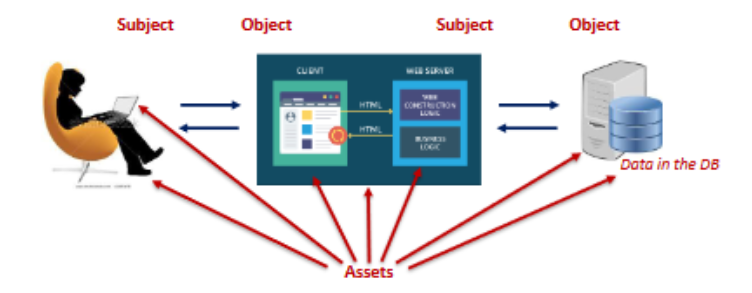
Access Control

Basic Concepts

* Assets: information, systems, devices, facilities, personnel
* Subject: active entity that access a passive object to receive information from, or data about, an object
* Object: passive entity that provides information to active subjects



Main Process

1. Identify & authenticate subjects attempting to access resources
2. Determine whether access is authorized
3. Grant or restrict access based on subject’s identity
4. Monitor and record access attempts

Types of Access Controls

Types of access controls according to intention of control:

* Preventive: hamper or stop unwanted / unauthorized attempt (penetration testing)
* Detective: discover or detect unwanted / unauthorized attempt (monitoring access)
* Corrective: remediate problems occurring as result from incident (rebooting / quarantine)
* Deterrent: discourage violations (locks, cameras, …)
* Recovery: repair or restore afterwards (backups)
* Directive: control actions of subjects (procedures)
* Compensation: alternative when primary control impossible (hardware token – smartcard)

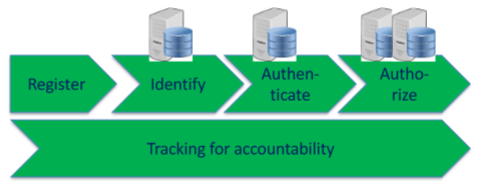
Types of access controls according to area of implementation

* Administrative: policies, procedures, regulations (trainings, HR policies, …)
* Logical / technical: hardware / software mechanisms (encryption, firewall, …)
* Physical: can be touched physically (cameras, dogs, locks, …)

Steps in Access Control

Providing access always consists of two steps:

1. Identification: subject’s claim of identity
2. Authentication: verify access to identity by comparing one or more factors against a database of valid identities



And additionally:

* Registration: check identity and, if successful, provide an account
* Authorization: granting subjects access to certain objects based on proven identities
* Accountability: tracking of subjects performing actions on objects makes it possible to hold subjects accountable of their actions

Authentication

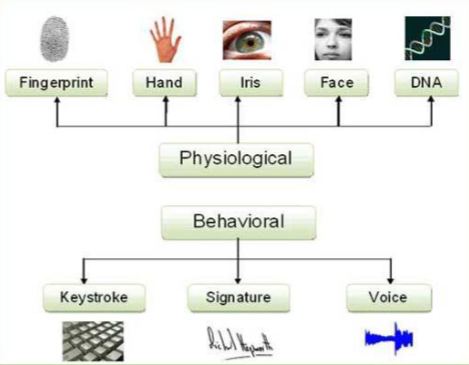
Authentication factors

* Type 1: something you know (password, PIN) 🡪 weakest
* Type 2: something you have (smartcard, hardware token) 🡪 middle
* Type 3: something you are or something you do (fingerprint, iris patters / signature, keystroke) 🡪 strongest

Type 1: Passwords / PINs

Problem: not carefully chosen, rainbow tables

Type 2: Devices like smartcards / token (🡪 password generation)

* Smartcard: integrated chip for identification and / or authorization
* Token: generating password synchronous (time-based) or asynchronous (algorithm-based)
* Problems: what if battery is empty or device breaks?

Type 3: Biometrics

* Problem: biometrics are not 100% reliable
  + Physiological are better than behavioural ones (behaviour can be trained)
  + The lower the ERR (y-axis), the better

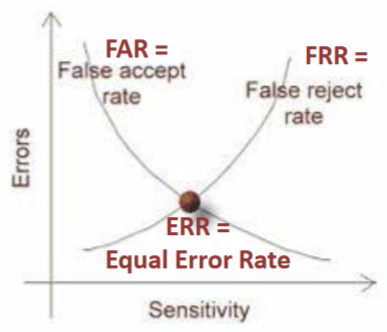
Diagram:

 Table for biometrics:

Best possible solution for problems: Multifactor Authentication

* At least two different types of authentications
* Trying to hack needs several attack methods combined 🡪 deterrent

Types of Identity Management

* Decentralized (distributed) access control
  + Various entities throughout a system perform authorization verification
* Centralized access control (single sign-on)
  + All authorization verification is performed by a single entity within a system
* Federated identity management (Eduroam, identity as service)
  + Extends IM beyond a single organization into a federation, formed by several organizations
* User-centric identity management (Blockchain)
  + Across several organizations, without a federation, sometimes even self-controlled

Access Control Models

* Basic Concepts:
  + Permission: access granted to an object and the actions that can be taken
  + Right: ability of a user to take an action on an object
  + Privilege: combination of permission and right
  + 🡪 Rights are something you have were granted to you, while permissions are something that the resources you need are configured to require
* Authorization Mechanisms
  + Access Control Matrix: table showing privileges on objects
  + Capability table: table showing subjects and their privileges on objects
  + Constrained interface: not showing all functions to everyone
  + Need to know, least privilege: principle for granting access
  + Separation of Duties and Responsibilities: sensitive functions are split into tasks to be performed by more than one person
  + Some more

Discretionary Access Control (DAC)

* A system that deploys DAC allows the owner / creator / custodian of an object to control and define access to that object to specific subjects
* DAC is implemented with access control lists on objects
* Problem: DAC cannot be controlled centrally because owner can change rights at any time

Non-Discretionary Access Control (non-DAC)

* A system that deploys non-DAC has administrators controlling access according to some principles
* Non-DAC is role-based, rule-based, attribute-based or mandatory