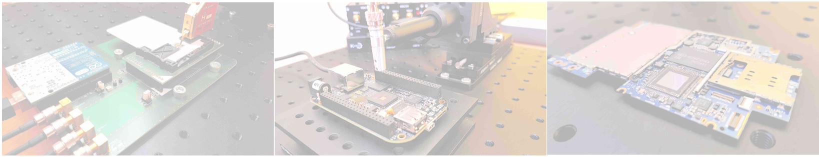
An Overview of the Security of Some Hardware FIDO(2) Tokens

Victor LOMNE

NinjaLab

Hardwear.io NL, The Hague, Netherlands
October 28, 2022



About Myself & this Talk

- Myself : co-founder & security expert @ **NinjaLab**
  - We are based in Montpellier, south of France
    - Cryptology
    - Side-Channel Attacks
    - Hardware security
- Roots of this talk :
  - Last year : publication of a SCA attack on **Google Titan Security Key**
    - Target the Titan Secure Element : NXP A7005
    - Then we bought a lot of different other HW FIDO tokens
      → Check which one use the same Secure Element
  - Today I share what we found inside these HW FIDO tokens
- Work in progress !
  - Note : this presentation has been updated with attendees remarks !

Agenda

1. FIDO(2) Protocol and Hardware Tokens

2. Partial Teardown of some FIDO(2) HW Authenticators

3. Other Interesting FIDO(2) HW Authenticators

4. Conclusions

Agenda

1. FIDO(2) Protocol and Hardware Tokens

2. Partial Teardown of some FIDO(2) HW Authenticators

3. Other Interesting FIDO(2) HW Authenticators

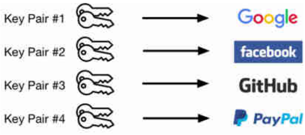
4. Conclusions

FIDO History

- **FIDO** initiative : open industry association
  - Goal : reduce reliance on passwords
    ⇒ thwart phishing attacks
  - Historically developed by Google, NXP and Yubico
  - Now hosted by **FIDO alliance**
- Concept : use of a second / strong authentication factor
  ⇒ *mobile app, HW token, . . .*
- Several specifications over time :
  - 2014 : U2F (Universal Second Factor)
    ⇒ renamed CTAP1 (Client To Authenticator Protocol)
  - 2014 : UAF (Universal Authentication Framework)
  - 2015 : FIDO2
  - 2016 : WebAuthn (W3C)
  - 2017 : CTAP2
- Today : FIDO2 = WebAuthn + CTAP2

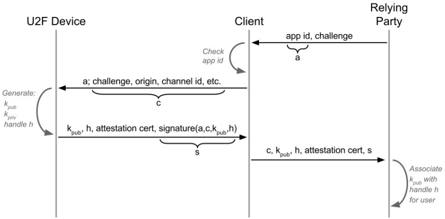
FIDO U2F / CTAP1

- In FIDO, three parties involved :
  - `Relying Party` (e.g. Google server)
  - `Client` (e.g. web browser)
  - `Authenticator` (e.g. mobile app, HW token, . . .)
- U2F / CTAP1 : protocol for communication with `Authenticator`
- Works in two phases : Registration & Authentication
- `Authenticator` stores two kind of key pairs :
  - Attestation key pair
    one per `Authenticator`
  - Credential key pairs
    one per web service :



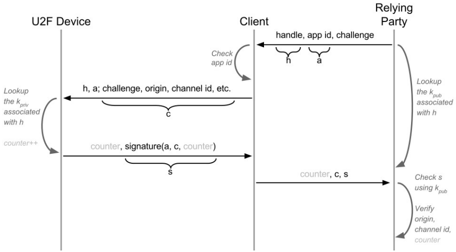
FIDO U2F / CTAP1 : Registration

1. `Client` contacts `Relying Party` for initiating Registration ceremony
2. `Relying Party` sends challenge to `Authenticator`
3. `Authenticator` generates an ECDSA Credential key pair
4. `Authenticator` sends back to `Relying Party` :
    - ECDSA Credential public key
    - Key handle (can contain wrapped Credential private key)
    - Attestation certificate
    - ECDSA Attestation signature (signed with Attestation private key)


