Introduction into Computer Security

EECE 412

Session 2

Outline

- Miscellaneous
- Last session re-cap
- Introduction into computer security
- Upcoming important dates and action items
- Next session preview

Introduction to Computer Security

Goals of Security

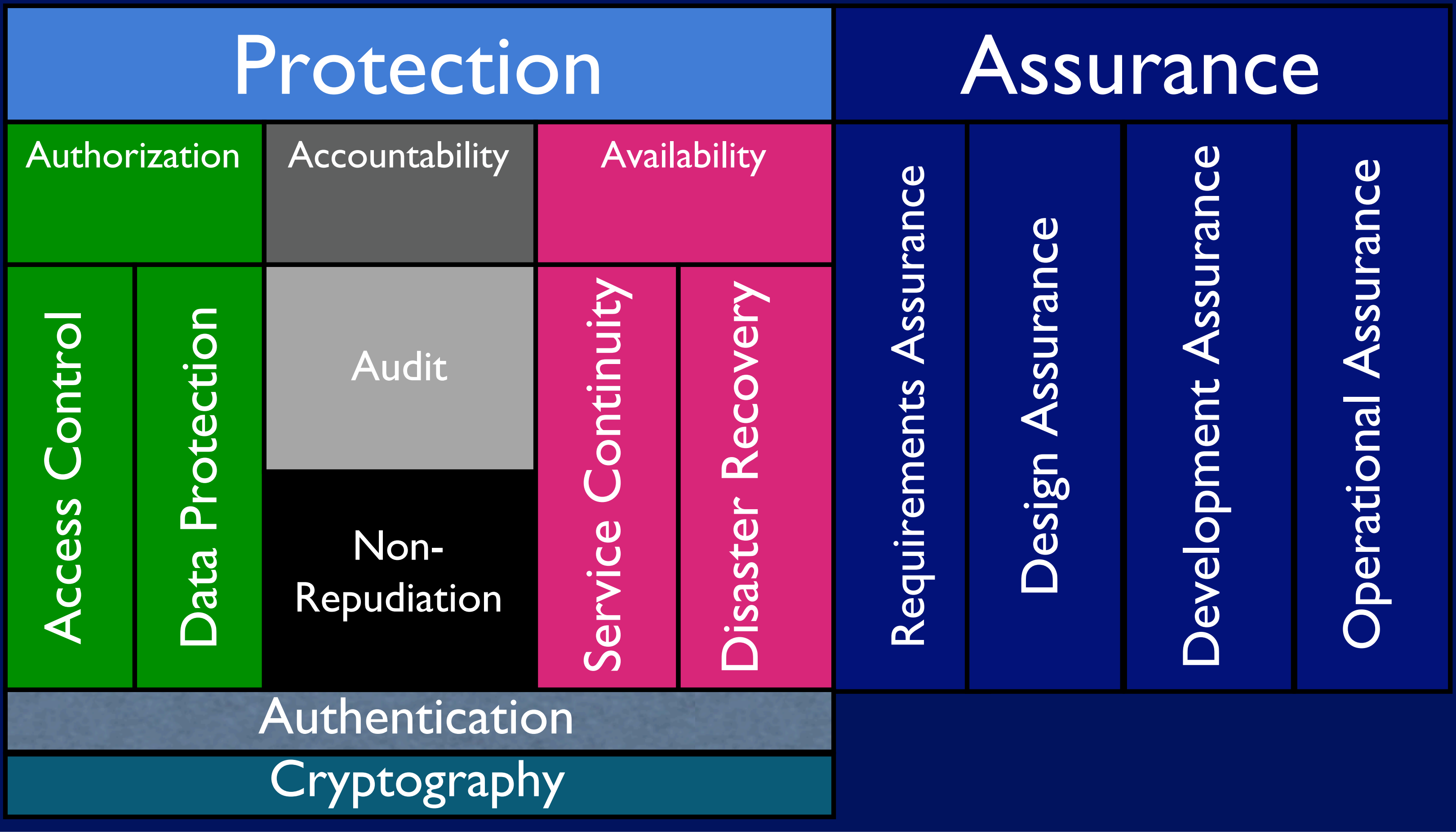
- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers’ violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

What Computer Security Policies are Concerned with?

