Agenda

- Goals of Security
- Policy and Mechanism
- Assumptions and Trust
- Assurance
- Operational issues
- Human issues
- Security life-cycle

Goals of Security

- *Prevention:* *P*revention involves implementation of mechanisms that are trusted to be implemented in a correct and unalterable way, so that the attacker cannot defeat the mechanism by changing it.

- *Detection:* *Detection mechanisms accept that an attack will occur; the goal is to determine that an attack is underway, or has occurred, and report it.*

- *Recovery:* *Recovery stops an attack and tries to assess and repair any damage caused by that attack.*

Policy and Mechanism

- A *security policy is a statement of what is, and what is not, allowed.*

- A *security mechanism is a method, tool, or procedure for enforcing a* security policy.

Assumptions and Trust

- Security rests on **assumptions** specific to the type of security required and the environment in which it is to be employed.
- An entity is *trustworthy if there is sufficient credible evidence leading one* to believe that the system will meet a set of given requirements. ***Trust*** *is a measure of* trustworthiness, relying on the evidence provided.

Assurance

- *Security assurance, or simply assurance, is confidence that an entity* meets its security requirements, based on specific evidence provided by the application of assurance techniques.

Operational Issues

- **Cost-Benefit Analysis:** The benefits of computer security are weighed against their total cost.
- **Risk Analysis:** To determine whether an asset should be protected, and to what level, requires analysis of the potential threats against that asset.
- **Laws and Customs:** Laws restrict the availability and use of technology and affect procedural controls.