U2F Device
Client
Relying Party
app id, challenge
a
Check app id
a; challenge, origin, channel id, etc.
c
Generate: k_{pub} k_{priv} handle h
k_{pub}, h, attestation cert, signature(a,c,k_{pub},h)
s
c, k_{pub}, h, attestation cert, s
Associate k_{pub} with handle h for user

FIDO U2F / CTAP1 : Authentication

1. `Client` contacts `Relying Party` for initiating Authenticat. ceremony
2. `Relying Party` sends key handle & challenge to `Client`
3. `Client` sends to `Authenticator`
   - Key handle & challenge
   - User presence control byte
4. `Authenticator` signs challenge w. Credential private key
5. `Authenticator` sends back ECDSA signature to `Relying Party`
6. `Relying Party` checks validity of ECDSA signature


U2F Device
Client
Relying Party
handle, app id, challenge
h
a
Check app id
Lookup the k_{pub} associated with h
h, a; challenge, origin, channel id, etc.
c
Lookup the k_{priv} associated with h
counter++
counter, signature(a, c, counter)
s
counter, c, s
Check s using k_{pub}
Verify origin, channel id, counter

FIDO U2F / CTAP1 : Optional Security Layers

- Attestation :
  - Each `Authenticator` should store an Attestation key pair
    - Allows to thwart *Man-in-the-Middle* attacks during Registration phase
    - Allows to prove genuineness of an `Authenticator` to `Relying Party`
  - Some `Authenticators` use self-signed Attestation certificate
  - Privacy requirement :
    → same Attestation key pair in several `Authenticators` of same model
    e.g. same Attestation key pair for 100k devices
- Counter :
  - A counter can be used for counting authentications
  - Counter stored in `Authenticator` & `Relying Party`
  - Allows to detect `Authenticator` clones
    But clone can connect until being discovered

FIDO2 = WebAuthn + CTAP2

- WebAuthn (W3C) : protocol between `Relying Party` & `Client`
- CTAP2 (FIDO alliance) : protocol between `Client` & `Authenticator`
- Main improvement : allows passwordless authentication
- Several possibilities :
  1. Strong 1FA with `Authenticator`
  2. 2FA with `Authenticator` + user presence
  3. Strong 2FA with `Authenticator` + PIN or biometry
  4. MFA . . .
- U2F / CTAP1 backward compatibility in FIDO2

FIDO Cryptography Signature Algorithms

- Provide authentication and non-repudiation
- FIDO U2F / CTAP1 :
  1. ECDSA on `NIST P256`
- FIDO2 :
  - During Registration : `Relying Party` & `Authenticator` → have to agree on a common supported signature algorithm
  - Supported signature algorithms :
    1. ECDSA on `NIST P256`
    2. ECDSA on `secp256k1`
    3. EdDSA on `Ed25519`
    4. RSA PSS 2048 bits
    5. RSA PKCS 1.5 2048 / 3072 / 4096 bits
    6. SM2 digital signatures

FIDO Hardware Authenticator

- `Authenticator` can be implemented in several ways :
  - Web browser application
  - Mobile application
  - Hardware token
    e.g. USB token, smartcard, . . .
- FIDO Hardware `Authenticator` :
  - Most secure form of `Authenticator`
  - Potential communication interfaces :
    - USB, NFC, BLE, contact & contactless smartcard (ISO7816 / ISO14443)
  - Minimum requirements :
    - Communication interface
    - Cryptographic capabilities
    - Non Volatile Memory (NVM)