- Confidentiality
  - Keeping data and resources hidden
- Integrity
  - Data integrity (integrity)
  - Origin integrity (authentication)
- Availability
  - Enabling access to data and resources

CIA

Conventional Approach to Security



Protection

Authorization

Access Control

Data Protection

Accountability

Audit

Non-Repudiation

Availability

Service Continuity

Disaster Recovery

Authentication

Cryptography

Assurance

Requirements Assurance

Design Assurance

Development Assurance

Operational Assurance

Protection

- provided by a set of mechanisms (countermeasures) to prevent bad things (threats) from happening

Authorization

protection against breaking rules

Rule examples:

- Only registered students should be able to take exam or fill out surveys
- Only the bank account owner can debit an account
- Only hospital's medical personnel should have access to the patient's medical records
- Your example…

Authorization Mechanisms: Data Protection

- No way to check the rules
  - e.g. telephone wire or wireless networks
- No trust to enforce the rules
  - e.g. MS-DOS

Accountability

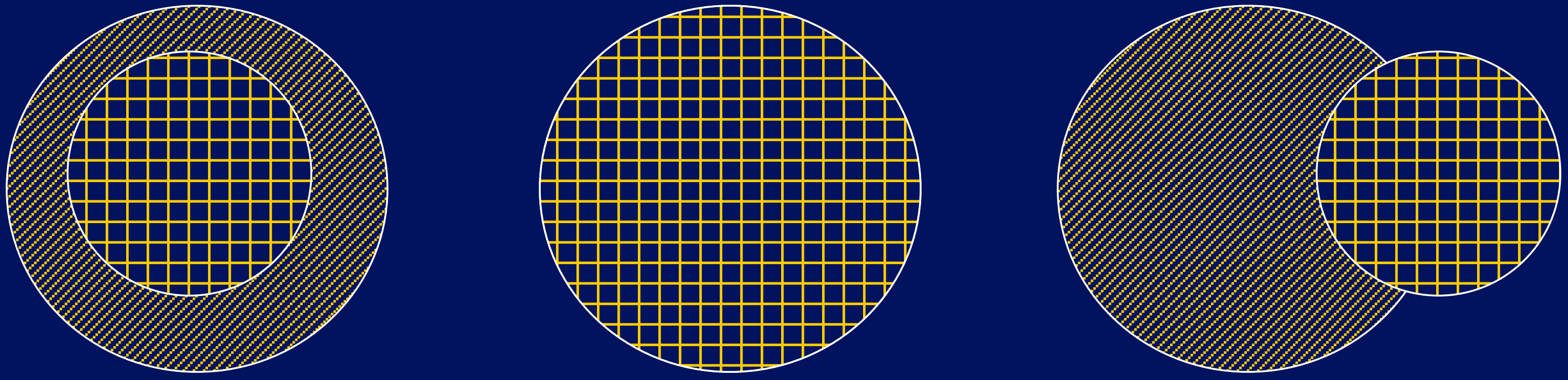
You can tell who did what when

- (security) audit -- actions are recorded in audit log
- Non-Repudiation -- evidence of actions is generated and stored

Availability

- Service continuity -- you can always get to your resources
- Disaster recovery -- you can always get back to your work after the interruption

