BSc

Daniel Guldberg Aaes

Spring 2020

Lecture 1

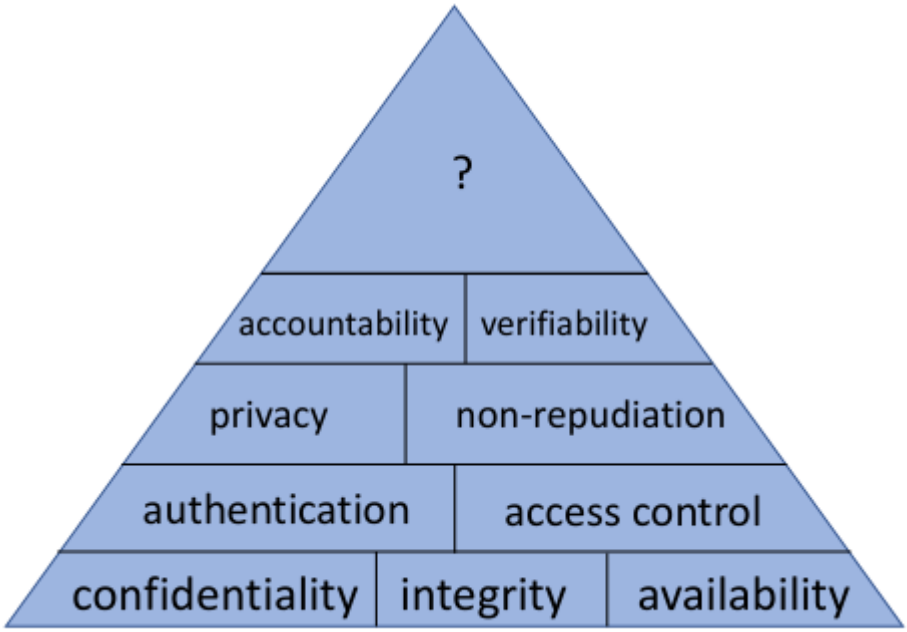
What is cyber security

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks coming from activists, criminals, states and so on.

Security Assumptions

Each assumption can be a potential vulnerability. For an example, forcing a user to use a complet password will fail if he put it on a stickit note

Security Goals



- **Confidentiality**
  - Attacks: eavesdropping, man-in-the-middle
- **Integrity**
  - Attacks: masquerading, message tampering, replaying
- **Availability**

  - Attacks: Denial of Service, distributed denial of service

- **Accountability** if I can't prevent it I can figure out who made the attack, maybe through logs.
- **Authenticity** (not covered in the lecture)

Security Principles

- **Economy of Mehanism**
  - Keep it simple, complex designs yields complet failure analysis
- **Open design** (not open source)
  - The security of a system should not depend on the secrecy of its protection mechanisms."
  - The adversary knows the system.
- **Minimum exposure**
  - "Minimise the attack surface a system presents to the adversary."
  - Reduce external interfaces (if they aren't needed).
  - Limit information and limit window of opportunity.
- **Least priviilige**
  - "Any component should operate using the least set of privileges necessary.".
- **Fail-safe defaults**
  - "The system should start in and return to a secure state in the event of a failure."
  - white/blacklist (firewalls)
- **Complete mediation**
  - "Access to any object must be monitored and controlled."
- **No single point of failure**
  - "Build redundant security mechanisms whenever feasible."
  - Key technique: separation of duty
- **Psychological acceptability**
  - "Design usable security mechanisms"
  - Help the user to make the right choice

Wrapping up

- **Adversary**: state-sponsored cyber attacks
- **Assumptions**: as few as possible
- **Goals:** as many as possible
- **Principles**: as many as possible