Attack Surface on FIDO HW Authenticators

- Relay attack if `Authenticator` always connected to `Client`
  - FIDO protocol : `Client` chooses user presence control byte → can be set to *dont-enforce-user-presence-and-sign*
  - Adversary has to be able to execute code on victim's `Client`
  - Note : possible to enforce user presence on some `Authenticators` *e.g. Yubico*
- Evil maid attack
  - Goal : extract Credential private key → clone `Authenticator`
  - Requirement : physical access to FIDO HW `Authenticator`
  - Possible attack paths :
    - SW attack on communication interface
    - Physical cryptanalysis (side-channel / fault attacks) on crypto. signature
    - Firmware extraction
- Generic remarks :
  - Attest. & Cred. private keys cannot be exported from `Authenticator` → makes physical cryptanalysis attacks harder to prototype !
  - Passwordless FIDO2 → make attacks more effective !

FIDO Certification for Authenticators (1/2)

- Different certification levels :
  - Functional
    - Conformance self-validation + interoperability tests
    - Allow vendors to use FIDO certified mark and logo
  - Level 1
    - Any SW or HW device
    - Protect against scalable remote attacks (e.g. phishing)
  - Level 1+
    - Any SW or HW device using white-box cryptography or similar technique
  - Level 2
    - Device must support :

      - ROE (Restricted Operating Environment)
      - Attestation
    - Protect against remote SW attacks
    - Examples :

      - TEEs based on ARM TrustZone / Intel VT - SGX - ME
      - Windows 10 Virtualization-based Security
      - Secure World of AMD PSP

FIDO Certification for Authenticators (2/2)

- Different certification levels (continuation) :
  - Level 3
    - Protect against remote SW attacks and local HW attacks
    - Examples :

      - GlobalPlatform cerftified TEE
      - USB token with CC certified OS at AVA_VAN.3 & tamper-evident FIPS
  - Level 3+
    - Protect against high level local HW attacks
    - Built on Common Criteria certified Secure Element with AVA_VAN.5
- FIDO certification process :
  - Pro :
    - webpage search engine very convenient
  - Cons :
    - Certification process not very well defined
    - No precise way to identify a product
    - No formal certificate accessible on the web

Agenda

1. FIDO(2) Protocol and Hardware Tokens

2. Partial Teardown of some FIDO(2) HW Authenticators

3. Other Interesting FIDO(2) HW Authenticators

4. Conclusions

Yubico (1/3)

- Founding member of FIDO alliance
- Historical product : Yubico YubiKey Neo
  - Chip for communication : NXP LPC11U24
  - Secure Element : **NXP A7005**
    → NXP P5 / SmartMX1 family
    → Certification : CC EAL5+ with AVA_VAN.5 until 2015
  - Known attack : see Google Titan Key

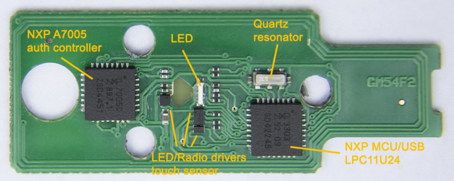
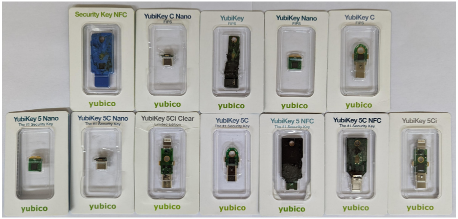


