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

15. BDCS, Bonn, 29. Oktober 2020

Motivation

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

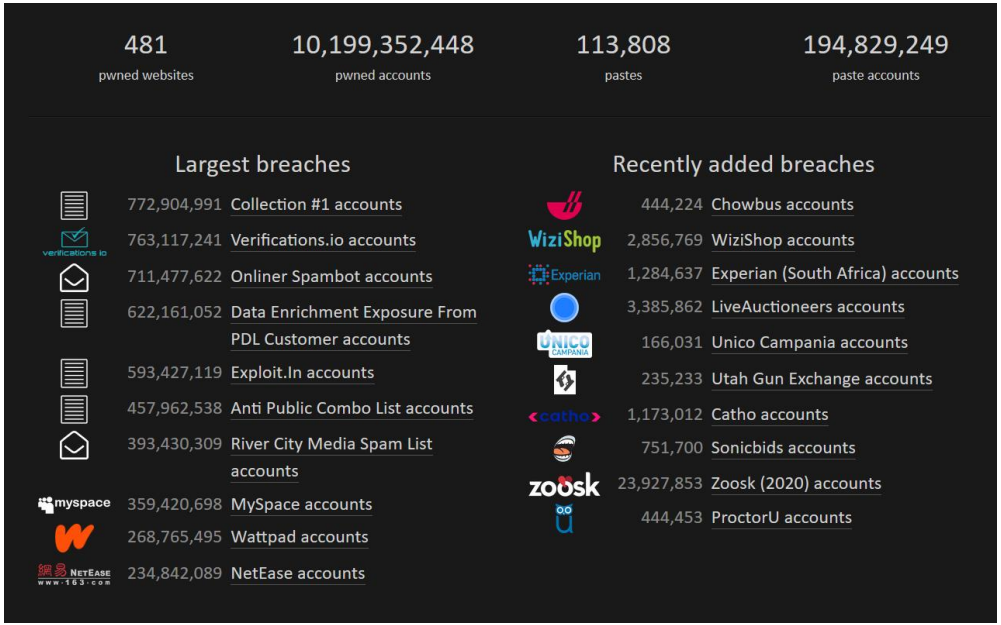
		Länge des Passworts						
Zeichensatz	Chars	8	12	16	20	24	28	32
Alphanumeric + Specials	94	6.10E+15	4.76E+23	3.72E+31	2.90E+39	2.27E+47	1.77E+55	1.38E+63
Base64	64	2.81E+14	4.72E+21	7.92E+28	1.33E+36	2.23E+43	3.74E+50	6.28E+57
Alphanumeric	62	2.18E+14	3.23E+21	4.77E+28	7.04E+35	1.04E+43	1.54E+50	2.27E+57
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

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.

Risko und Geschäftsmodell in einem

- Weitere Stärkung der Platformen
- Erhöhte usability, aber deutlicher User Lock-In
- Abhängigkeit weiterer Webdienste von der Datenerhebung und Zulieferung durch Platformbetreiber

- 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 (Biometic), 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 Autenticator

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 Autentiction Services hinterlegt werden
- Im WebAuthn/FIDO2 Standard wird ein TLS Tunnel zum “Durchreichen” der Authentication zwischen Endgerät und Diensteanbeiter 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

