

# Hardware Sicherheit

## Proof-of-Concept-Implementierung einer Anwendung mit FIDO2 Support

Mara Schulke

Matrikelnr. 20215853, SS22 B.Sc. IT Security, THB

31. Juli 2022

# Übersicht

Der FIDO2 Standard

Ablauf einer Registrierung

Ablauf einer Authentifizierung

Vorteile gegenüber einfacher asymmetrischer Kryptografie

Möglichkeiten durch den Einsatz von FIDO2

Details zur Implementierung des PoC

Anhänge / Verweise

# Der FIDO2 Standard

- ▶ Industriestandard für hardwaregestützte Authentifizierung
- ▶ Setzt sich im wesentlichen aus zwei Protokollen zusammen:
  - ▶ CTAP
  - ▶ WebAuthn
- ▶ Der Hardwaretoken kann innerhalb des Systems verbaut sein (z.B. über ein TPM) oder ein externes Gerät sein (bspw. Yubikey oder Google Titan)
- ▶ Quelloffen und nicht proprietär
  - ▶ Durch Projekte wie OpenSK lassen sich sogar eigene Hardwaretokens bauen

# Ablauf einer Registrierung

- ▶ Client erhält vom Server Schlüsselgenerierungsparameter
- ▶ Client reicht diese an den Authenticator weiter
- ▶ Authenticator speichert das Schlüsselpaar für die Relying Party und gibt den Public Key an den Client
- ▶ Client leitet den Public Key an den Server weiter
- ▶ Server persistiert den Public Key und ordnet ihn dem Nutzer zu

# Ablauf einer Authentifizierung

- ▶ Client erhält vom Server eine Challenge
- ▶ Client reicht diese an den Authenticator weiter
- ▶ Authenticator signiert die Challenge mit dem Private Key
- ▶ Client leitet die Signatur an den Server weiter
- ▶ Server überprüft mit dem Public Key ob die Signatur gültig ist

# Vorteile gegenüber einfacher asymmetrischer Kryptografie

- ▶ Erhöhte Sicherheit durch separate Schlüsselpaare pro Relying Party
- ▶ Verlust eines Schlüsselpaars wäre verhältnismäßig unkritisch da dieses nur Zugriff auf einen Online-Dienst gibt
- ▶ Schlüsselpaare werden nicht auf dem System des Nutzers gespeichert
  - ▶ Kompromitierte Verbindungen und Nutzersysteme stellen keine schwerwiegende Gefahr dar
  - ▶ Verlust des Systems unkritisch
- ▶ Physikalischer Diebstahl des Tokens notwendig um erfolgreiche Impersonation-Attacken auszuführen

# Möglichkeiten durch den Einsatz von FIDO2

- ▶ viele Angriffsvektoren lassen sich zu weiten Teilen durch den Einsatz von FIDO2 ausschließen bzw. verharmlosen (bspw. Man-In-The-Middle, Phishing etc.)
- ▶ Nutzer müssen keine Passwörter mehr verwalten
- ▶ Nutzer können sich einfach und sicher passwortlos Anmelden

# Details zur Implementierung des PoC

- Siehe Bildschirmübertragung



# Anhänge / Verweise

- ▶ Quellcode: [github.com/mara214/fido2-auth](https://github.com/mara214/fido2-auth)
- ▶ Authenticator: Google Titan