YubiKey und Nitrokey - oder allgemein Security Keys (Work in Progress)

Matthias Brüstle

Nürnberg 2024-11-24

Was sind denn das?

- Dongles auf denen man geschützt Schlüssel und Passwörter speichern kann
- Schlüssel verlassen den Dongle nicht
- Verwendung für Authentisierung und Verschlüsselung

Übersicht

YubiKey 5

- https://www.yubico.com
- USB-A, USB-C, USB-A+NFC, USB-C+NFC, USB-C+**Lightning**
- USB-A und USB-C als fitzelig
- Präsenztaste
- RSA bis 4096 bits
- EC (normal und *25519)
- so grob 50 – 90 €

Nitrokey 3

- https://www.nitrokey.com
- USB-A, USB-C, USB-A+NFC, USB-C+NFC
- USB-A als fitzelig
- Präsenztaste
- RSA bis 4096 bits
- EC (normal und *25519)
- um 50 €
- Auch leer für Eigenentw.

Und andere?

- Ja, gibt es.
- Reine FIDO-Keys
  - Sind für mich nicht interessant
  - Mit einem reinen FIDO Use Case kann man damit Geld sparen
- Andere Hersteller
  - YubiKey und Nitrokey haben das beste Info-Material
  - Zwei reichen erstmal
- Haufen anderes Zeug (Fingerprint, FIPS, HSM, ...)

Innere Werte

YubiKey 5

- Infineon M7893
- CSPN-zert.? ("CC EAL2")
- FIPS Level 1 und 2
- Keine Firmwareupdates
- 100 Passkeys
- 24 PIV*-Zertifikate
- 3 PGP-Schlüssel
- 64 OATH-Schlüssel
- 2 OTP-Schlüssel

Nitrokey 3

- GnuPG/(PIV): NXP JCOP 4 SE050M (CC EAL6+)
- Alles übrige: nRF52
- Firmwareupdates
- ca. 50 Passkeys
- (PIV-Zertifikate) "unstable"
- 3 PGP-Schlüssel
- OATH-Schlüssel
- 2 OTP-Schlüssel

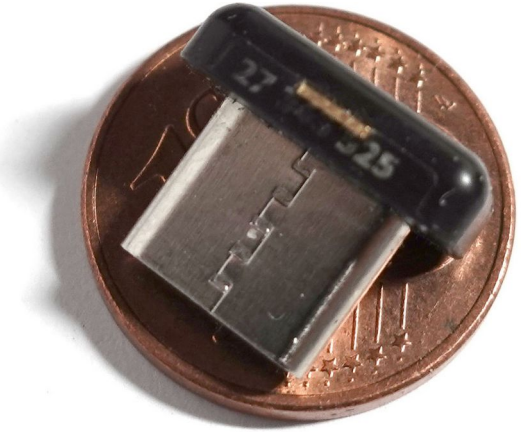
* Personal Identity Verfication – FIPS 201

EUCLEAK

- https://eprint.iacr.org/2024/1380
- Betroffen: Sicherheitscontroller von Infineon (vgl. ROCA)
- Analyse der elektromagnetischen Abstrahlung
- Erfolgreicher Angriff der ECDSA-Signaturerstellung
- "Sensitive modular inversions are not exclusively found in the ECDSA scheme. It would be interesting to look at the RSA (and especially the key generation) and study the application of EUCLEAK there."
- YubiKey 5 sind ab Firmware v5.7 gegen EUCLEAK abgesichert.
- YubiKeys werden oder wurden anscheinend mit alter Firmware abverkauft.
- Ein Sicherheitscontroller mit Schwachstelle wird sicherer sein als ein normaler Microcontroller (wenn die Softwarequalität sonst gleich ist)

Präsenzerkennung

- Für einige Funktionen wird eine Präsenzerkennung unterstützt
- Kapazitive Sensoren, die bei Bedarf berührt werden müssen, z.B. Authentisierung



Btw. der Nitrokey hat einen richtigen USB-Stecker!

