Two types of attacks revolving authentication
  - Eavesdropping
  - Replay Attacks

Card Types
  - Embossed (raised characters, physical based)
  - Magnetic Stripe (credit card)
  - Memory (prepaid phone card)
  - Smart (Contact & Contactless) (contactless utilizes RFID or something of the sort) (biometric ID card)
  - Issue: All are physical, and can be stolen

Memory Cards
  - Physical access
    - ATMs, Hotel room cards, etc
  - Stores information, doesn’t process
  - Sometimes works in combination of a pin

Smart Tokens
  - Manual/electric interface
  - Electrical interfaces with some sort of reader/writer
  - Types
    - Static (password remains the same)
    - Dynamic (password changes on the fly)
    - Challenge-Response (password is dynamic, prevents replay attacks)

Smart Cards
  - Contains microprocessors
    - Typically performs some hash algorithm
  - Contains memory (flash, rom, eeprom)
  - Very similar to smart tokens
  - Dynamic, Static, Challenge Response
  - Typically dynamic is time-synced, and uses that as it’s variable

Biometrics
  - Authenticates off of physical features (using patterns)
    - Facial, Voice, Signature, Fingerprints
  - Expensive
  - Technically Complex
○ More accurate, more cost
○ False-positives should be taken in consideration
  ■ Low-amount could result in low usability
  ■ High-amount is insecure
○ Iris identification is the best solution

● Direct Authentication
  ○ No potential of MITM (man-in-the-middle) attack
  ○ Not done over a network

● Remote User Authentication
  ○ Done over a network
  ○ Needs to prevent replaying / eavesdropping
    ■ Solution
      ● Client sends request
      ● Host responds with a Random Number
      ● Client that hashes their password, in addition to hashing once again with the random number
        ○ hash(randomnumber + hash(password))
      ● Host Verifies & Responds