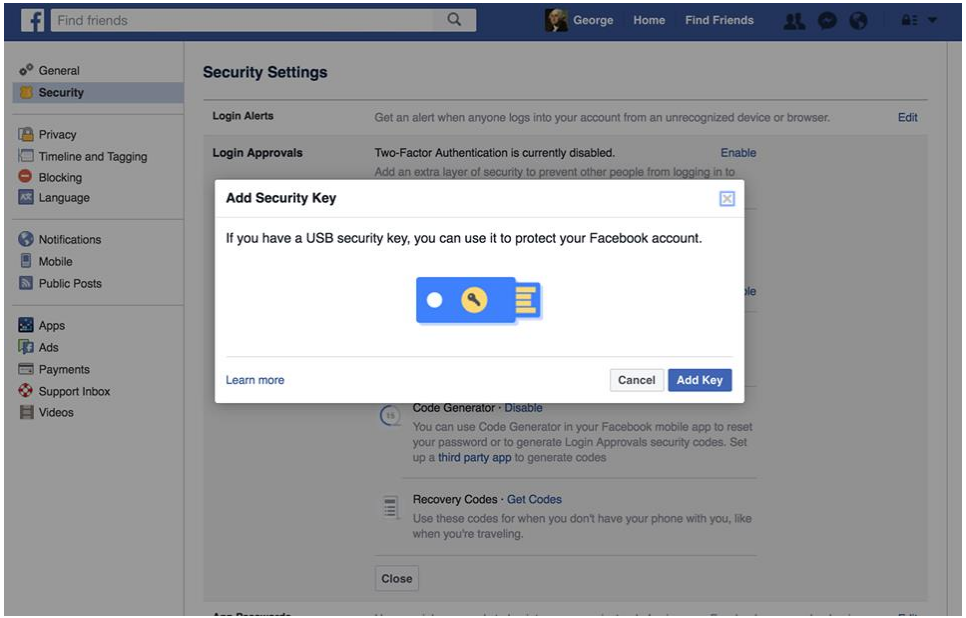
- Fehlende TPMs in Kundenrechnern
- TPM ist Standard in mobile Geräten, bei Notebooks dringend empfohlen (z.B. für Festplattenverschlüsselung)
- TPMs als externe Geräte

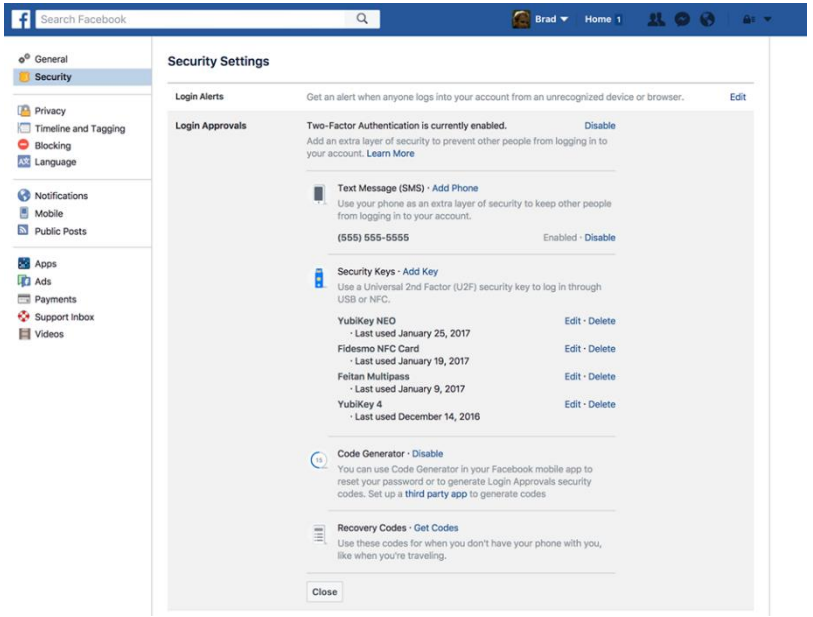
Externe Authenticators (CTAP-Erweiterung)

- Mit/ohne Fingerabdruck
- USB, Bluetooth, NFC verfügbar

- YubiKey
- Thetis
- Google Titan Security Key
- SoloKeys
- CryptoTrust
- Kensington
- u.v.a.m.

Registrierung beim Dienst





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	Lsreh7Crm55w1oj3abBBDMQ6Bdpc4SXjIn3O7luKHNQ=	-----BEGIN RSA PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6Z/VObbL0Yniwd3W5gFrdF5amJQfLuLUqqPXtFuGHn9zppCE8pppe54nT5p9UJjVxx1xPttvGm1AP04VbOooc0n5yRmNK53Z8AjgbjyirXKKU5wZE3Rsa3GS+DXbGIgBi9/NKNb52s1/YTZNH2oxfX41KDYart/qk2sJbIKw7vQU7WiEV1z5pEimXN+QM1QLMJ/6ullAaEosNCMhyYZh4g2pYONquMcdEFknlJESPfHGvGvEtimJGeUXr8xBMyo7hz3asGNPIp5//YskGviMmHkTwuJvyp1D7yR8lvEmBaV/IbG0yR42dR10s0D45LfU1DDK9uGBiNj7059i/36spwIDAQAB -----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