vertrauensmodell zwischen den Anbietern
- Login beim Vertrauenprovider sollte so sicher wie möglich sein.

# Risiko und Geschäftsmodell in einem

- Weitere Stärkung der Plattformen
- Erhöhte usability, aber deutlicher User Lock-In
- Abhängigkeit weiterer Webdienste von der Datenerhebung und Zulieferung durch Plattformbetreiber
  
- Aus EU-Sicht keine souveränen Dienste möglich

# Multi (Two-) factor Authentication

- Two-Factor Paradigma: “Etwas was ich weiss, etwas was ich habe”
- (Multi: Wissen, Besitz, Inherent (Biometric), Lokation)
  
- z.B. Username/Passwort und Zugriff auf Gerät (SMS)
- Wird durchbrochen wenn alles auf einem Gerät (z.B. Mobiltelefon) gespeichert
  
- z.B. auch Google Authenticator

# Public key authentication im Web - WebAuthn

- Konzept prinzipiell verfügbar seit über 20 Jahren (ssh-1 1995, ssh-2 2006)
- Public Key Authentication ist vorgesehen als Varianten z.b. in 802.1x Ethernet oder WPA-EAP, hier können im Prinzip alle möglichen Autentication Services hinterlegt werden
- Im WebAuthn/FIDO2 Standard wird ein TLS Tunnel zum “Durchreichen” der Authentication zwischen Endgerät und Diensteanbieter etabliert.

# Stand der Umsetzung

# Zentraler Login als Authenticator in allen Fällen

## Mobile Devices

- Apple Touch ID, Face-ID
- Google Imprint, Face Unlock
- Samsung Pass

## Dektop

- Microsoft Hello
- MacOS

# Umsetzung von WebAuthn bei Diensten

## Umsetzung bei Social Media

- Facebook, Instagram, Twitter, Youtube

## Multi-Services

- Google Accounts, Microsoft Accounts

## Gaming

- EA, Epic

## Services

- AWS, Dropbox, Teamviewer

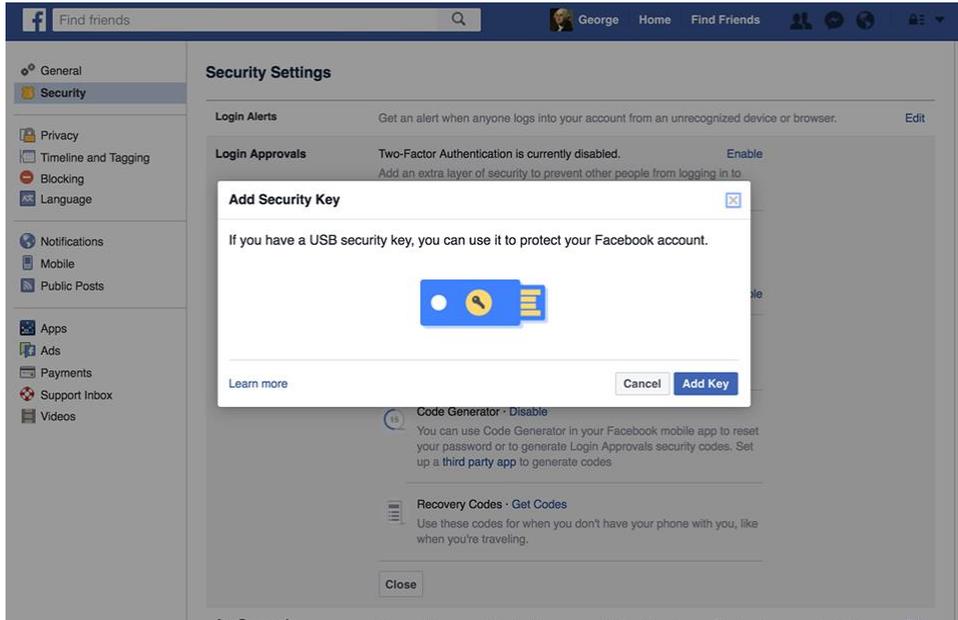
# Umsetzungshindernisse

- Gängige Browser unterstützen sämtlichst WebAuthn (Chrome, Edge, FireFox, Safari) – in der aktuellen Version (2019+)
- Uneinheitlich: z.B. unterstützt AWS FIDO2, Amazon bisher nicht
- Fehlende TPMs in Kundenrechnern
- TPM ist Standard in mobile Geräten, bei Notebooks dringend empfohlen (z.B. für Festplattenverschlüsselung)
- TPMs als externe Geräte

