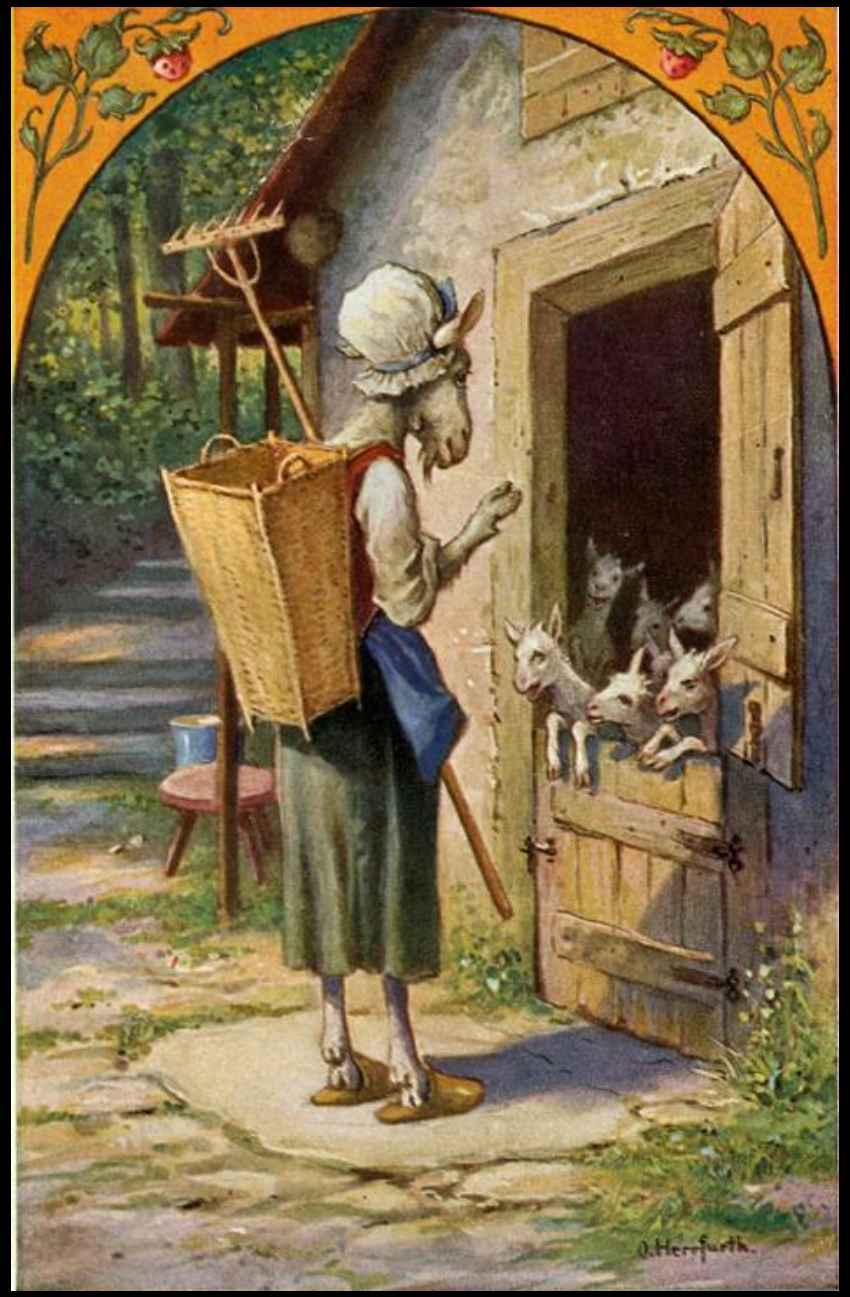
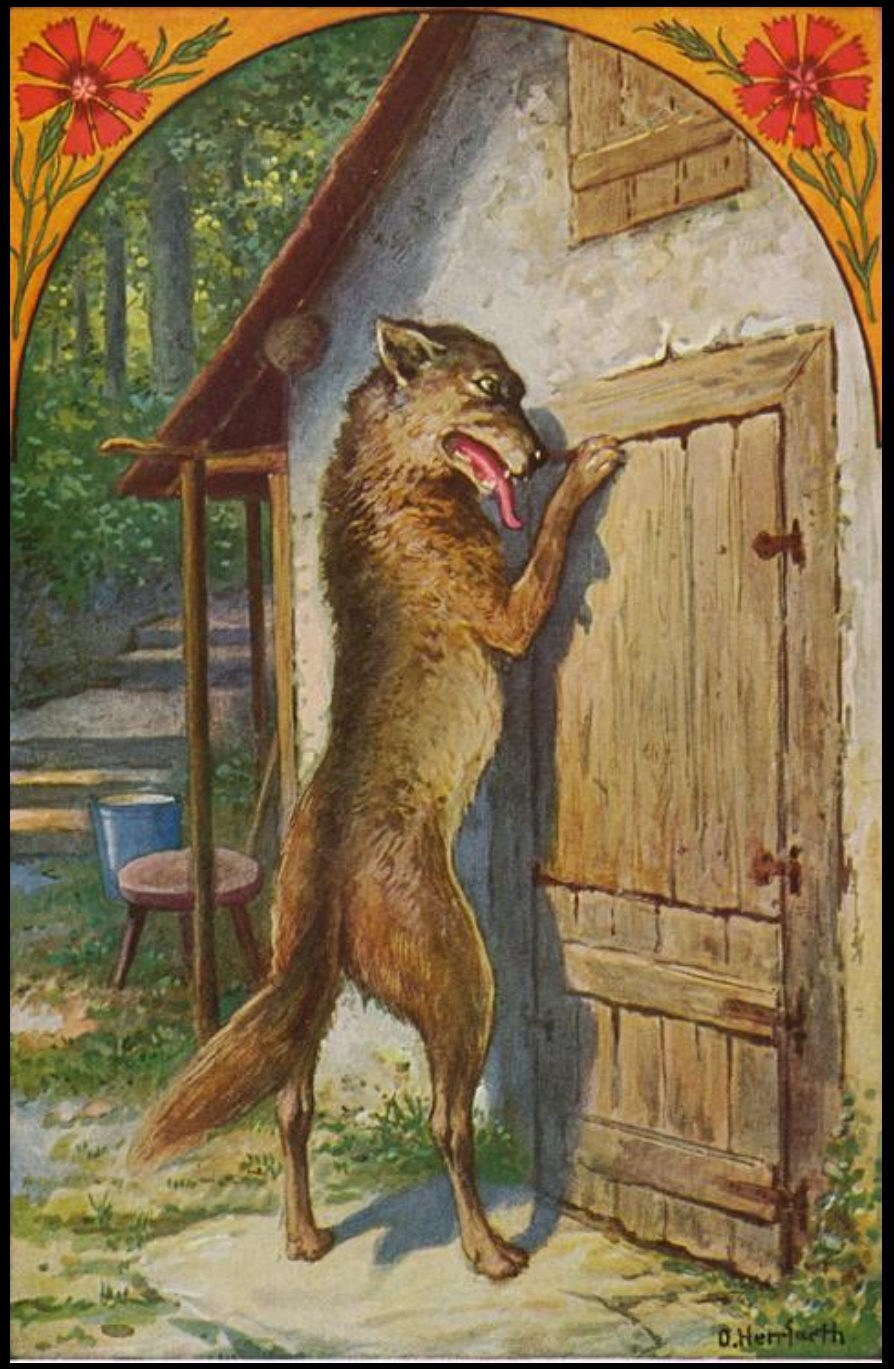