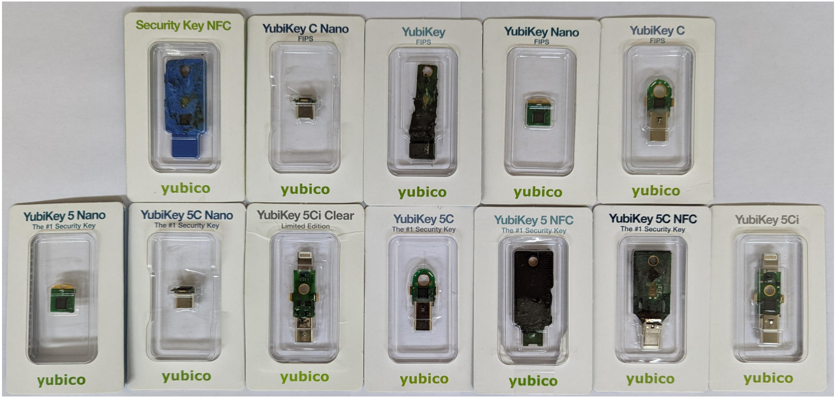
Figure – Yubikey Neo teardown - from http://www.hexview.com/ scl/neo/

Yubico (2/3)

- New products :
  - YubiKey 5 Series
  - YubiKey 5 FIPS Series
  - YubiKey 5 CSPN Series
  - YubiKey Bio Series
- All based on Infineon **SLE78CLUFX5000** Secure Element
  - Provides communication and crypto
  - Certification : CC EAL6+ with AVA_VAN.5
- U2F & FIDO2 / certification level 1
- Casing really hard to remove / No known attack



Yubico (3/3)


Security Key NFC
yubico
YubiKey C Nano
FIPS
yubico
YubiKey
FIPS
yubico
YubiKey Nano
FIPS
yubico
YubiKey C
FIPS
yubico
YubiKey 5 Nano
The #1 Security Key
yubico
YubiKey 5C Nano
The #1 Security Key
yubico
YubiKey 5Ci Clear
Limited Edition
yubico
YubiKey 5C
The #1 Security Key
yubico
YubiKey 5 NFC
The #1 Security Key
yubico
YubiKey 5C NFC
The #1 Security Key
yubico
YubiKey 5Ci
yubico

Google Titan Key (1/3)

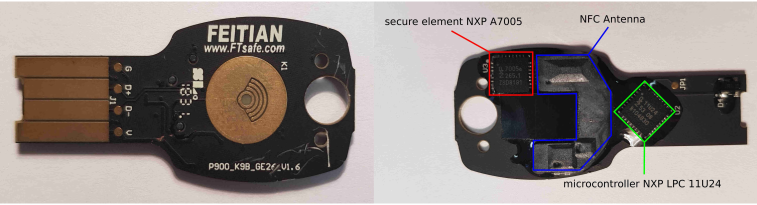
- Historically only released for Google employees
- Available on Google Store from 2018
- Three versions :
  - micro-USB, NFC and BLE
  - USB type A and NFC
  - USB type C
- Casing can be easy or hard to open depending on version

Google Titan Key (2/3)

- Hardware made by Feitian
- All based on same architecture :
  - Chip for communication : NXP LPC11U24
  - Secure Element : **NXP A7005**

    → NXP P5 / SmartMX1 family

    → Certification : CC EAL5+ with AVA_VAN.5 until 2015
- U2F / certification level functional



Google Titan Key (3/3)

- Known attacks :
  - 2019 : Microsoft attack (only apply on Titan key w. BLE)

    → Relay attack

    → Exploit bad configuration of BLE

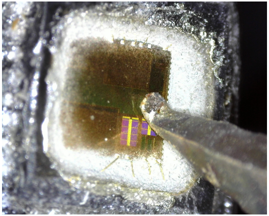
    → Concerned products recalled / Patched by Google
  - 2021 : NinjaLab SCA attack on NXP A7005 ECDSA signature

    → Evil maid attack (access during 10 hours to token)

    → ECDSA private key extraction ⇒ token cloning

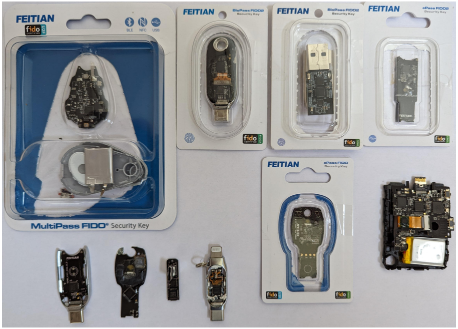
    → 12k$ of equipment, high SCA & cryptanalysis skills