Types of Mechanisms



secure

precise

broad

▦ set of reachable states

▨ set of secure states

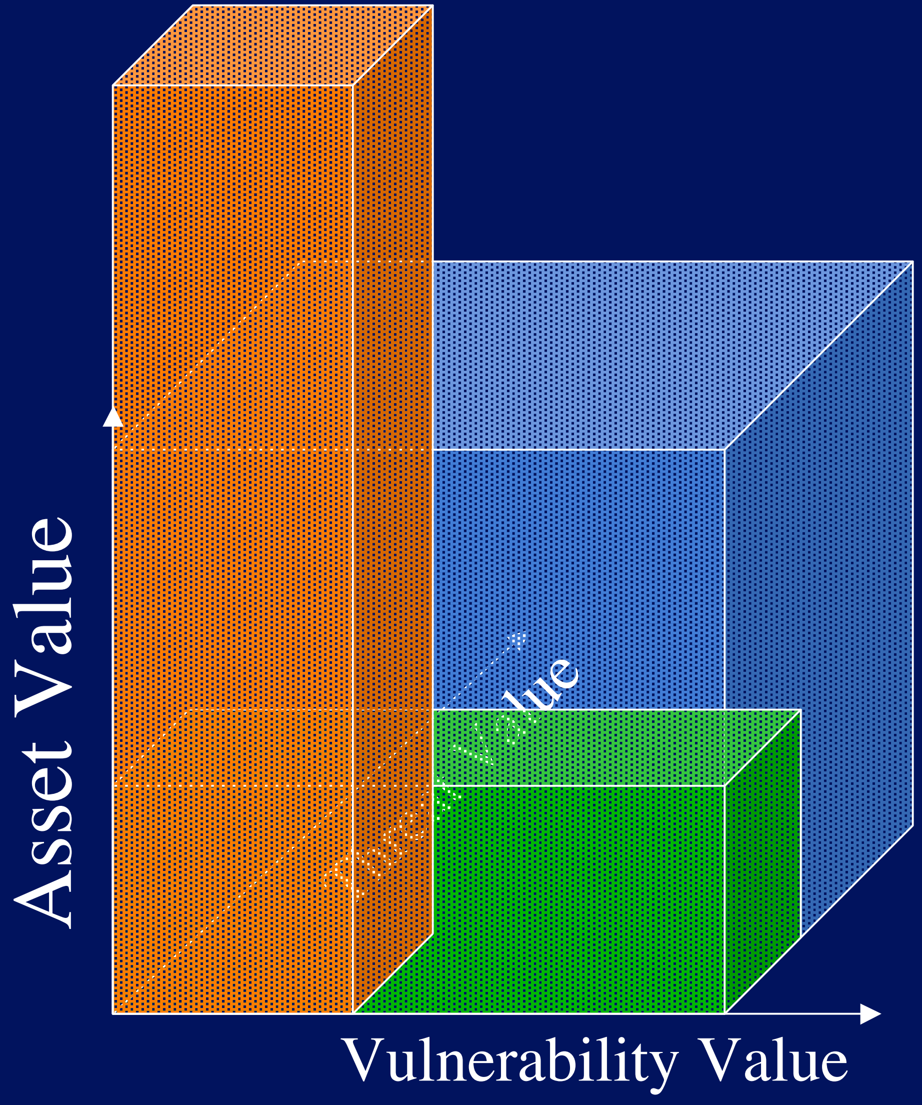
Assurance

Set of things the system builder and the operator of the system do to convince you that it is really safe to use.

