Sicher Authentisieren

Cornelius Kölbel
@cornelinux
cornelius.koelbel@netknights.it

FFG2017 – GUUG – 24.03.2017

Vorstellung

- 2005: Smartcards, eToken, M$ CA
- 2005: RFC 4226
- 2006: erstes OTP OSS Produkt
- 2007: iPhone 1
- 2009: Produktmanager 2FA-Lösung
- 2014: privacyIDEA

Hackerangriff

68 Millionen Dropbox-Passwörter gestohlen

Stand: 01.09.2016 11:25 Uhr

Hacker sind an 68 Millionen Passwörter von Kunden des Online-Speicherdienstes Dropbox gelangt. Das hat das Unternehmen nun bestätigt. Betroffen sind Dropbox-Nutzer, die zuletzt vor Mitte 2012 ihr Passwort geändert haben.

Der Online-Speicherdienst Dropbox hat bestätigt, dass ihm höchstwahrscheinlich im Jahr 2012 über 68 Millionen verschlüsselte Passwörter gestohlen wurden. Bisher gebe es keine Anzeichen für

AUS DEM ARCHIV

Passwörter von Telekom-Kunden i
27.06.2016

Nach Hackerangriff bei LinkedIn: D
gedacht, 19.05.2016

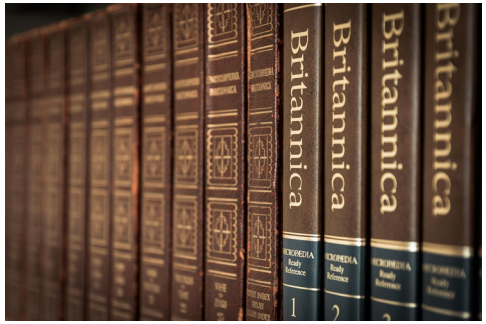
Medienbericht: Hacker erbeuten M
06.08.2014


Das Passwort ist tot
Nun Ja, es hat Unzulänglichkeiten!

Partnerwahl

Zwei-Faktor-Authentifizierung

Besitz



Passwort

Eigenschaft

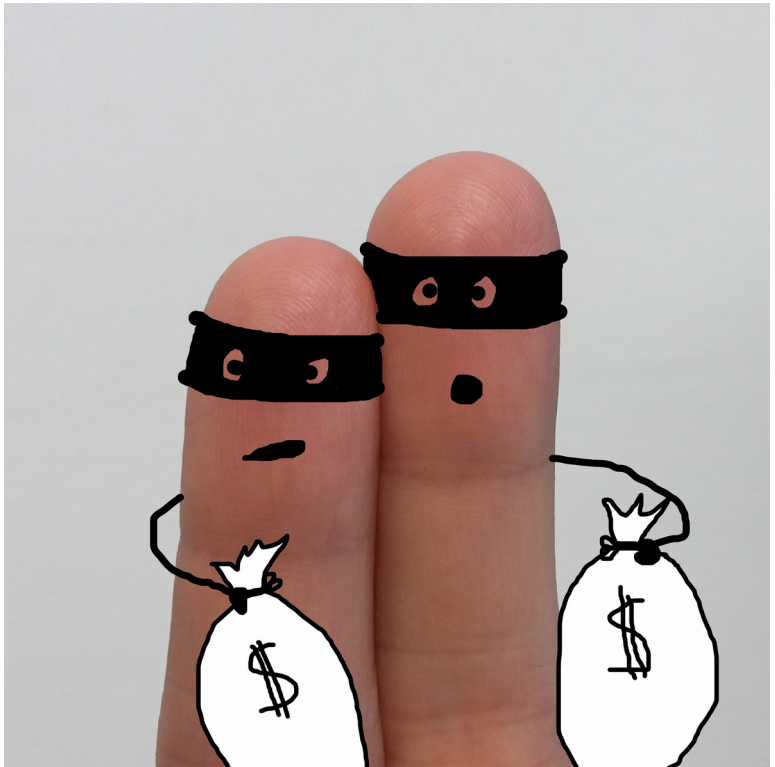
Sinn von 2FA

- Foto

Skillprofil!