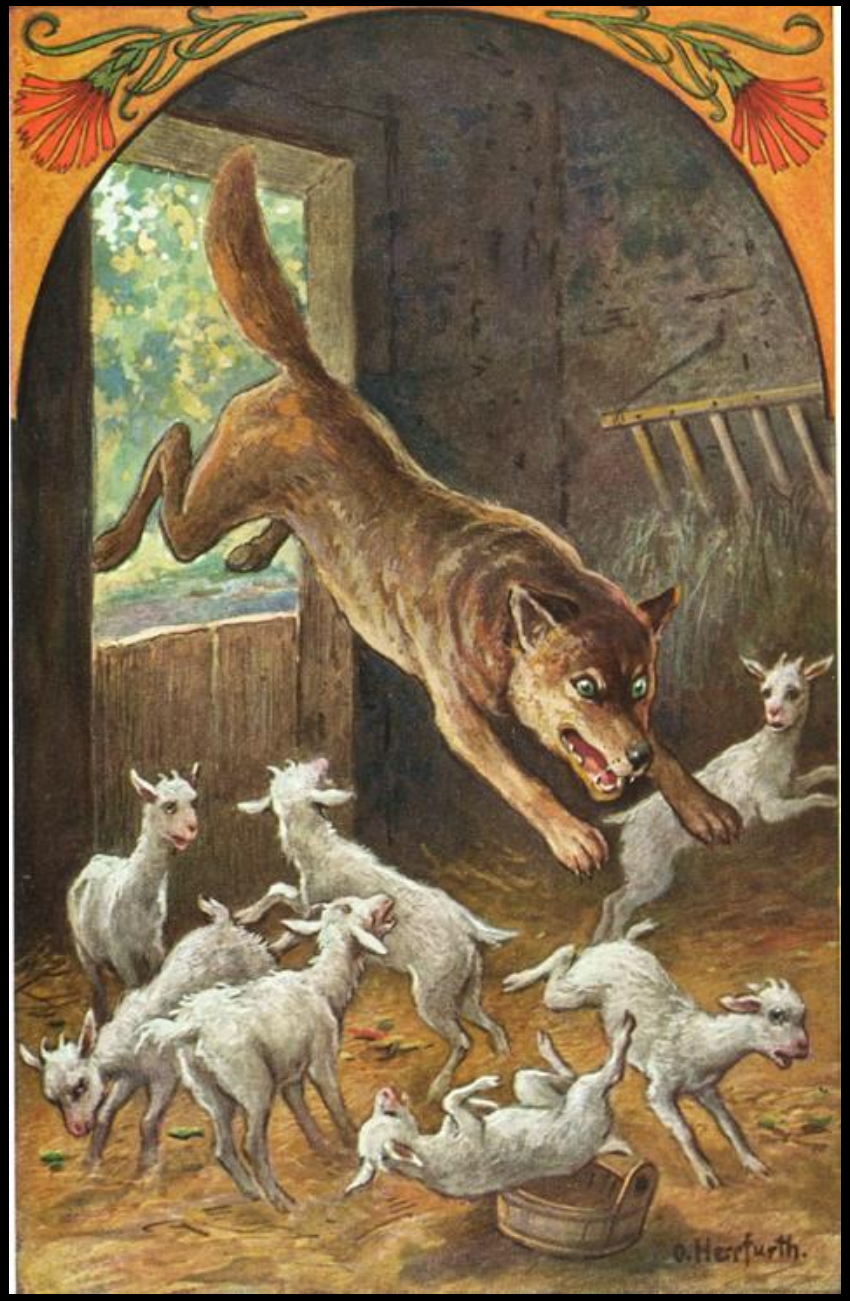

