Intro Lecture!

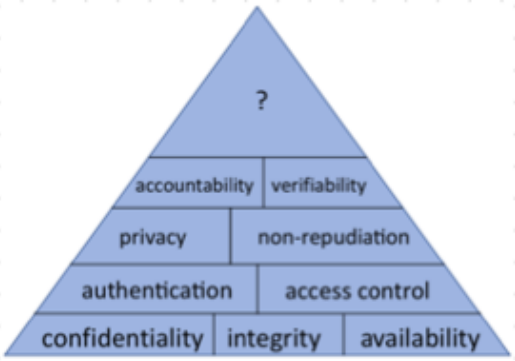
- In Security Assumptions will be broken!!!

Security Goals

- Confidentiality → Eavesdropping, man-in-the-middle.
- Integrity → masquerading, message tampering, replaying.
- Availability → Denial of Service.

So... what does it mean that a system is secure?!?

- We can take a look at the following:



- The pyramid shows what is needed to for a system to be secure
- many other aspects can apply!

We can say that "Security is impossibly hard"!

- you must defend against all possible attacks
- adversary needs to find just one attack that works
- ~~∃~~ no perfect security
- Security is measured in the resources required of the adversary!

Security Principles

- Economy of Mechanism:
  - Keep it simple!
  - Complex design yields complex failure analysis!
- Open Design:
  - Security of the system should not depend on secrecy of its protection mechanisms.
  - The adversary knows the system!
- Minimum Exposure:
  - Minimise the attack surface a system presents
  - Reduce external interfaces
  - Limit info & window of opportunity!

- **Least Privilege:**
  - Any component should use the least set of privileges.
  - Restrict email access, Powerpoint doesn't run as root.
- **Fail Safe Defaults:**
  - Start & end in a secure state
  - If failure, no-one has access!
- **Complete Mediation:**
  - Access to anything must be controlled!
  - OS access to file sys, circumvented if access to physical disk is possible!
- **No single point of failure**
  - Build redundant security!
  - Separation of duty is key!
- **Psychological Acceptability:**
  - Design usable things!!!
  - Help user to make the right choice!