    → Not patched by Google / NXP

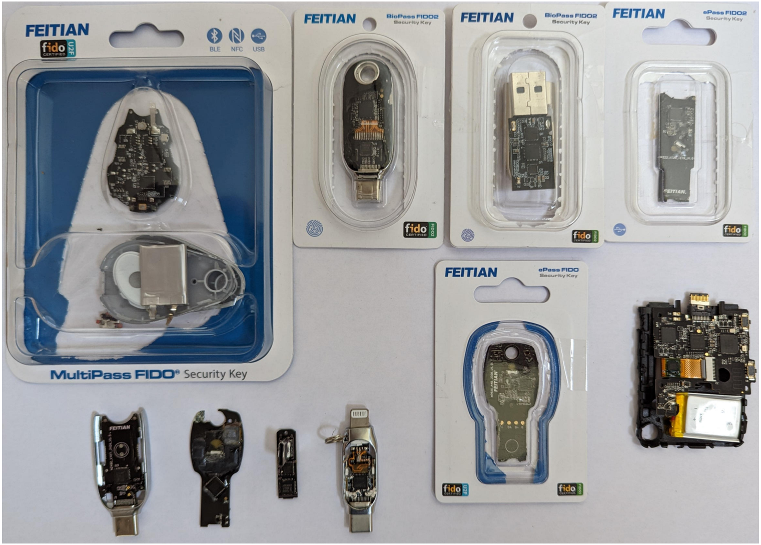


Feitian (1/5)

- Propose FIDO security keys for end-users but also in white-labelling
- Propose generic FIDO security keys with customization for :
  - Casing
  - Packaging
  - Related services
- Casing can be easy or hard to open depending on products



Feitian (2/5)


FEITIAN
fido CERTIFIED U2F
BLE
NFC
USB
MultiPass FIDO® Security Key
FEITIAN
BioPass FIDO2 Security Key
fido CERTIFIED FIDO2
FEITIAN
BioPass FIDO2 Security Key
FEITIAN
ePass FIDO2 Security Key
FEITIAN
ePass FIDO Security Key
fido CERTIFIED U2F
fido CERTIFIED FIDO2

Feitian (3/5)

- Feitian ePass A4B
  - USB type A
  - U2F & FIDO2 / certification level 1
  - Chip for communication & SE : **NationZ Z32HUB**
    Chinese CC EAL4+ / FIPS 140-2
- Feitian ePass K9
  - USB type A + NFC
  - U2F & FIDO2 / certification level 1
  - Product similar to Google Titan Key
    - Chip for communication : NXP LPC11U24
    - Secure Element : **NXP A7005**
      CC EAL5+ with AVA_VAN.5 until 2015
- Feitian ePass K12
  - USB type A
  - U2F & FIDO2 / certification level 1
  - Chip for communication & SE : **NationZ Z32HUB**
    Chinese CC EAL4+ / FIPS 140-2

Feitian (4/5)