O. Herrfurth.


O. Herrlerth


O. Herrfurth.

Der böse Wolf!

- Was ist passiert?
- Weshalb haben die sieben Geisslein die Türe geöffnet?
  - der Wolf gibt sich als Mutter aus, die Geisslein fallen aber nicht 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
- Der Wolf hat das Benutzerkonto der Mutter kompromittiert.

Authentifizierung

2M – Sicherheit im Netz

Authentifizierung (A15g)

- Was heisst Authentifizierung?
  - **authentisch**: echt, glaubwürdig, belegt
  - Nachprüfen, ob die vorgegebene Identität stimmt.
    - "Ich bin Harry Hasler" – wirklich?

- Wo findet Authentifizierung im Alltag statt?
  - überlegen Sie sich vier Situationen (2m)

Authentifizierung

- Wozu?
  - Autorisierung ist oft an Identität geknüpft.
    - Prüfungszulassung
    - Fahrerlaubnis (Führerschein)
    - Bahnbillett mit Swisspass
    - Covid-Zertifikat + Ausweis
    - Mobiltelefon entsperren
- Wie?
  - Lichtbildausweis
  - Kennwort (Passwort)
  - Biometrische Merkmale (Fingerabdruck)

Keine Authentifizierung

- Autorisierung: Zugangsberechtigung
  - oft an Identität geknüpft, aber nicht immer

- Keine Authentifizierung findet statt:
  - Bahnbillett (ohne Swisspass)
  - Fahrrad aufschliessen mit Schlüssel (jeder mit dem Schlüssel ist autorisiert)

Authentifizierung am Computer

- Standard-Methode seit 50 Jahren:
  - Passwörter
  - Grundidee: nur der richtige Benutzer kennt das Passwort, also ist er identifiziert.