Konfiguration – YubiKey 5

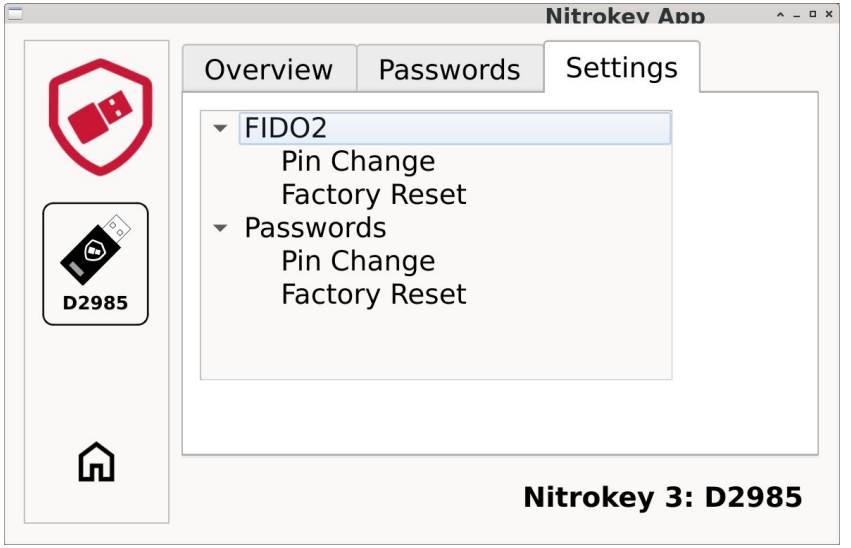
- https://docs.yubico.com/software/yubikey/tools/ykman/intro.html
- YubiKey Manager (CLI und GUI)
- Funktionierender YubiKey Manager (CLI und GUI) ab Debian 12
- ykman info

```
Device type: YubiKey 5 NFC
Firmware version: 5.7.1
Form factor: Keychain (USB-A)
Enabled USB interfaces: OTP, FIDO, CCID
NFC transport is enabled.

Applications USB      NFC
OTP          Enabled  Disabled
FIDO U2F     Enabled  Disabled
OpenPGP      Enabled  Enabled
PIV          Disabled Disabled
OATH         Enabled  Disabled
FIDO2        Enabled  Disabled
```

Konfiguration – Nitrokey 3

- https://docs.nitrokey.com/de/software/
- GUI: nitrokey-app (v2)
- CLI: nitropy
- Debian 11 und 12: Pakete nicht für Nitrokey 3, aber nitrokey-app2 binary läuft unter Debian 12 https://github.com/Nitrokey/nitrokey-app2/releases
-
```
$ nitropy nk3 status
Command line tool to interact
   with Nitrokey devices 0.4.50
Firmware version:   v1.7.2
Init status:        ok
Free blocks (int):  235
Free blocks (ext):  468
Variant:            NRF52
```



2FA / FIDO2

- Wo kann ich Second Factor bei meinen (wichtigeren) Konten verwenden:
  - Amazon: TOTP
  - Discord: TOTP, Security Key
  - ebay: TOTP
  - Halbleiterlieferant: TOTP
- Keine Ahnung warum mir Amazon und ebay kein FIDO2 anbietet, obwohl es gehen soll
- FIDO2-Testwebsite hat funktioniert
- Ich hab keinen Use Case für FIDO2

Aber ... ssh mit FIDO2, kinda

```
ssh-keygen
  -t ed25519-sk (Schlüsseltyp)
Alles weitere optional
  -O resident
# -O verify-required (PIN wird abgefragt, sonst nicht)
# -O no-touch-required (Keine Präsenzprügung, aber login pwd nötig)
  -O "application=ssh:$name" (Schlüsselname auf dem Security Key)
  -f "$HOME/.ssh/id_ed25519_sk_$name" (Zieldatei für Schlüsselinfo)
  -C "sk_$name" (Kommentar am Ende des öffentlichen Schlüssels)
```

Aber ... ssh mit FIDO2, kinda

- Das Private Key File von ssh kann man noch mit einem Passwort schützen
- Private Key File???
  "the private key file does not contain a highly-sensitive private key but instead holds a "key handle" that is used by the security key to derive the real private key at signing time."
  https://undeadly.org/cgi?action=article;sid=20191115064850
- Keine Konfiguration und keine spezielle Software nötig
- Wie normales login, Key kurz antippen, drin => Total Easy!
- Obwohl "FIDO2" können das keine reinen FIDO-Keys, auch kein ecdsa-sk
- Geht aber nicht mit allen Gegenstellen, weil nicht jeder ed25519 oder ECDSA spricht

Und ssh ohne FIDO

PIV

- Benötigt den Agent pivy-agent
  - Selbst compilieren
  - Geht nur mit ECDSA
- oder yubikey-agent
  - ggf. noch installieren

GPG (OpenPGP Card)

- Benötigt nur den Agent gpg-agent
- Den hat man wahrscheinlich, wenn man GnuPG hat
- Unterstüzt RSA und damit vermutlich alle Gegenstellen

ssh mit gpg etwas genauer

- Das OpenPGP-Applet wird fast ausschließlich mit gpg verwaltet
- Dafür muß man mit GnuPG in der shell zurechtkommen
- Keine Softwareinstallation
- Konfiguration nur in GnuPG und ssh
- Installation mitteleinfach oder eher mittelschwer
- Für Verwendung nur PIN eingeben
- Geduldig, wenn der Security Key nicht steckt
- Nitrokey 3: Schlüssel sind von EAL6+-zertifizierter JavaCard geschützt

ssh mit gpg etwas genauer (2)

