Authentifizierung

Grundlagen & Passwörter

Lektion 1

Der Wolf und die sieben Geisslein

- Märchenstunde mit Herrn Schärer

- Warum?
- Neues Thema: **Authentifizierung**!
- Überprüfung von Identität …
- … z.B. um sich in Online-Konto einer Website einzuloggen.

Der Wolf und die sieben Geisslein

- Was ist passiert?
- Weshalb haben die sieben Geisslein die Türe geöffnet?
  - der Wolf gibt sich als Mutter aus, die Geisslein fallen aber nicht (gleich) darauf hinein
  - die Stimme ist zu tief
    - ➔ Wolf frisst Kreide, um die Stimme zarter zu machen.
  - die Pfote ist nicht weiss
    - ➔ mit Mehl bestäubt funktionierts
- Analogie: Der Wolf ist ein ‘Hacker’ und hat das Benutzerkonto der Mutter kompromittiert!

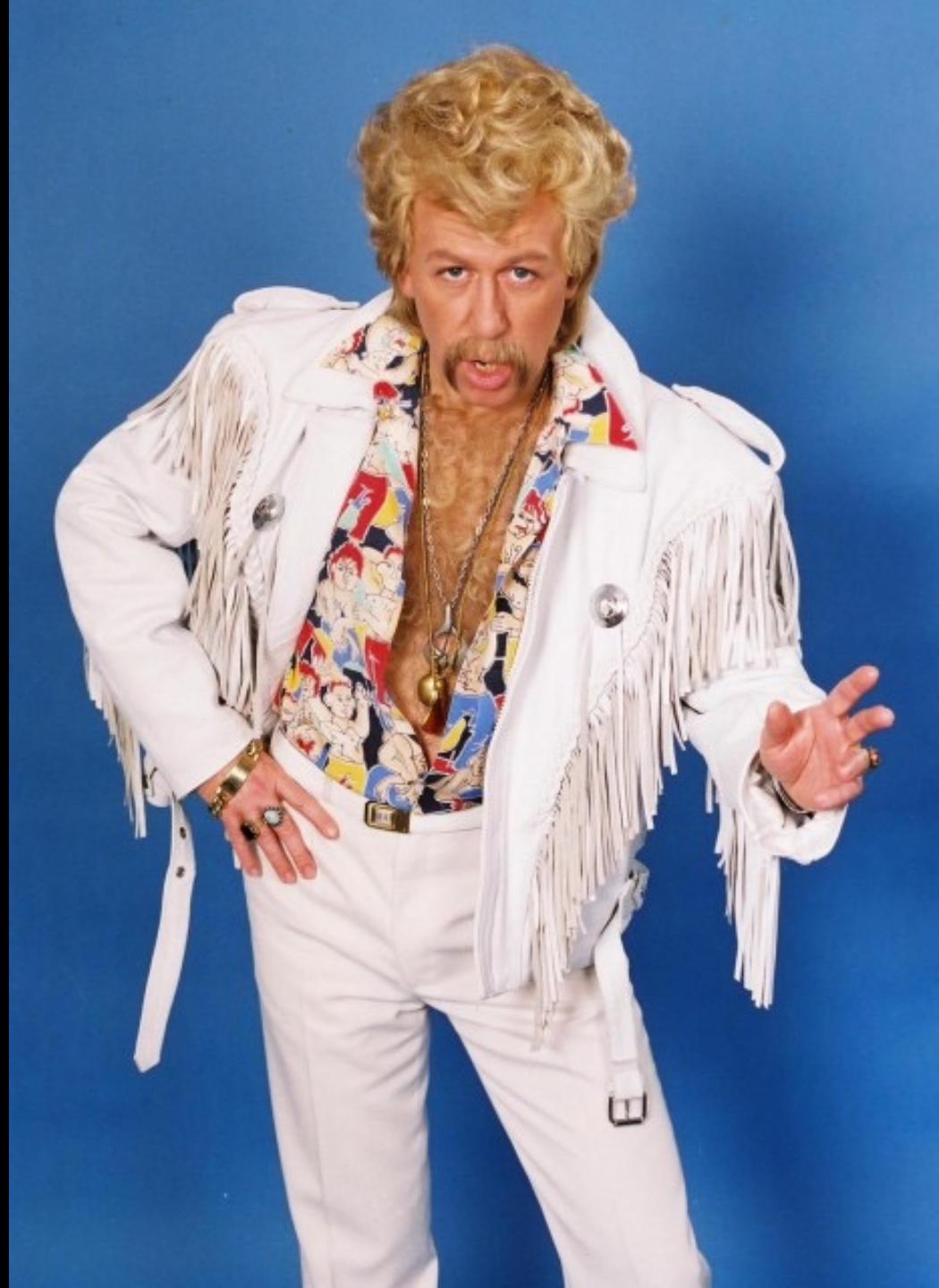
Der Wolf und die sieben Geisslein

- Fragen:
  - Was haben die Geisslein **gut** gemacht?
    - Überprüfung …
    - … mit mehreren Faktoren (Stimme & Pfote)
  - Was haben sie **nicht gut** gemacht?
    - Stimme und Pfote sind beides direkte Attribute eines Tiers. Hätten noch andere Faktoren überprüfen sollen.
  - Konkrete **Verbesserungsvorschläge** für Familie Geiss?
    - Frage stellen, die nur Mutter beantworten kann (‘Was ist dein Lieblingsessen?’)
    - Passwort abmachen
    - Schlüssel, Fingerabdruckscanner, … an Tür
    - …

Authentifizierung

- Was heisst **Authentifizierung**?
  - authentisch: echt, glaubwürdig, belegt
  - Nachprüfen, ob die vorgegebene Identität stimmt.

    "Ich bin Harry Hasler" – wirklich?



Authentifizierung

- Wo findet **Authentifizierung im echten Leben** (nicht Internet) statt?
  - Diskussion: überlege dir mind. vier Situationen (3’)
  - Mögliche Antworten:
    - Personenkontrolle bei Grenzübergang, Authentifizierung mit ID
