openHPI Course: Digital Identities – Who am I on the Internet?

Authentication Methods: Knowledge, Ownership, Biometrics, Behavior

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

Digital Identity: Authentication

We already know that a person must provide proof in order to use a particular digital identity

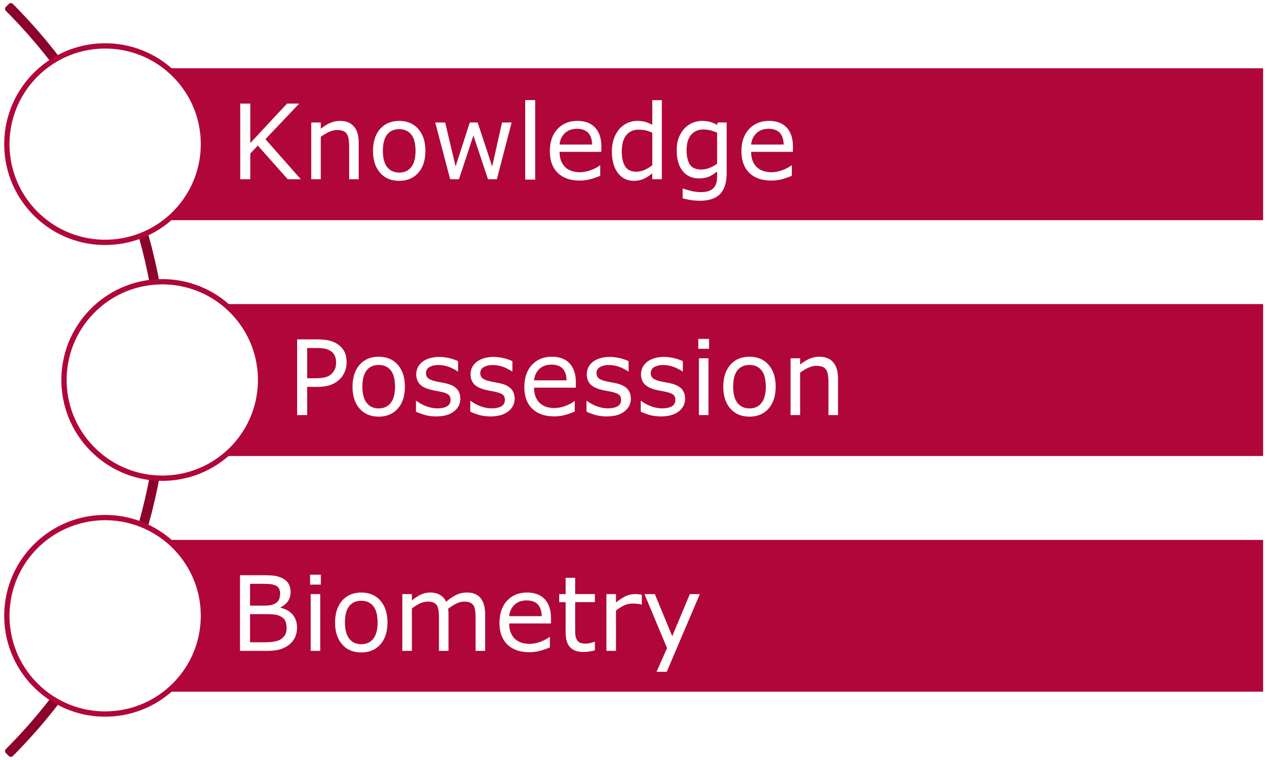
- Process for proving ownership of a digital identity requires **authentification** and **authentication**
  - **Authentification**: Produce evidence to the system
  - **Authentication**: System validates the evidence

Most popular authentication method: **Password entry**

- A person produces evidence by knowing a password that he or she owns a digital identity

Types of Authentication

In addition to the use of passwords, there are other types of authentication. Authentication can be based on:



Knowledge

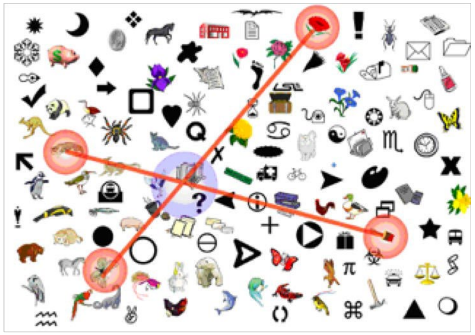
Possession

Biometry

Authentication through Knowledge

In the case of authentication through knowledge, the knowledge of a secret is checked

- Text secrets
  - □ password
  - □ PIN
  - □ …
- Graphical Secrets
  - □ detect specific points in an image
  - □ select pictures with friends on them
  - □ …



Authentication through Knowledge
Advantages and Disadvantages

Advantages:

- Widespread used
  → everyone knows how it works, simple application
- Secret can be changed at any time
- No special hardware required

Disadvantages:

- Security depends on complexity of the secret
  - the more complex the better
  - but the more difficult to remember
- Too many secrets are hard to remember
- Others can guess the secret or systematically find it out

Authentication through Ownership

In the case of authentication by ownership, the existence of a particular object is checked

- signet ring (earlier)
- identity card / membership card
- USB token
- …

After "showing" the object, access is granted

Authentication through Possession
Advantages and Disadvantages

Advantages:

- No special knowledge necessary

Disadvantages:

- Object in ownership can be lost
- Object in ownership can be stolen and thief can get direct access to digital identity
- Often additional hardware is required, e.g. card readers

Authentication through Biometric Features

Biometric authentication is based on the verification of:

- Physical characteristics
  - fingerprint
  - facial shape
  - iris
  - …
- Behaviour
  - Running behaviour
  - Typing behaviour
  - Movement patterns
  - …

Authentication through Biometrics
Advantages and Disadvantages

Advantages:

- No knowledge necessary
- No ownership necessary
- Biometric features are unique to each person

Disadvantages:

- Special hardware required to record a physical characteristic
- May include sensitive information
- Testing not possible exactly, but only with probability
  - enables the production of counterfeits
  - counterfeiting only has to be "good enough”
- Once a feature is compromised, it is impossible / difficult to change
  - fingerprint can only be changed nine times ...

Multi-Factor Authentication

To compensate for disadvantages of the single authentication methods, two or more methods are combined simultaneously:

- **Multi-factor authentication** (MFA) refers to the simultaneous combination of several different authentication methods or factors
- **2-factor authentication** (2FA) refers to a combination of 2 different methods or factors

Example 1: Cash Card for access to bank account

- 1st factor: **ownership** of the card
- 2nd factor: **knowledge** of the PIN

Example 2: Website account with 2FA

- 1st factor: **knowledge** of password
- 2nd factor: **ownership** of smartphone with TAN generator

Types of Authentication
Summary

- There are three classed / factors of authentication
  - knowledge
  - ownership
  - biometrics (physical characteristic and behaviour)
- Each of these classes / factors has its advantages and disadvantages
- Secure method of authentication is simultaneous combination of several types / factors
  - 2-factor authentication (2FA)
  - multi-factor authentication (MFA)
- However, combination increases security at the expense of usability, more steps are needed to produce authentification evidence