Access Control

bottom line: controlling access
- how does this occur on campus? at a military base? at Google? in the cyberLAB?
- how does this occur on land? on the sea? in the air? in space? underground?
- how does this occur on information technology/computer information systems?

logic?
- tools and protocols in computer information systems used for:
  - identification: making a claim attesting to one's identity
    - who are you?
  - authentication: confirming truth claimed true by some entity (i.e., confirming identity)
    - are you who you say you are?
  - authorization: specifying access rights to resources
    - are you allowed to access this?
  - accountability: acknowledgment and assumption of responsibility for actions
    - you screwed up, so I will temporarily reduce your access and log the incident

- enforce access control measures for systems, programs, and information
  - at various levels (e.g., OS, apps, security packages, databases, etc)

examples in computer information systems
- identification and authentication:
  - user name and password
  - physical biometrics
  - behavioral biometrics
  - key fobs and dongles
  - ?
- authorization:
  - file permissions
  - dongles
  - ?

examples in other areas (e.g., airports, military bases, etc)?

threat avoidance sidebar
- threats simply don't matter
- we don't care about detection, mitigation, prevention, attribution
- we have an invisibility cloak
- e.g., beaconing malware, unauthorized network users/apps, port knocking

port knocking
- ports are the only way for remote users to get in
- if ports are closed, no one can get in
- wouldn't it be cool if we could monitor special packets at a lower level?
- and then perhaps selectively open ports temporarily for specific remote users

- forms:
  - knock on several ports in a timed sequence

knock on a single port with a symmetric key
knock with a client key (SPA: single packet authorization)

is port knocking a form of access control?

tutorials
fwknop
chroot jail