- Problem:
  - Passwörter sind unsicher. Full Stop.

Passwörter sind unsicher!

- Attacken auf Passwörter:
  - Brute-Force (alle durchprobieren)
  - Keylogger: Malware (Virus), die die Passwort-Eingabe mitschneidet.
  - ein:e Mitstudent:in hinter deinem Rücken
  - Unsichere Verbindung: Passwort wird im Klartext übertragen

- ^ das ist alles nicht so dramatisch (obwohl real)

Passwörter sind wirklich unsicher!

- Niemand kann sich für jede Webseite ein separates Passwort merken.
  - … also verwenden wir für viele Seiten das gleiche Passwort.
- Wird eine davon gehackt, gelangt das Passwort und dazugehörige Email in den Umlauf, und kann gekauft werden.
  - Bsp: http://pruefungsvorbereitung.ch/ wird gehackt.
  - Passwort wird darauf bei http://gmx.ch probiert – wenn das Passwort das gleiche ist, gute Nacht.
- **Angriff kann skaliert werden.**

- https://haveibeenpwned.com

Brute Force!

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

Wenn nicht Passwörter, was dann?

- Password Manager:
  - Ein separates Passwort für jede Seite.
    - -> wird eine Seite gehackt, sind die anderen isoliert.
    - -> integriert in Chrome, Edge, Firefox...
  - Problem 1: was, wenn der Password Manager gehackt wird?
  - Problem 2: was, wenn Sie dem Password Manager nicht vertrauen?
  - Problem 3: Computerviren können immer noch Passwörter stehlen.

- Trotzdem: sehr empfehlenswert

Wenn nicht Passwörter, was dann?

- Log in with {Facebook, Google, Apple... }
  - Grundidee: grosse Firmen werden weniger schnell gehackt, als kleine.
  - Problem 1: was machen die grossen Firmen mit den Informationen über meine verbundenen Dienste?
  - Problem 2: was, wenn Sie der Seite eine andere Emailadresse angeben möchten?

- Trotzdem: Viel sicherer als Passwörter

Wenn nicht Passwörter, was dann?

- Multifaktor-Authentifizierung
  - Mindestens ein zweiter Faktor ausser dem Passwort:
    - SMS-Code
    - App auf Mobiltelefon, die ans Gerät gebunden ist
    - Streichliste
    - Hardware-Token (Smartcard / USB-Stick / OTP-Generator)
  - Standard bei E-Banking.
  - Problem: etwas mühsamer...
- Sehr empfehlenswert
  - 50% weniger kompromittierte Konten (Google, Februar 2022)
  - informieren Sie sps@ksr.ch!

Multifaktor-Authentifizierung

- Faktoren:
  - Wissens-Faktoren
    - Passwort, PIN-Code
  - Besitz-Faktoren
    - Token / Mobiltelefon / Schlüssel
  - Inhärenz-Faktoren
    - Fingerabdruck / Retina-Scan

Multifaktor-Authentifizierung

- Multifaktor-Authentifizierung prüft >1 Faktoren
  - aus unterschiedlichen Klassen!
  - 7 Geisslein: Stimme + Pfote ist nicht multifaktor (beides biometrisch)
  - 2FA: Two-Factor-Authentification
  - Motivation:
    - Unterschiedliche Angriffs-Vektoren:
      - Schlüssel: physisch einfach zu stehlen, schwierig at scale
      - Kennwort: via Virus / Keylogger relativ einfach, einfach at scale
      - Mobiltelefon: traditionell schwierig, immer dabei, es gibt immer mehr Attacken.

Probleme bei Multifaktor-Authentifizierung

- Verlust eines Faktors
  - Mobiltelefon / Schlüsselverlust
- Am besten mehrere Alternativen bereithalten:
  - Streichliste auf Papier
  - SMS
  - App

Aufgabe

- Überlegen Sie sich, welche Ihrer Konten Ihnen am meisten bedeuten.
  - bzw. deren Verlust Sie am meisten stören würde.

- Schalten Sie 2FA ein! Jetzt!
  - tiktok instagram facebook snapchat twitter
  - galaxus digitec zalando
  - gmail microsoft apple