    - Billetkontrolle im Zug: Swisspass
    - Zugang Zuhause oder Büro: Schlüssel, Batch
    - Smartphone / Laptop: Passwort, Fingerabdrucksensor, Gesichtserkennung
    - Zugang zu Party, Covid-Zertifikat + Ausweis
  - Typische **Mittel zur Authentifizierung**:
    - Ausweis
    - Passwort / Pin
    - Biometrische Merkmale (Fingerabdruck, Gesichtserkennung)
    - Schlüssel, Batch

Passwörter

- Standardmethode zur **Authentifizierung am Computer:**
- **Passwörter**!
- Top-10 der Passwörter

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

- Weitere schlechte Passwörter: `Romanshorn` `iloveyou`
- Problem: Passwörter sind grundsätzlich **unsicher**!

Passwörter

- Diskussion: **Verschiedene Möglichkeiten**, um an fremde Passwörter zu gelangen? (3’)
- Mögliche Antworten:
  - Brute-Force
    - alle durchprobieren
    - Beliebige Zeichenfolge `q3r`
    - oder Liste mit vielen Wörtern `Arbeiterunfallversicherungsgesetz`
    - Aufgabe: selber Code schreiben, der Brute-Force-Attacke simuliert
  - Phishing (z.B. falsche Login-Seite)
  - Keylogger: Malware (Virus), die die Passwort-Eingabe mitschneidet.
  - Mitstudent:in hinter deinem Rücken
  - Unsichere Verbindung: Passwort wird im Klartext übertragen

Passwörter

- Umgang mit Passwörtern:
  - Problem: Niemand kann sich für jede Webseite ein separates sicheres Passwort merken.
  - … also verwendet man für viele (oder sogar alle) Seiten das gleiche Passwort.
  - Wird eine davon gehackt, gelangt das Passwort und dazugehörige Email in den Umlauf, und kann gekauft werden.
- Beispiel:
  - http://pruefungsvorbereitung.ch/ wird gehackt.
  - Verwende gleiches Passwort bei Gmail -> Zugriff auch dort
  - … dann gute Nacht.
- Hat es mich bereits erwischt?
  - https://haveibeenpwned.com

