

LO2-6.857

2/2/22

Outline: Finish list of "security principles"  
Killian Award lecture

Security mechanisms:

prevention

detection/recovery

(deterrence)

Who is adversary?

outsider/insider

assumptions about capabilities

corruption

computation

communication

Vulnerabilities

threat

risk

risk management

---

identification

authentication

authorization

physical protection

cryptology

economics

deception

randomness

Be skeptical & paranoid

Don't aim for perfection

"Only degrees of insecurity"

Be prepared for loss

Tradeoff cost / security

KISS "Keep it simple, stupid"

Ease of use

Separation of privilege

complete mediation

least privilege

education

transparency