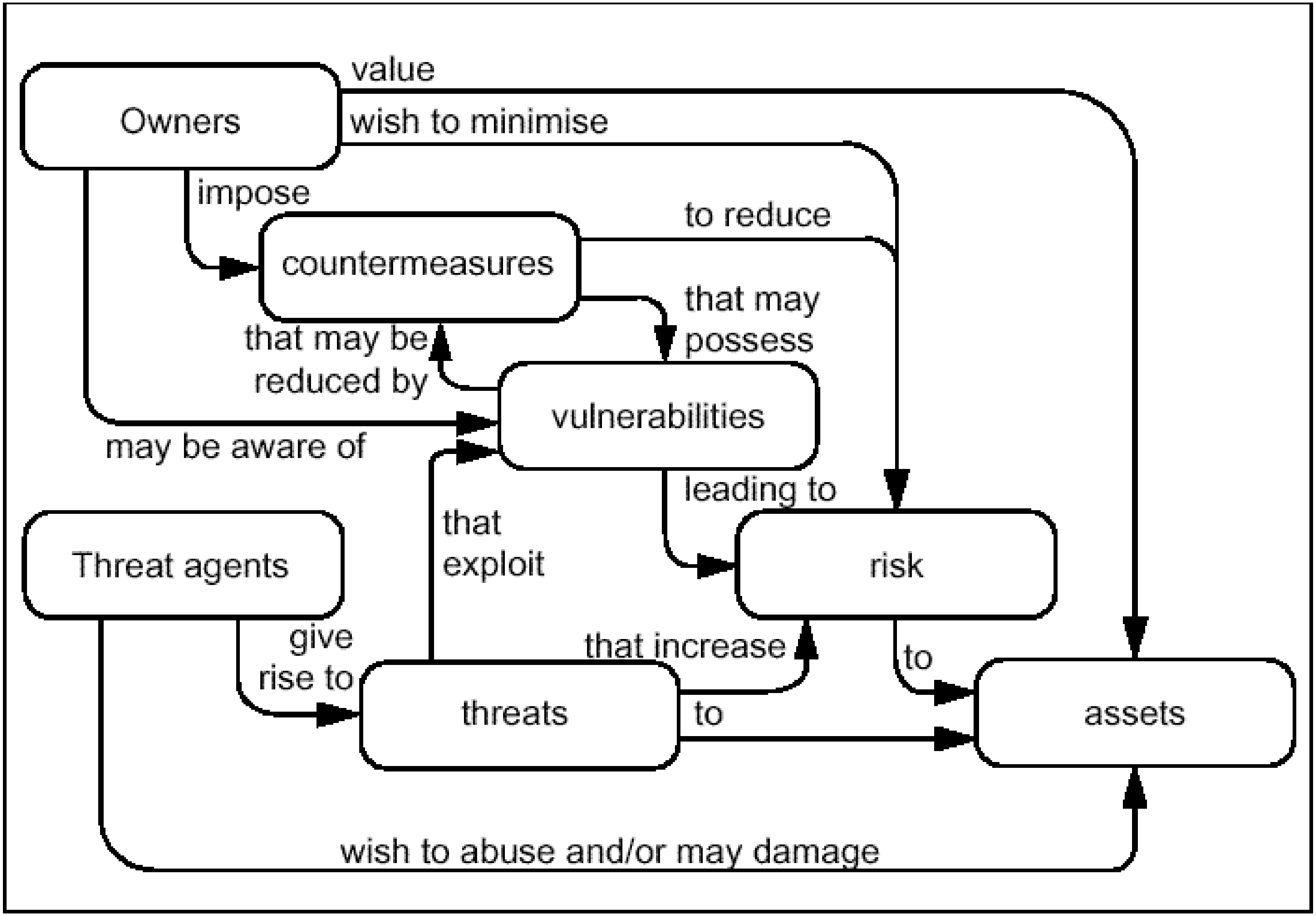
- the system can enforce the policy you are interested in, and
- the system works as intended