Passwörter

- Diskussion: Wie kann man Problem mit Passwörtern lösen?
- Mögliche Antworten:
  - Passwort-Manager
  - Mehrfaktor-Authentifizierung
  - Login with {Facebook, Google, …}
- Mehr dazu später

Passwortmanager

- **Idee**:
  - **Programm**, in dem alle **Passwörter gespeichert** sind.
  - Sind verschlüsselt (→ eigenes Thema später)
  - Um PW einzusehen (entschlüsseln): **Masterpasswort**, **Schlüsselfile,** …
  - Beispiel Masterpasswort: muss sich nur ein einziges Passwort merken!
  - → für jedes Login ein anderes, langes Zufallspasswort
- Viele Browser haben integrierten Passwortmanager
- Alternativ (besser?): separates Passwortmanager-Programm
- Installiere den Open Source Passwortmanager **KeePass** …
- und probiere diesen aus
- https://keepass.info/

- https://haveibeenpwned.com
- KeePass: https://keepass.info/

Multifaktor-Authentifizierung

Passwörter

- Passwörter sind unsicher, relativ einfach hackbar
- Wie hackt man …
  - **Kurzes Passwort aus Zufallssymbolen**?
    - Beispiel: `rkU5`
    - Brute-Force, einzelne Zeichen (haben gemacht!)
  - **Langes Passwort aus Wörtern**?
    - Beispiel: `kuchenbierapfel`
    - Brute-Force, Listen aus Wörtern
  - **Langes Passwort aus Zufallssymbolen**?
    - Beispiel.: `fu37vjD!J1i_dk1sc093eK9vc`
    - Praktisch unmöglich mit Brute Force
    - Aber mit Social Engineering, Malware, …
- Wie schütze ich mich am besten?

Multifaktor-Authentifizierung

- Multifaktor-Authentifizierung!
- Zugang zu Online-Konto mit mehreren unterschiedlichen Faktoren abgesichert
- Beispiel: **Drei-Faktor-Authentifizierung**
  - Idee: Für Zugang muss man …
  - … etwas besonderes **wissen**, **Wissensfaktor**
  - … etwas besonderes **haben**, **Besitzfaktor**
  - … und etwas besonderes **sein**. **Inhärenzfaktor**
- Viele Onlinedienste erlauben Multifaktor-Authentifizierung
  - Vorteil: viel höhere Sicherheit
  - Nachteil: Einloggen umständlicher
  - **Empfehlung: Richte Multifaktor-Authentifizierung ein für wichtigste Dienste, also diejenigen, bei denen der Verlust am schlimmsten wäre.**
  - Diskussion: Welche Dienste sind das?

Multifaktor-Authentifizierung

- Problem bei «Sieben Geisslein»:
  - Überprüfen zwar zwei Faktoren (Stimme und Pfote) …
  - … sind aber *beides Inhärenzfaktoren*
  - … sollten auch andere beiden Faktoren berücksichtigen
- Diskussion: Schlage den «Sieben Geisslein» ein sinnvolles Sicherheitssystem mit einer **Drei-Faktor-Authentifizierung** vor mit jeweils einem …:
  - Wissensfaktor — z.B. Passwort
  - Besitzfaktor — z.B. Schlüssel
  - Inhärenzfaktor — z.B. Stimmerkennung

Aufgabe / Diskussion

1. Angenommen, du hättest an deinem Safe einfach drei Pin-Code-Schlösser. Wäre das dann auch eine Drei-Faktor-Authentifizierung? Wäre sie mehr oder weniger sicher als die Variante mit Schlüssel, Pin-Code und Fingerabdruck?

2. Überlege dir für jeden der drei Faktoren (Wissen, Besitz, Inhärenz) mind. ein **konkretes Real-Life Beispiel** (nicht am Computer/Smartphone)