Zwei Faktor Authentifizierung

Eine Übersicht

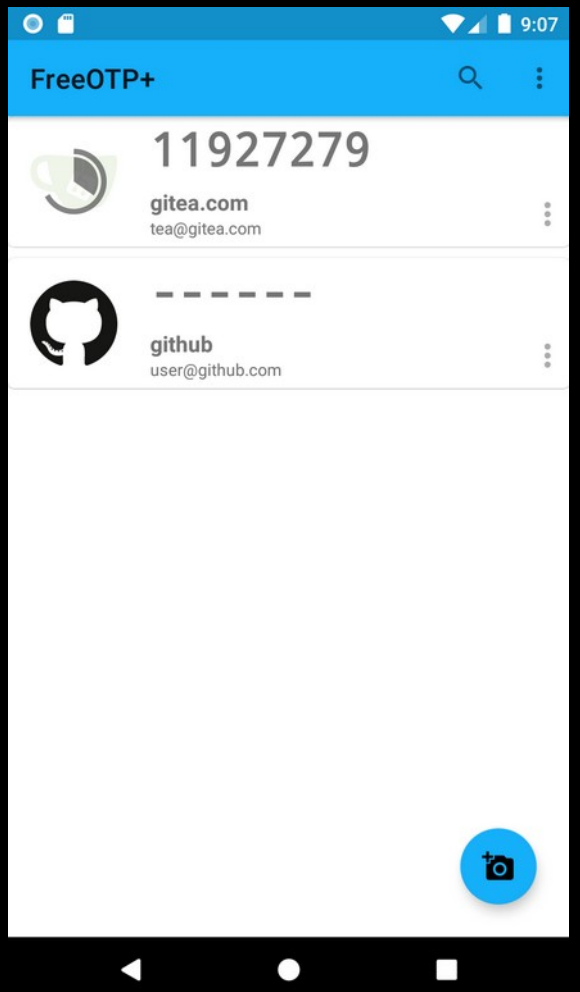
- Warum n > 1 Faktoren?
- Übersicht der 2FA Mechanismen
- Übersicht der Softwarelösungen
- Übersicht der Hardwaretokens

Warum n > 1 Faktoren?

- Vorteile
  - Angreifer muss mehrere Faktoren stehlen bzw. kompromittieren
  - Sichert Wiederverwendung von Passwörtern ab => Kein Passwortmanager notwendig
- Nachteile
  - Mehraufwand
  - Backup/Recovery Faktor notwendig
    - Entfernung ohne 2FA wäre ein Sicherheitsproblem
  - Schützt nur begrenzt bei kompromittiertem PC

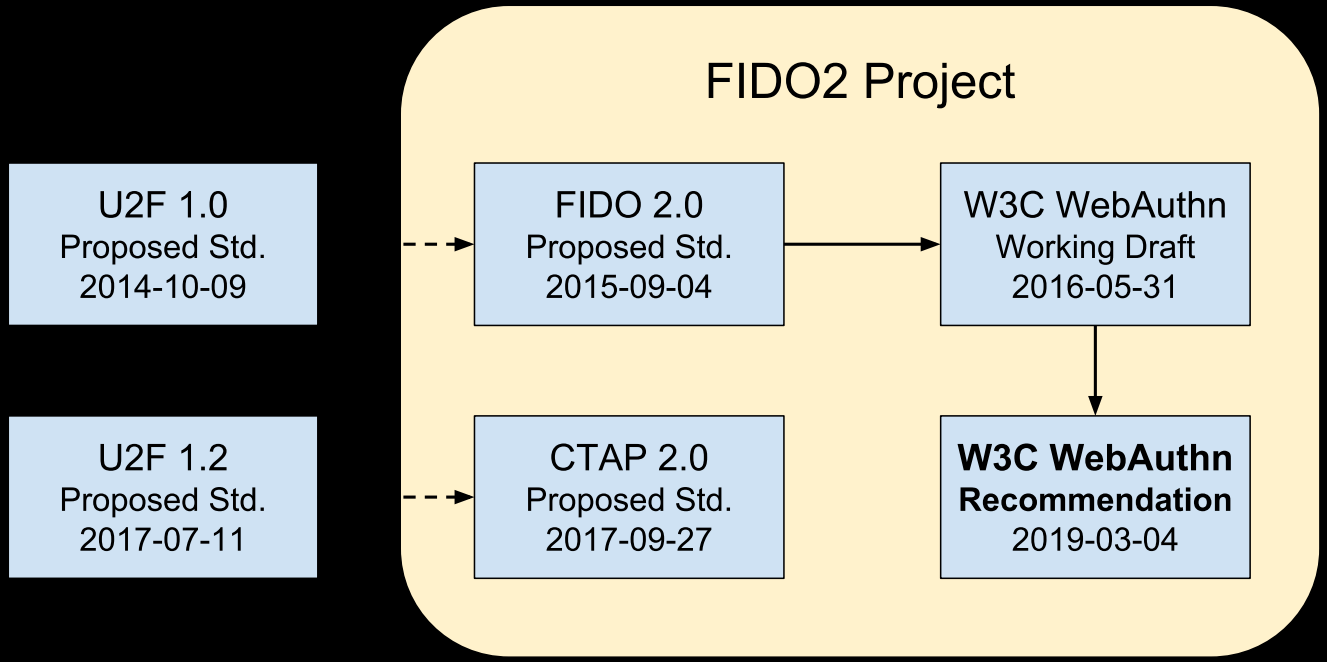
One Time Password

- Idee: Ein einmalig gültiger Token pro Login
- Umsetzungen:
  - (Recovery-)Tokenliste
  - HOTP (RFC 4226)
    - HMAC aus Secret und Counter
  - TOTP (RFC 6238)
    - HMAC aus Secret und aktueller Zeit
    - Sehr häufig anzutreffen
  - Token per E-Mail/SMS