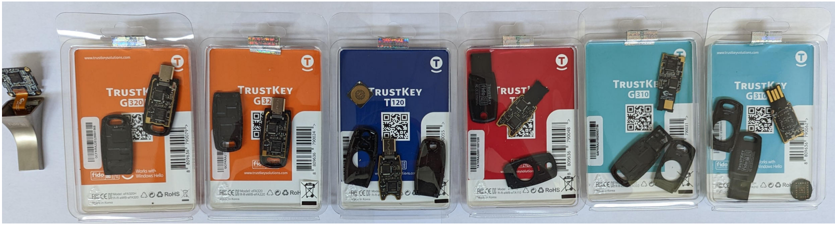
- Feitian MultiPass K16
  - micro-USB + NFC + BLE
  - U2F & FIDO2 / certification level 2
  - Product similar to Google Titan Key
    - Chip for communication : NationZ Z32HUB
    - SE : **NXP A7005**
      CC EAL5+ with AVA_VAN.5 until 2015
- Feitian ePass K21
  - USB type C
  - U2F & FIDO2 / certification level 2
    - Chip for communication : NationZ Z32HUB
    - SE : **NXP A7005**
      CC EAL5+ with AVA_VAN.5 until 2015
- Feitian BioPass K26 & K27
  - USB type C (K26) or USB type A (K27) + fingerprint sensor
  - U2F & FIDO2 / certification level 2 + FIPS-140-2 level 2
    - Chip for biometry : SYNOCHIP AS578
    - Chip for communication & SE : **NationZ Z32HUB**
      Chinese CC EAL4+ / FIPS 140-2

Feitian (5/5)

- Feitian AllInPass K33
  - USB type C + NFC + BLE + fingerprint sensor
  - U2F & FIDO2 / certification level 1
    - Chip for biometry : SYNOCHIP AS578
    - Chip for BLE : Nordic SemiConductor nRF52832
    - SE : Infineon LFH1621 (non identified)
      Probably Infineon SLE78 → CC EAL6+ with AVA_VAN.5
- Feitian ePass K40
  - USB type C + NFC
  - U2F & FIDO2 / certification level 1
    - Chip for communication : NationZ Z32HUB
    - SE : **NXP A7005**
      CC EAL5+ with AVA_VAN.5 until 2015
- Feitian iePass K44
  - USB type C + Lightning
  - U2F & FIDO2 / certification level 1
  - Chip for communication & SE : Infineon MTH1833 (non identified)
    Probably Infineon SLE78 → CC EAL6+ with AVA_VAN.5

TrustKey (1/2)

- TrustKey : South Korea company
- All products based on same architecture :
  - Chip for communication : NUVOTON NUC121ZC2
  - SE : **eWBM MS500** (South Korea fabless startup)
    No certification found for the SE
- Con : case easy to open with a scalpel & without damage



TrustKey (2/2)

- TrustKey T110
  - USB type A
  - U2F & FIDO2 / certification level 1
- TrustKey T120
  - USB type A
  - U2F & FIDO2 / not certified
- TrustKey G310 & G320
  - USB type A (G310) or USB type C (G320)
  - U2F & FIDO2 / certification level 1 (U2F) & 2 (FIDO2)
- TrustKey G500
  - USB type A
  - U2F & FIDO2 / certification level 2

Neowave

- French startup company
- All products base on same architecture :
  - Chip for communication & SE : **WISeKey MS6003C**
  - Chip certified CC EAL5+ with AVA_VAN.5
- Con : case easy to open with a scalpel & without damage

Agenda

1. FIDO(2) Protocol and Hardware Tokens

2. Partial Teardown of some FIDO(2) HW Authenticators

3. Other Interesting FIDO(2) HW Authenticators

4. Conclusions

Initiatives from BSI (German Cybersecurity Agency)

- 2017 : publication of a **Common Criteria Protection Profile** :
  - FIDO Universal Second Factor (U2F) Authenticator
  - Certification report : BSI-CC-PP-0096-V3-2018
  - Last version : v3 (2018)
  - Target assurance level : EAL4+ with AVA_VAN.5

- 2020 : **de.fac2** - FIDO U2F `Authenticator` JavaCard Applet
  - Last version : v1.34 (2022)
  - Available at https://github.com/BSI-Bund/de.fac2
  - Initially developped for G+D Sm@rtCafe Expert 7.0 smartcard :
    - Common Criteria certified at level EAL4+ with AVA_VAN.5
      Certification report BSI-DSZ-CC-1060-2020
    - FIDO certified at level 3+
      Currently only Authenticator certified at level 3/3+
  - Vulnerability reported by Sergei Volokitin :
    - Reset command sent by reader can circumvent user presence check