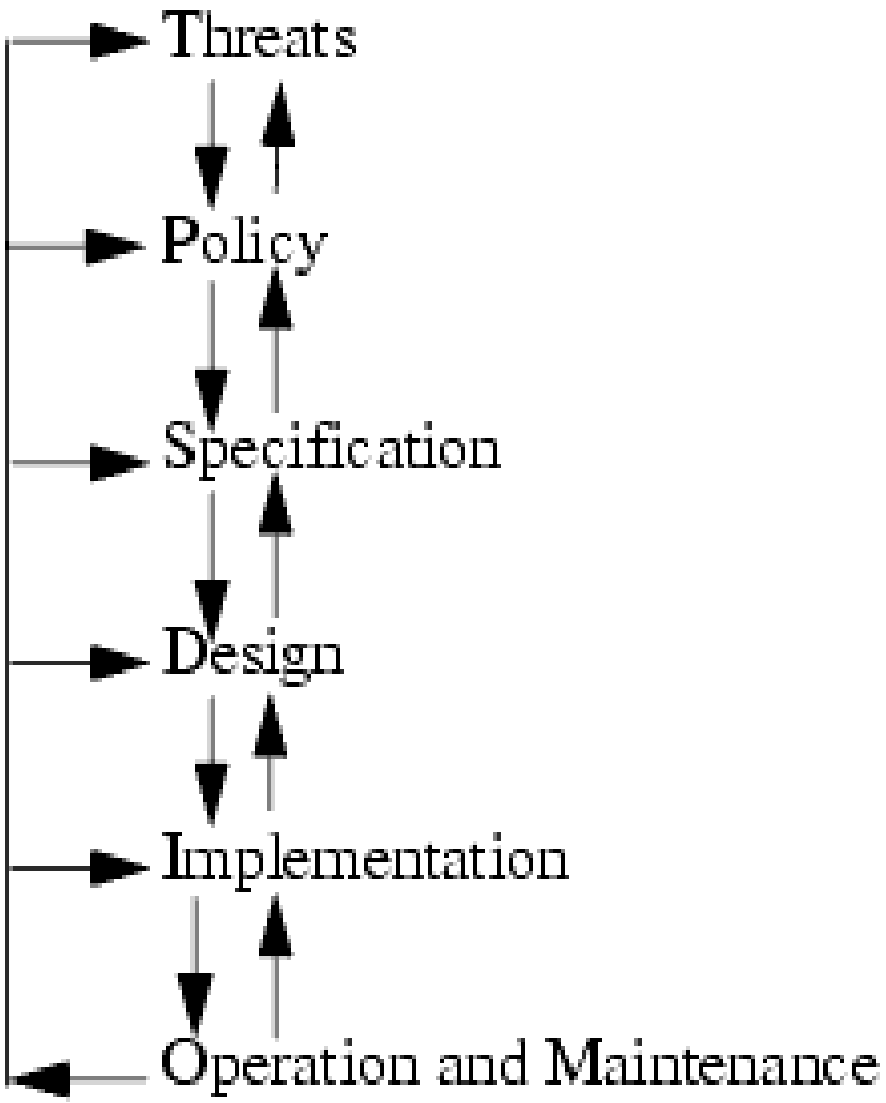
Human issues

- **Organizational Problems:** The most common problem a security manager faces is the lack of people trained in the area of computer security.

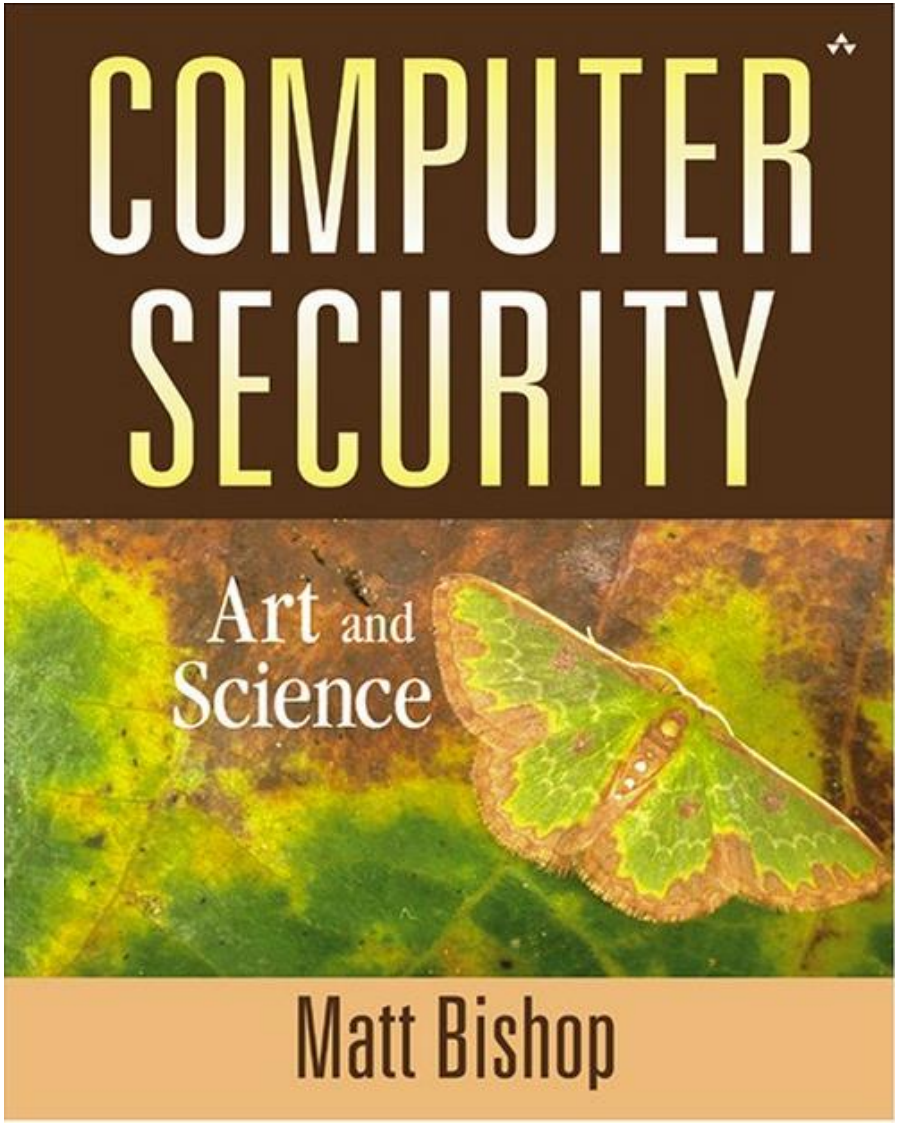
- **People Problems:** Untrained personnel also pose a threat to system security.

Ref. *Matt Bishop [pages: 104-105]*

Security life-cycle



Book



Thank You