Anforderungen an Faktoren

- Eindeutig → Nicht kopierbar
- Verlust sollte bemerkbar sein
- Revozierbar / Neu ausstellbar



Besitzfaktor

- Smartphone (SMS)
- OTP AES/HOTP
- OpenPGP Smartcard
- PIV (x.509) Smartcard
- U2F

„OOB using SMS is deprecated, and may no longer be allowed in future releases of this guidance.“

NIST.
Draft Digital Authentication Guideline SP800-63B

Besitzfaktor

- ~~Smartphone (SMS)~~
- OTP AES/HOTP
- OpenPGP Smartcard
- X.509 Smartcard
- U2F

Einzigartigkeit

des zweiten Besitz-Faktors

HOTP

- RFC 4226
  - HMAC-SHA1, Truncating
  - Secret Key, Counter
- Tastatur


```
ykpersonalize -1 -a
313233343536373839303132333435363737
83940 -oappend-cr -ooath-hotp
```

OTP Yubico Mode (AES)

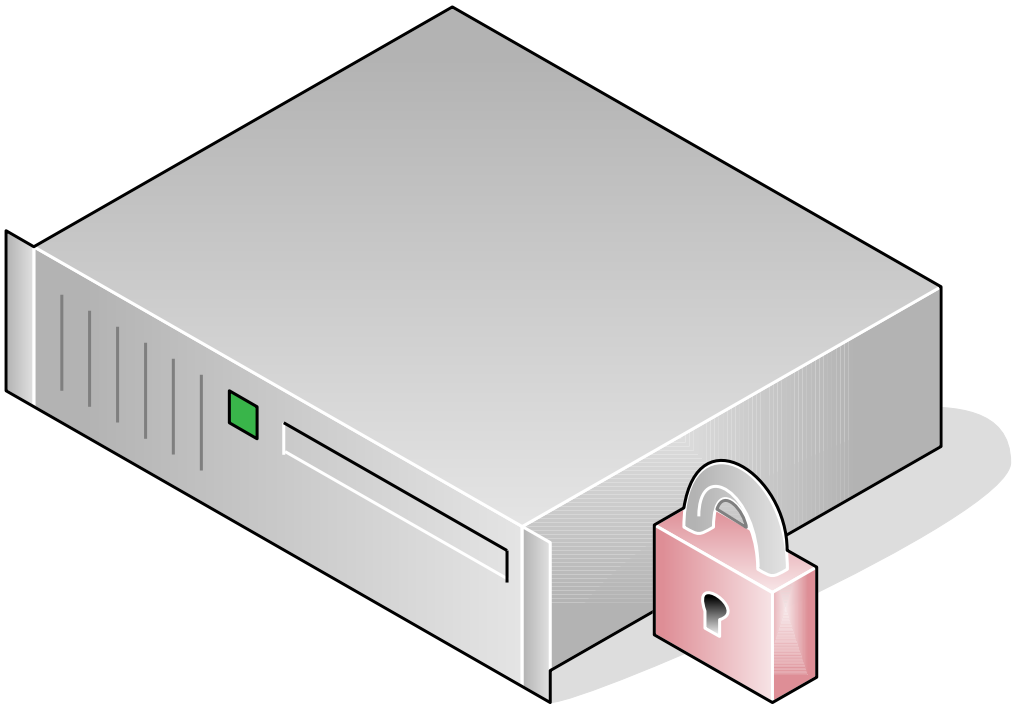
- Tastatur
  - Steck Counter
  - Press Counter
  - ID
  - Werden mit sym. Key AES-128 verschlüsselt

```
ykpersonalize -1 -a
31323334353637383930313233343536
-oappend-cr
```

