

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 funktioniert
- 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 Lieblingessen?')
    - 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?

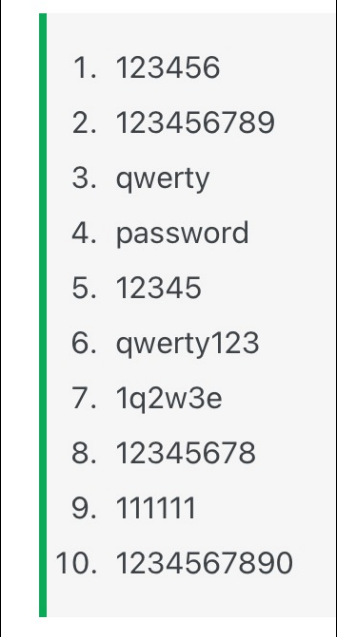


# Authentifizierung

- 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: Swissspass
    - 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)
    - Schlüssen, 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
  - 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

# Aufgabe

- Siehe Wiki
- Aufgabe 1: Brute-Force-Attacke
- HA: Version 1 der Aufgabe 1 fertig machen

# Brute-Force Attacke

Lektion 2

# Auftrag

- Siehe Wiki
- Aufgabe 1, Versionen 2 und 3

# Multifaktor-Authentifizierung

Lektion 3

# 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**

# 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



# Auftrag

- Siehe Wiki
- Aufgaben 2 & 3
- Wenn fertig: Weiter an Aufgabe 1
- HA: A2 & 3 fertig