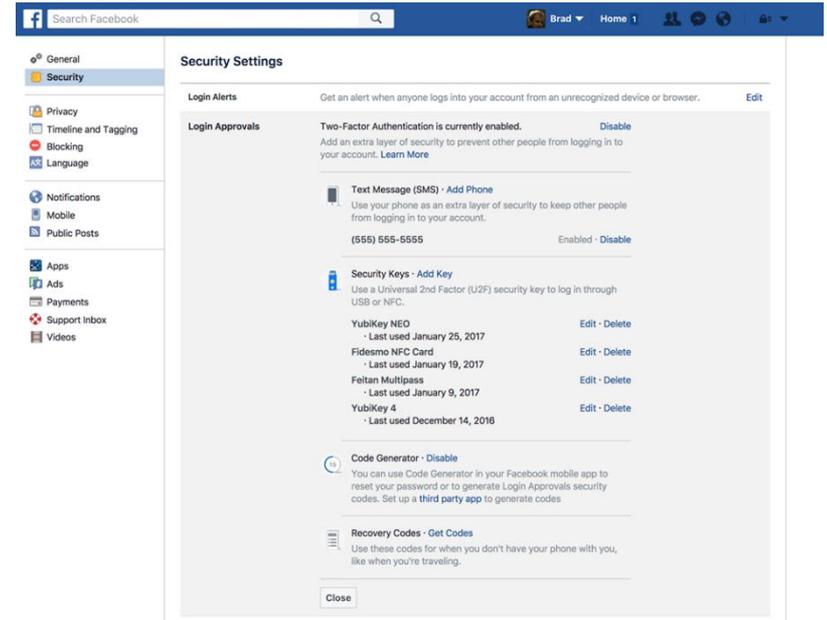
# Externe Authenticators (CTAP-Erweiterung)

- Mit/ohne Fingerabdruck
- USB, Bluetooth, NFC verfügbar
  
- YubiKey
- Thetis
- Google Titan Security Key
- SoloKeys
- CryptoTrust
- Kensington
- u.v.a.m.

# Registrierung beim Dienst



The screenshot shows the Facebook Security Settings page for a user named George. A modal dialog box titled "Add Security Key" is open in the center. The dialog contains the text: "If you have a USB security key, you can use it to protect your Facebook account." Below the text is a blue icon representing a USB security key. At the bottom of the dialog are three buttons: "Learn more", "Cancel", and "Add Key". The background settings are dimmed, showing sections for "Login Alerts", "Login Approvals", "Code Generator", and "Recovery Codes".



The screenshot shows the Facebook Security Settings page for a user named Brad. The "Login Approvals" section is active, showing that "Two-Factor Authentication is currently enabled." Below this, there are several security options:

- Text Message (SMS) - Add Phone:** Use your phone as an extra layer of security to keep other people from logging in to your account. (555) 555-5555. Status: Enabled - Disable.
- Security Keys - Add Key:** Use a Universal 2nd Factor (U2F) security key to log in through USB or NFC. A list of keys is shown:
  - YubiKey NEO - Last used January 25, 2017. Edit - Delete
  - Fidestmo NFC Card - Last used January 19, 2017. Edit - Delete
  - Feltan MultiPass - Last used January 9, 2017. Edit - Delete
  - YubiKey 4 - Last used December 14, 2016. Edit - Delete
- Code Generator - Disable:** You can use Code Generator in your Facebook mobile app to reset your password or to generate Login Approvals security codes. Set up a third party app to generate codes.
- Recovery Codes - Get Codes:** Use these codes for when you don't have your phone with you, like when you're traveling.

# Test der Voraussetzungen

- Auf <https://webauthn.io/> kann man die eigenen Voraussetzungen prüfen
- Testregistrierung
- Testlogin

Credentials for landefeld@andastra.de		
*Credentials are stored for 24 hours.		
Date created	Raw ID	Public Key
Thu, 6:25AM UTC	Lsreh7Crm55w1oj3abBDDMQ6Bdpc4SXjn3O7luKHNQ=	-----BEGIN RSA PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgkCAQEAE6Z/VObbL0Yniwd3W5gFr dF5amJQfLuLUqqPXtFuGHn9zppCE8pppe54nT5p9UJjVxx1xPttvGm1AP04VbOoo c0n5yRmNK53Z8AjbjyirXKKU5wZE3Rsa3GS+DXbGlgBi9/NKNb52s1/YTZNH2ox fX41KDYart/qk2sJbIKw7vQU7WiEV1z5pEimXN+QM1QLMJ/6ullAaEosNCMhyYZh 4g2pYONquMcdEFknJESPfHGvGvEtimJGeUXr8xBMyo7hz3asGNPIp5//YskGviM mHkTwwJvyp1D7yR8lvEmBaV/lbG0yR42dR10sOD45LfU1DDK9uGBiNj7059i/36s pwIDAQAB -----END RSA PUBLIC KEY-----

# Henne-Ei-Problem

- Keine automatische Umstellung betehender Accounts
- Anwendern ist die verbesserte Sicherheitsvariante oft nicht bekannt
- Problem analog der Adaption https vs http – erst ein “Sicherheits-Gau” (Snowden) und der automatische Test und die Bevorzugung von https in den Browsern brachte den Durchbruch.
- Seit 1/2020 auch keine unsicheren https-Seiten mehr akzeptiert
- Die aggressive Einführung von Two-Factor Authentication über Apps etc. in den letzten zwei Jahren (z.B. Banking) lässt derzeit kein Unsicherheitsgefühl aufkommen.

# Vielen Dank für Ihre Aufmerksamkeit!

Klaus Landefeld  
Stellv. Vorstandsvorsitzender  
Vorstand Infrastruktur und Netze

eco Verband der Internetwirtschaft e.V.  
Französische Strasse 48  
10117 Berlin