OTP Backend

Yubico-AES und HOTP

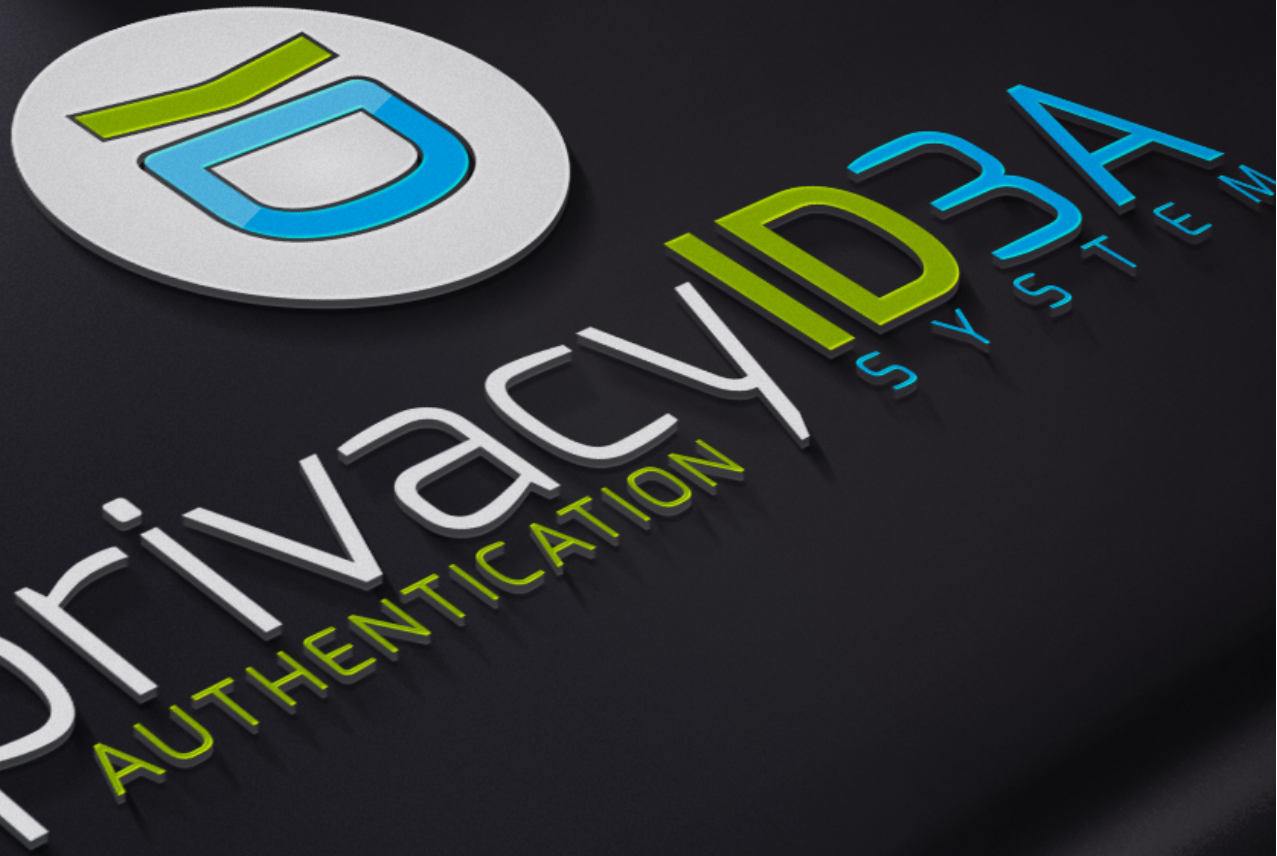
- Symmetrischer Key für Yubico-AES und HOTP
- => Backend-System nötig oder pam_google_auth



privacyIDEA

Authentication System

- Das aktivste Open Source 2FA Projekt auf Github
  - 20 Contributors
  - 640 Issues
  - 1923 Commits
  - 77 Pull Requests
  - **220 Stars**



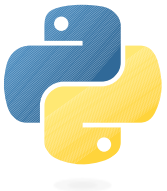
privacyIDEA

Ein eigenes 2FA System

- On Premise
- Schlüsselmaterial kann erzeugt werden
- Unterstützte Algorithmen (HOTP, TOTP, mOTP, TiQR/OCRA, RSA)
- Webservice mit gut dokumentierter “REST” API
  - Flask / Python / Token-DB

privacyIDEA
AUTHENTICATION SYSTEM

Flask
web development,
one drop at a time



python™

privacyIDEA

unterstützte Authentifizierungsobjekte

- Key-fob Tokens
- OTP Karten
- SMS, Email, Smartphone
- Yubikey
- U2F
- eToken NG/OTP
- SSH Keys
- x.509-Zertifikate
- ...

Überblick OTP

- Keine Treiber: Ja
- Heterogen: Ja
- Geeignet für lokale Anwendung: Nein
- Geeignet für Verschlüsselung: Nein
- Leichte Benutzung: Ja

OpenPGP

- GnuPGP

  /
  home/cornelius/.gnupg/scdaemon.conf

  gpg --card-status

OpenPGP

Lokale Anmeldung

- Einbindung in PAM-Stack mit libpam-poldi

  `/etc/pam.d/common-auth`

- Benutzer-Mapping in

  `/etc/poldi/localdb/keys/`

  `/etc/poldi/localdb/users`

PIV (x.509) Smartcard

- X.509 → CA → Business ;-)
- PIV-Manager (Personal Identity Verification)
  - 9a is for PIV Authentication
  - 9c is for Digital Signature (PIN always checked)
  - 9d is for Key Management
  - 9e is for Card Authentication (PIN never checked)

```
pivman

yubico-piv-tool -k
010203040506070801020304050607080102030405060708 -a generate -s 9c
```

Siehe: https://developers.yubico.com/yubico-piv-tool/YubiKey_PIV_introduction.html
https://www.yubico.com/why-yubico/for-businesses/computer-login/yubikey-neo-and-piv/

Überblick Smartcard

- Keine Treiber: Nein
- Heterogen: Jein
- Geeignet für lokale Anwendung: Ja
- Geeignet für Verschlüsselung: Ja
- Leichte Benutzung: Nein

Gegen Account-Phishing

Facebook unterstützt Yubikey und Fido U2F Token

30.01.17 | Autor / Redakteur: Moritz Jäger / Peter Schmitz

Wer sein Facebook-Konto gegen ungewollten Zugriff schützen möchte, kann ab sofort aktuelle YubiKeys und U2F-Token für die Zwei-Faktor-Anmeldung nutzen. Per NFC klappt das auch mit der mobilen App.