- Am besten Schlüssel erst im GnuPG erzeugen
- Dritten Authentisierungsschlüssel für ssh hinzufügen
- Schlüsselbackup machen wegen den nicht-ssh-Schlüsseln
- Auch die öffentlichen Schlüssel aufheben, da sie sich anscheinend nicht von dem Security Key ziehen lassen
- Schlüssel auf den Key verschieben(!) mit keytocard
- PINs setzen nicht vergessen
- Mit keygrip das use-for-ssh-Attribut setzen
- Tip: In config den Agent mit `IdentityAgent` setzen

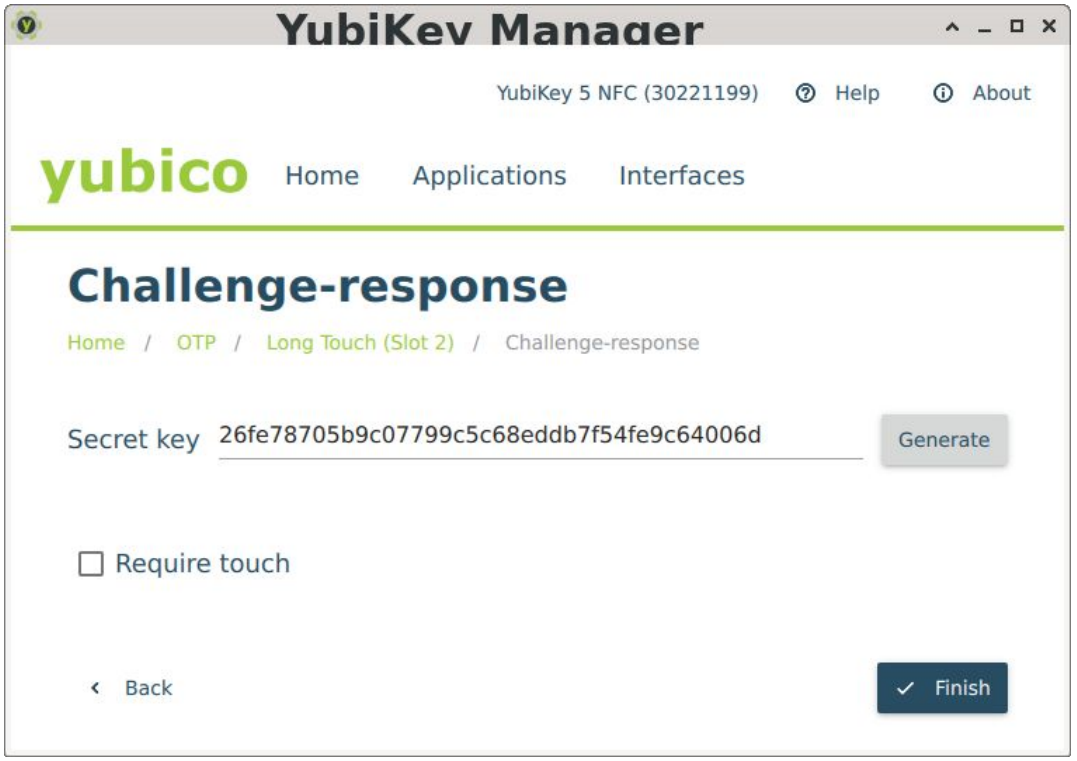
gpg

- Wer ssh mit gpg eingerichtet hat, kann sofort gpg nutzen
- Deswegen das vorhin empfohlene Backup
- Thunderbird konfigurieren
  - mail.openpgp.allow_external_gnupg = true
  - Privaten Schlüssel löschen (über Umwege)
  - "Use your external key through GnuPG"
  - Ggf. pinentry konfigurieren
- Funktioniert auch unter Android mit openkeychain
  - mit USB, bei YubiKey auch mit NFC
  - USB: bei mir kein virtuelles Keyboard mehr (HID)
- Festplattenverschlüsselung (Anleitung für dm-crypt/LUKS)

Challenge/Response

- 2 Passwort-Funktionen durch kurz und lang Berühren des kapazitiven Sensors
- Am besten lang, weil das nicht so aus Versehen passiert
- Der Slot kann mit Challenge/Response belegt werden
- Beim Anlegen gleich ein Backup des Keys machen
- HMAC-SHA1 mit 160bit-Key
- Wird als Hardware Key von keepassxc akzeptiert
  - Bei jedem Speichern erzeugt keepassxc eine neue Challenge
  - Die immer andere 160bit-Response wird als als Schlüssel verwendet
  - Kombinbierbar mit Passphrase und Schlüsseldatei

