Federal Office
for Information Security

Augmenting passwords

Lightning talk

Tobias Damm, BSI - Division TK11 – Chip Security

Omnisecure Berlin, 23.01.2024

Passwords – Knowledge bound to individual

Does a good password exist?

Everyone uses passwords

- Trivial concept
- Easy to use
- Toolless
- Easy to implement (really?)
- Easy to manage and support (well…)

How secure are passwords?

- Credential stuffing
- **Phishing**
- Malware, key logger
- Social engineering

Your password (complexity, length) does not matter !

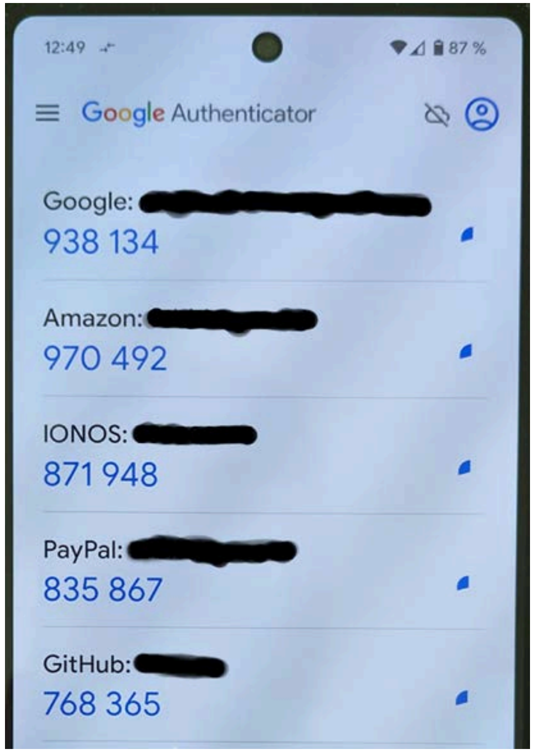
- Password spraying
- Brute force

Your password does matter !
(so please choose a good one)

- …

-> Authentication enforced by (only) presenting a static shared secret is problematic !

Augmenting passwords



12:49 87 %

Google Authenticator

Google: [redacted]
938 134

Amazon: [redacted]
970 492

IONOS: [redacted]
871 948

PayPal: [redacted]
835 867

GitHub: [redacted]
768 365

Adding (sort of) ‘Possession’ as an additional factor:

➢ Typ. ‘Knowledge’ weakly bound to device or similar

  - TAN list (deprecated)
  - mTAN / smsTAN (still widely used)

More advanced (and recommended):

- TAN generator
- Time-based one-time passwords (TOTP)
  (widely adopted; authenticators available as software or hardware)

Still a shared secret susceptible to phishing / MITM

Strong second factor, Strong multi-factor & Strong single factor authentication

FIDO U2F & FIDO 2

Strong 2nd factor utilizing asymmetric cryptography with FIDO U2F

- Authenticator creates private/public key pair
- Mutual registration of authenticator and relying party
- Signed Challenge-Response and Attestation scheme
- Dedicated hardware (Client connected via USB/NFC/BT)

-> Strong mitigation against phishing attacks

‘Passwordless’ authentication with FIDO 2 (WebAuthn & CTAP 2)

- Enhanced protocols and functionality
- Added user authentication for authenticator (PIN, gesture, biometrics)
- Discoverable credentials enable strong single factor

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1060-2020(*)

de.fac2 - FIDO U2F Authenticator Applet
v1.34

Common Criteria

from	Federal Office for Information Security (BSI)
PP Conformance:	FIDO Universal Second Factor (U2F) Authenticator Version 3, 5 November 2018, BSI-CC-PP-0096-V3-2018
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5

Hot topics

Acceptance: Usability vs. Security?

- Possibilities for backup or synchronisation of authenticators?
- ‘Passkeys’ to solve all problems?
- Software tools vs. hardware tokens?

Security Assurance, i.e. evaluation and certification of secure authenticators and services

State of adoption

- FIDO 2 on/with mobile devices, i.e. iOS and Android
- FIDO 2 browser integration
- Services offering FIDO 2 authentication

Thank you for your attention!

Contact

Tobias Damm
Division TK11 – Chip Security

Tobias.damm@bsi.bund.de

Federal Office for Information Security (BSI)
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de

BSI as the Federal Cyber Security Authority shapes information security in digitalization through prevention, detection and response for government, business and society.