Facebook führt eine zusätzliche Methode zur Zwei-Faktor-Authentifizierung für Nutzer ein. Ab sofort unterstützt das soziale Netzwerk Sicherheitsschlüssel – Hardware-Token, die bei Berührung eine komplex generierte Kombination aus Buchstaben und Zahlen übertragen. Unterstützt werden aktuelle Yubikeys mit Fido U2F Zertifizierung. Darüber hinaus lassen sich alle anderen Hardware-Token nutzen, die Universal 2nd Factor (U2F) unterstützen.

Facebook reiht sich damit in eine Reihe von Dienste ein, die neben SMS oder App-Kennwörtern auch Hardware-Token für die Authentifizierung nutzen. Dazu gehören beispielsweise LastPass, Google, Salesforce, Bitbucket oder Dashlane.

Quelle: security-insider.de

Was ist U2F und wieso hat es sich immer noch nicht durchgesetzt?

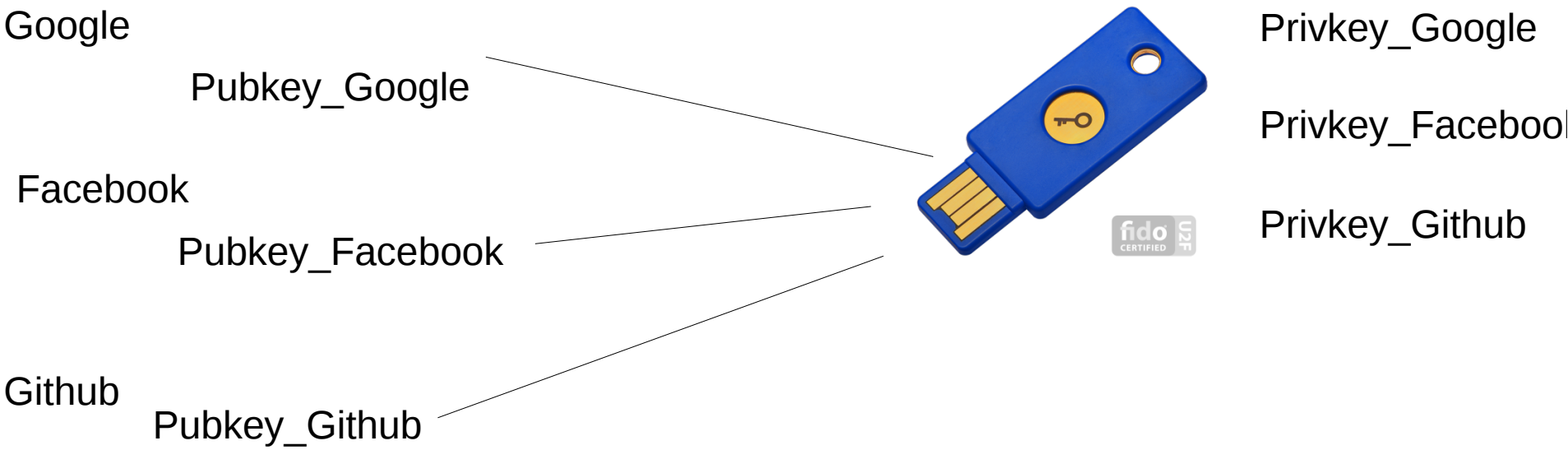
Universal 2nd Factor

- FiDO Alliance (Fast iDentity Online)
  - Universal Authentication Framework (UAF)
    Bspw. **Biometric** am lokalen Gerät
  - Universal 2nd Factor (U2F)
    Zusätzlich zum Passwort ein Besitz von Hardware zur Anmeldung an **Webseiten**.

https://fidoalliance.org/approach-vision/

Wie funktioniert U2F?

- Public Key Crypto
- Keine zentrale Instanz



Probleme mit U2F

- Keine bei Benutzern!
- Keine Unterstützung der Webseiten
- Schlechte Unterstützung der Browser
- Ggf. Masterkey

Überblick U2F

- Keine Treiber: Ja
- Heterogen: Ja
- Geignet für lokale Anwendung: Jein
- Geignet für Verschlüsselung: Nein
- Leichte Benutzung: Ja

Vergleich OTP / SC / U2F

	OTP	Smartcard	U2F
Keine Treiber	Ja	Nein	Ja
Heterogen	Ja	Jein	Ja
Lokale Anwendung	Nein	Ja	Jein
Verschlüsselung	Nein	Ja	Nein
Leichte Benutzung	Ja	Nein	Ja

Vielen Dank

- @cornelinux, @privacyidea
- https://netknights.it
- https://privacyidea.org
- Cornelius.koelbel@netknights.it