Challenge/Response (2)



Nochmal in der Übersicht

- 2FA/FIDO2
- HOTP-, TOTP-, Password-Challenge/Response-Authentisierung
- OpenPGP-Card
  - login
- PIV (FIPS 201) / S/MIME
- Festplattenver-schlüsselung
- Secure Shell (ssh)
  - passkey/Ed25519
  - GPG
  - PIV
- keepassxc
  - Challenge/Resp.

Und noch ein paar Debian-Pakete zur Inspiration

- freeradius-yubikey - Yubikey module for FreeRADIUS server
- glewlwyd - Single-Sign-On server with multiple factor authentication
- libpam-yubico - two-factor password and YubiKey OTP PAM module
- ykcs11 - PKCS#11 module for the YubiKey PIV applet
- yubikey-luks - YubiKey two factor authentication for LUKS disks
- yubiserver - Yubikey OTP and HOTP/OATH Validation Server

Unterschiede zwischen YubiKey und Nitrokey auf einem Blick

YubiKey

- Ausgereiftere und umfangreiche Software
- Mehr Hardware-Varianten
- Sicherheitshardware für alles
- keine Firmware-Updates
- Closed Source

Nitrokey

- Mehr OpenSource
- Firmware-Updates
- Zertifiziertes SE fuer GPG
- Richtiger USB-A-Stecker
- Standard-Controller für die meisten Funktionen
- Weniger ausgereifte und umfangreiche Software

Was läuft bei mir? Oder auch nicht?

- Technisch geht das beschriebene alles, aber wie verwendet man es?
- Stecken lassen oder abziehen?
  Aktuelles Ziel abziehen, aber ich vergesse es dauernd.
- Wie ist eine Verwendung mit keepassxc praxistauglich?
  Aktuell mit Auto-Logout, aber dann werden neue Passwörter nicht gespeichert.
  Unsicher wie man keepassxc grundsätzlich verwendet.

Was läuft bei mir? Oder auch nicht? (2)

- Secure Shell: Mit OpenPGP-Card. Funktioniert gut. Müsste nur mal endlich alles umstellen.
- E-Mail-Verschlüsselung mit GPG: Funktioniert gut. UI ist geduldig, wenn der Key nicht steckt.
- Festplattenverschlüsselung: Noch nicht ausprobiert.
- Web-Authentisierung: Nutze ich nicht. TOTP-App für ein paar Web-Dienste. Deswegen sind für mich reine FIDO-Key nutzlos.

Noch ein paar Tips

- Planen was man machen möchte, dann die passenden Keys raussuchen
- Man kann auch mehrere Keys verwenden (unterschiedliche Arbeitsbereiche, Zwecke), z.B. eigener Key für Login auf Backup-Rechner
- Karabinerhaken sind ganz praktisch

Links

- YubiKey
  - https://www.yubico.com
  - https://support.yubico.com/hc/en-us/
  - https://developers.yubico.com/
  - https://docs.yubico.com/hardware/yubikey/yk-tech-manual/index.html
  - Übersicht: https://marcusb.org/posts/consolidated-yubikey/
- Nitrokey
  - https://nitrokey.com
  - https://docs.nitrokey.com/nitrokeys/nitrokey3/
  - https://docs.nitrokey.com/de/software/

Links (2)

- GPG
  - https://developers.yubico.com/PGP/
  - https://developers.yubico.com/PGP/PGP_Walk-Through.html
  - https://developer.okta.com/blog/2021/07/07/developers-guide-to-gpg
  - https://docs.nitrokey.com/nitrokeys/features/openpgp-card/
  - https://github.com/Nitrokey/SmartPGP
  - Thunderbird: https://strobelstefan.de/blog/2023/12/06/thunderbird_openpgp_ready_-_e-mails_verschl%c3%bcsseln_und_signieren/

Links (3)

- PIV
  - https://github.com/FiloSottile/yubikey-agent
  - https://github.com/arekinath/pivy
- keepassxc
  - https://docs.nitrokey.com/software/nk-app2/keepassxc
  - https://support.yubico.com/hc/en-us/articles/360013779759-Using-Your-YubiKey-with-KeePass
- LUKS-Festplattenverschlüsselung mit Linux
  - https://marcusb.org/posts/consolidated-yubikey/

YubiKey und Nitrokey - oder allgemein Security Keys

Matthias Brüstle

Nürnberg 2024-11-24