Securing Systems

It’s all about risk



Risk = Asset * Vulnerability * Threat



Source: Common Criteria for Information Technology Security Evaluation. 1999

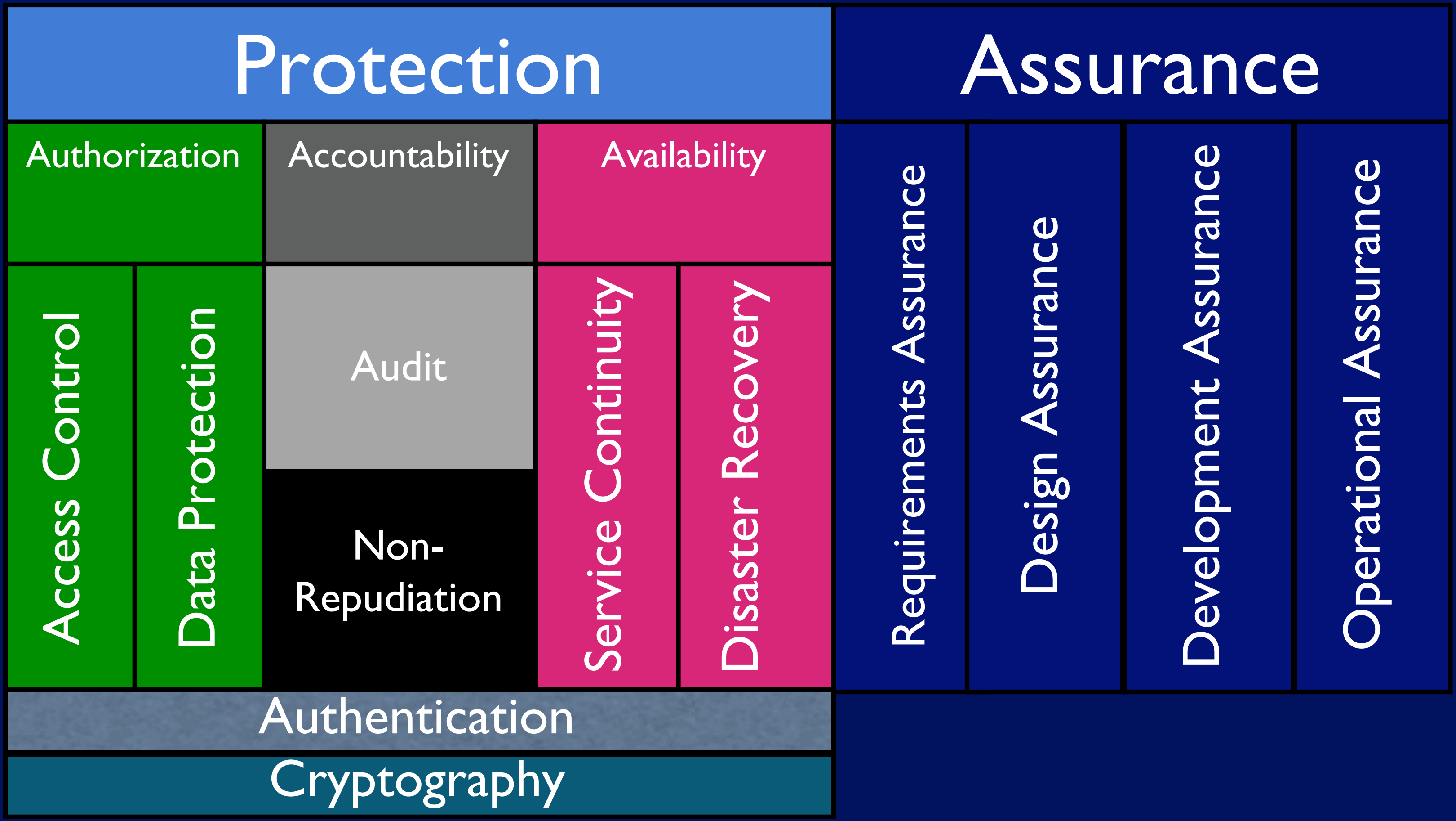
Steps of Improving Security

1. analyze risks
   - asset values
   - threat degrees
   - vulnerabilities
2. develop/change policies
3. choose & develop countermeasures
4. assure
5. go back to the beginning

Classes of Threats

- Disclosure
  - Snooping
- Deception
  - *Modification*
  - *Spoofing*
  - repudiation of origin
  - denial of receipt
- Disruption
  - *Modification*
  - denial of service
- Usurpation
  - Modification
  - *Spoofing*
  - Delay
  - denial of service

Key Points



Protection

Authorization

Access Control

Data Protection

Accountability

Audit

Non-Repudiation

Availability

Service Continuity

Disaster Recovery

Authentication

Cryptography

Assurance

Requirements Assurance

Design Assurance

Development Assurance

Operational Assurance

Key Points (cont-ed)

- *Secure*, *precise*, and *broad* mechanisms
- Risk = Asset * Vulnerability * Threat
- Steps of improving security
- Classes of threats
  - Disclosure
  - Deception
  - Disruption
  - Usurpation

Next session preview

- Introduction to Cryptography
  - Historical background
  - Random Oracle Model

Important dates
in the next three weeks

- 9/9 Optional “get to know” social at Koerner’s Pub 6 PM
- 9/15 online student entry survey due
- 9/20 Assignment #1 due