User authentication

Accomplished by → Four methods

Executed by two steps:
1. Identification: picking out the user from among the users with access to the system
2. Verification: determining the person requesting authentication is the same as the person identified

Four methods
- which depend on
  - Something the individual is
    - like → Fingerprints, Iris scan, Retina scan → which vary greatly in → cost and accuracy
  - Something the individual does
    - vulnerable to → Impersonation
    - like → Voice (uniqueness of voices)
    - Typing speed (people have different typing speeds)
  - Something the individual possesses (e.g. keycard)
    - implemented by → Keycard
      - like → Smart card: can process information
      - Magnetic strip card: passive information in strip
      - Memory card: passive information (more than strip)
    - vulnerable to → Token theft
  - Something the individual knows (e.g. passwords)
    - vulnerable to → Password cracking → ameliorated by → Strong passwords, salt
- which exhibit
  - Vulnerabilities
    - like → Password cracking
    - which can be protected against by → Countermeasures → like → Strong passwords, salt