Thales / Gemalto

- Thales / Gemalto : historical French smartcard vendor
  Worldwide biggest smartcard vendor / highly secure products

- SafeNet IDPrime 3930 FIDO
  - Dual interface smartcard (ISO7816 & ISO14443) / U2F & FIDO2
  - Chip : **Infineon SLE78CLFX400VPH**
  - Certification : FIDO level 1 / NIST FIPS 140-2

- SafeNet IDPrime 3940 FIDO
  - Dual interface smartcard (ISO7816 & ISO14443) / U2F & FIDO2
  - Chip : **Infineon SLE78**
  - Certification :
    - FIDO level 1
    - CC EAL5+ with AVA_VAN.5 for chip, JavaCard OS & applet

- SafeNet eToken FIDO
  - USB type A & touch sensor / U2F & FIDO2
  - Chip : D9C03 (non identified)
  - Certification :FIDO level 1 / CC EAL6+ with AVA_VAN.5

FIDO & HW Crypto-Currencies Wallets

- Ledger
  - Official Ledger application for FIDO U2F
  - Supported on both Ledger Nano S & Nano X
  - Device PIN required for authentication
  - BIP39 seed allows to backup FIDO credentials
  - FIDO2 soon supported
    - Chip for communication : STM32F042K6 (S) / STM32WB55 (X)
    - SE : **ST31H320** (S) / **ST33J2M0** (X) → *both certified CC EAL5+ with AVA_VAN.5*
- Satoshi Labs
  - Official Satoshi Labs application for FIDO U2F & FIDO2
  - Trezor One : only U2F since firmware v1.4.0
  - Trezor model T : U2F + FIDO2 since firmware v2.1.6
  - BIP39 seed allows to backup FIDO credentials
  - Chip for com. & SE : **STM32F205** (One) / **STM32F427** (model T)

Other Big Players

- Apple
  - 2018 : exp. support in macOS / Safari webkit for WebAuthn
  - 2019 : native support in iOS for FIDO authenticators
  - 2020 : Apple joins FIDO alliance
  - 2020 : Face ID and Touch ID support FIDO2
    - iPhones & MacBooks w. Touch ID can be used as FIDO `Authenticators`
    - Use of Secure Enclave as Secure Element
- Google
  - 2019 : Android 7+ smartphones can be used as FIDO2 `Authenticators`
    - Use of Android Keystore Attestation & device TEE as Secure Element
    - Use of device biometrics & secure display for user presence control

Agenda

1. FIDO(2) Protocol and Hardware Tokens

2. Partial Teardown of some FIDO(2) HW Authenticators

3. Other Interesting FIDO(2) HW Authenticators

4. Conclusions

How to Choose a Good FIDO(2) Authenticator ?

- FIDO HW `Authenticator` is the best :-)
- Casing hard to open / replace
  ⇒ Adds a security layer against evil maid attacks
- Secure Element with CC certification AVA_VAN.5 is a best !
- Architecture with two chips
  ⇒ Adds a security layer against attacks targeting USB interface
- PIN or biometry adds an authentication factor

Future ?

- HW FIDO(2) `Authenticators` certified at higher levels :
  - FIDO level 3 / 3+
  - Common Criteria EAL4+ with AVA_VAN.5 (c.f. BSI Protection Profile)

- Other Potential Attack Paths on FIDO(2) HW `Authenticators` :
  1. Attacking USB interface / stack of single chip HW FIDO tokens ?
     - Some HW FIDO tokens have only one chip for USB & SE
     - USB interface / stack : interruptions, parsing
     - Huge attack surface : fuzzing, SW + FI combined attacks, . . . ?
  2. Fault based cryptanalysis on ECDSA signature ?

Thank You for your Attention :-) Any Question ?