FIDO2

- Standardisierte Möglichkeit für 2FA auf Webseiten, die auch HW-Tokens unterstützt
- Abwärtskompatibel zum Vorgänger U2F



FIDO2

- Besteht aus zwei Komponenten
  - W3C WebAuthn: JS-API für den Browser
  - CTAP2: Kommunikationsprotokoll für HW-Tokens
- Noch nicht so weit verbreitetet
  - Übersicht: https://2fa.directory/
  - Häufig bieten Webseiten nur TOTP, SMS oder spezielle Apps an

PKCS #11 / PIV (FIPS 201)

- Standardisiertes Verfahren zur Ansteuerung kryptografischer Tokens
- Token speichert privaten Schlüssel
- Signieren/Entschlüsseln benötigt 2FA
  - PIN und PUK (begrenzte Anzahl an Versuchen)
  - Fingerabdrucksensor
- Nutzung häufig außerhalb vom Browser
  - Signierung von E-Mails/Software/TLS-Certs
  - macOS Login, OpenSSH Login

OpenPGP Smartcard

- Ähnlich wie PKCS #11, nur speziell für OpenPGP
- Hat drei Slots für je einen Key
  - Entschlüsseln
  - Signieren
  - Authentifizieren
- Wird by default von gpg unterstüzt
- Smartcard kann Public-Key nicht speichern, kann lediglich als URL angegeben werden

OTP Smartphone-Apps

- FreeOTP+
  - Fork von der nicht weiterentwickelten FreeOTP-App von RedHat
  - Unterstützt HOTP und TOTP
- KeePassDX
  - Unterstützt HOTP und TOTP
- Google Authenticator
  - Wird häufig von Webseiten angegeben, wenn diese TOTP nutzen

FIDO2 auf Smartphones

- Android unterstüzt mittels der proprietären Play Services FIDO2
- Es können die üblichen Anmeldeverfahren als zweiter Faktor genutzt werden
- Alternativ kann auch ein Hardware Token mit NFC genutzt werden
- Wird leider (noch) nicht von micoG unterstützt

FIDO2 auf Windows

- Unter Windows kann über Edge Windows Hello als FIDO2-Provider genutzt werden
- Kann somit alle Windows Hello Möglichkeiten als zweiten Faktor nutzen
  - PIN
  - Fingerabdruck
  - Gesichtserkennung

Yubikey

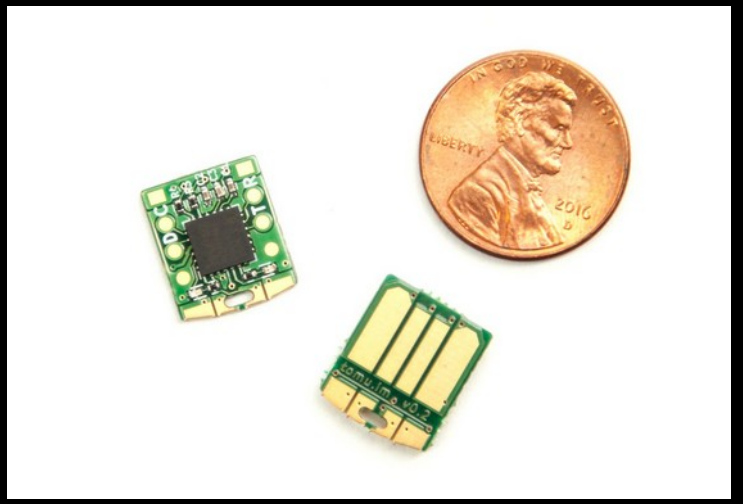
- Wohl die bekanntesten 2FA Hardware Tokens
- Lediglich die Client-Software ist komplett OSS
- Stellen für quasi alle Anwendungen Anleitungen und Software bereit
- Preis: 45 – 85€, 20€ für FIDO2 only (blau)
- Funktionen:
  - HOTP, TOTP, Yubikey spezifisches OTP
  - FIDO2 Token
  - PIV / PKCS #11 und OpenPGP Smartcard

Nitrokey

- In Deutschland entwickelt und produziert
- Komplett Open Source und Open Hardware
- Preis: 29 – 109€
- Funktionen (abhängig vom Stick):
  - TOTP, HOTP
  - FIDO2 Token
  - PKCS #11 und OpenPGP Smartcard
  - Passwortmanager
  - Verschlüsselter Storage mit abstreitbarem PW

Tomu

- Bastelprojekt mit einem ARM-Microcontroller, der einfach direkt per USB angeschlossen ist
- Keine garantierte Sicherheit
- Preis: Zum Selbstbau gedacht,
  aktuell $25 für einen fertig assemblierten Stick
- Funktionen: U2F, FIDO2 ?



Solokey

- Komplett Open Source und Open Hardware
- Gibt es als „Hacker“-Version, um eigene Firmware zu nutzen
- Preis: 20 - 25€
- Funktionen: U2F, FIDO2