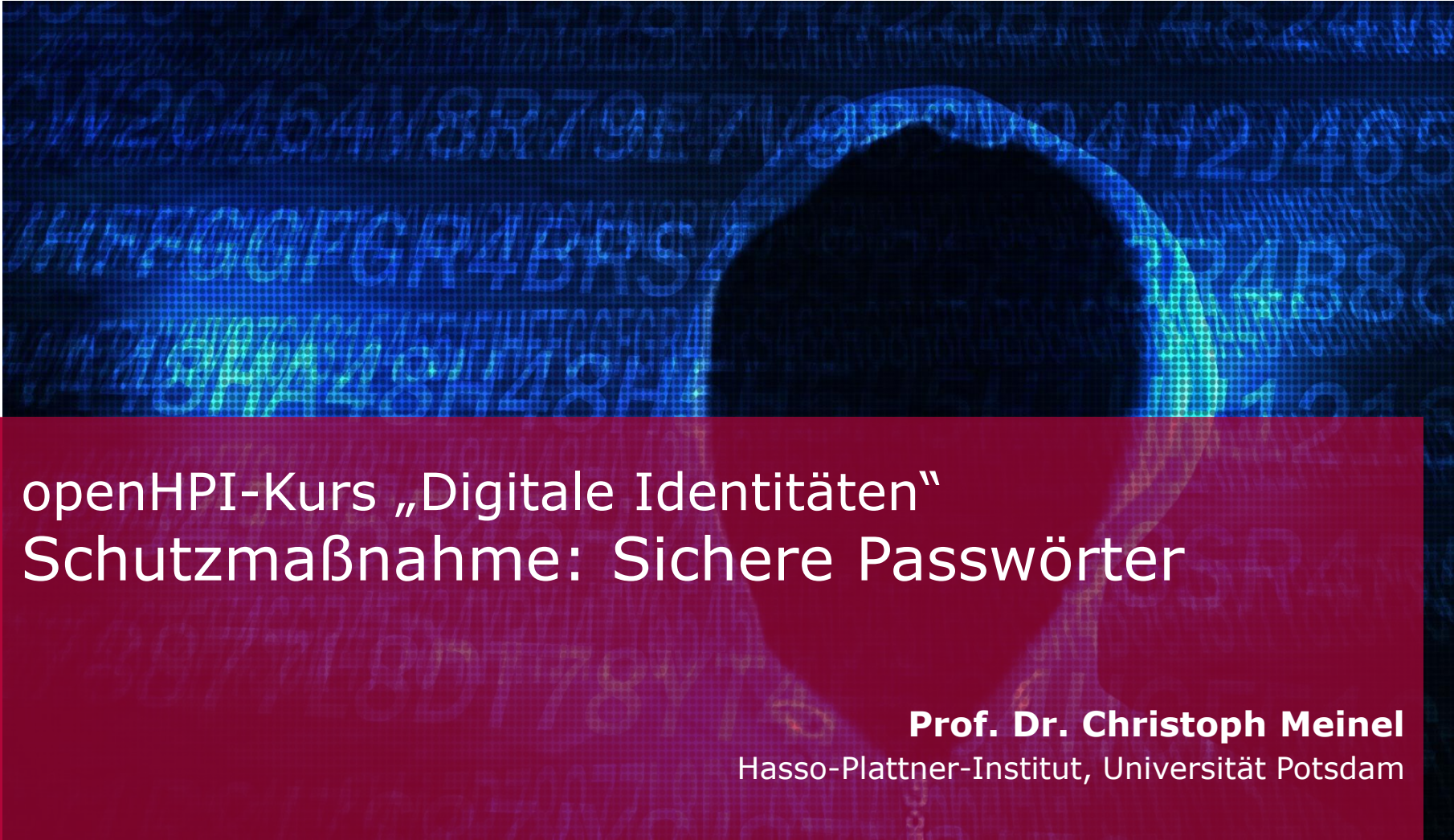




openHPI-Kurs „Digitale Identitäten“ Schutzmaßnahme: Sichere Passwörter

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Universität Potsdam

Wahl „guter“, also sicherer Passwörter (1/2)

Passwörter sind gut, wenn sie schwer zu raten oder knacken sind ...

■ **Ratschläge** für die Wahl guter Passwörter:

- Passwörter **sollten Groß- und Kleinschreibung** mischen, auch **Kombinationen** mehrerer Wörter sind sinnvoll
- Passwort sollte neben **Buchstaben** auch **Ziffern** und **Sonderzeichen** (\$%&:;_-?§!...) enthalten
- **Minimallänge** von 12 Zeichen
 - umso länger die Zeichenlänge, desto höher die Sicherheit, weil mit jeder zusätzlichen Stelle Komplexität für Brute Force und Wörterbuchangriffe exponentiell steigt
- **Keine** Passwörter aus dem **Nutzerkontext** oder aus einem **Wörterbuch**
- **Keine alten** Passwörter wieder verwenden

Wahl „guter“, also sicherer Passwörter (2/2)

Passwörter sollten trotzdem leicht zu merken sein, damit sie nicht aufgeschrieben werden müssen

Eselsbrücke:

Schwierige Passwörter kann man sich merken, wenn man sich vollständigen Satz merkt, dessen Wortanfangsbuchstaben (groß- und kleingeschrieben) das Passwort bilden, z.B.

- Wo ein Wille ist, ja da ist auch ein Weg. – **W1Wi,jdia1W.**

Sichere Speicherung von Passwörtern

Neben der Wahl sicherer Passwörter, kommt es auf deren sichere Speicherung an

- Passwörter niemals an Dritte weitergeben
- für Datendiebe unerreikbaar, z.B.
 - verschlüsselter Speicher → Passwortmanager

Verwendung von Passwortmanager (1/3)

Problem selbst mit sicheren Passwörter:

- jeder Account braucht sein eigenes sicheres Passwort
- viele haben >20 Internetkonten/Identitäten
- alle Passwörter kann sich kein Mensch merken

Eine Lösung: **Passwortmanager**

- Dienst oder Programm, bei dem alle Passwörter mit einem einzigen, sehr starken Passwort verwaltet/verschlüsselt werden
- es gibt Offline und Online-Varianten von Passwortmanagern
- für jeden Onlinedienst kann neues Passwort generiert werden
- automatisches Eintragen der Passwörter auf Webseiten

Verwendung von Passwortmanager (2/3)

Offline Passwortmanager

- Grundsätzlich sicherer, da kein Dritter Zugriff auf Passwörter hat
- Backups müssen selbst gemacht werden
 - Datenbank kann auf Cloud ausgelagert werden
- Zum Ausprobieren empfiehlt sich z.B. das kostenlose **KeePass**



Verwendung von Passwortmanager (3/3)

Online Passwortmanager

Speichern Passwortdatenbank
online (in der Cloud)

- Passwörter sind auf allen
Geräten verfügbar
- Ungewiss, ob Anbieter Passwörter
im Klartext speichert oder nicht

LastPass ****



iCloud Keychain



Zusammenfassung: Sichere Passwörter

Sichere Passwörter...

- ...enthalten Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
- ...sind mindestens 12 Zeichen lang
- ...findet man nicht im Wörterbuch
- ...lassen sich nicht aus dem Nutzerkontext ableiten
- ...werden nicht wiederverwendet

Passwortmanager helfen beim Generieren und Aufbewahren von Passwörtern