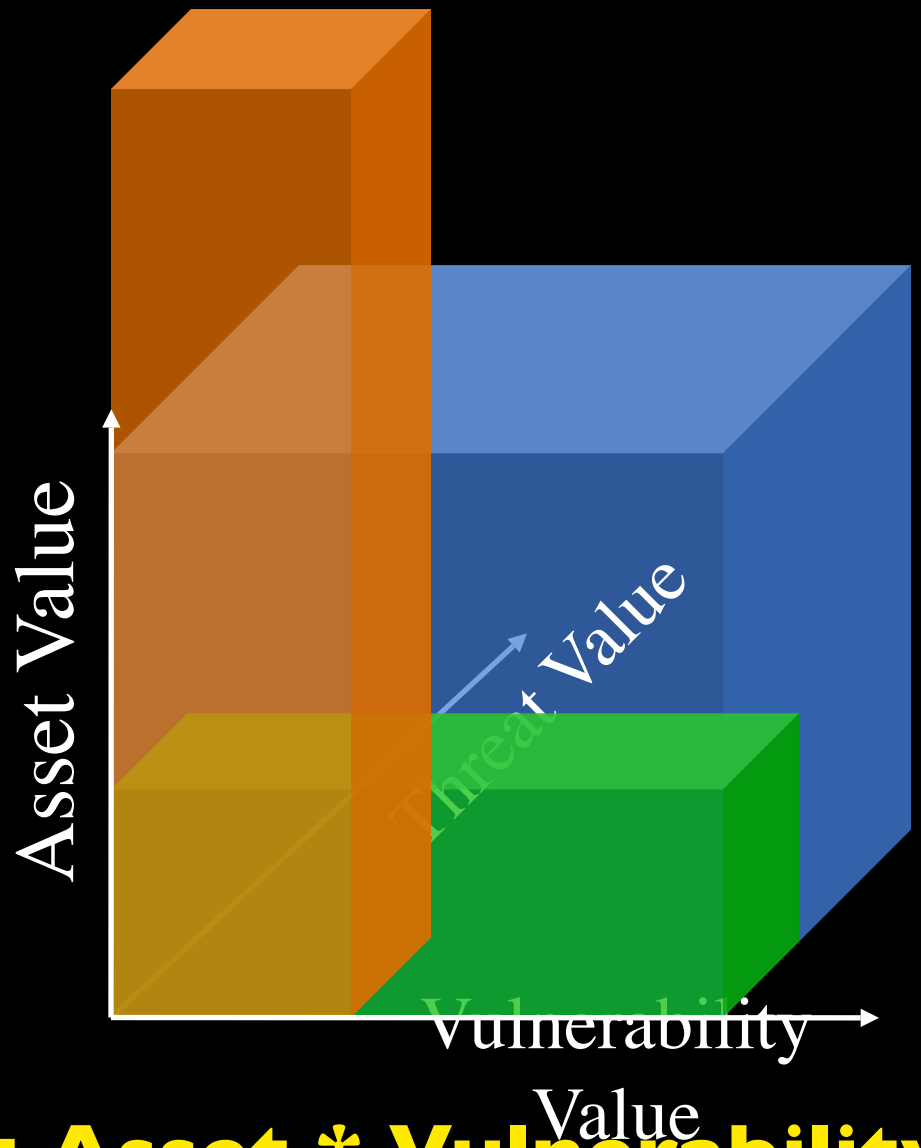
Introduction into Computer Security

What is Security?

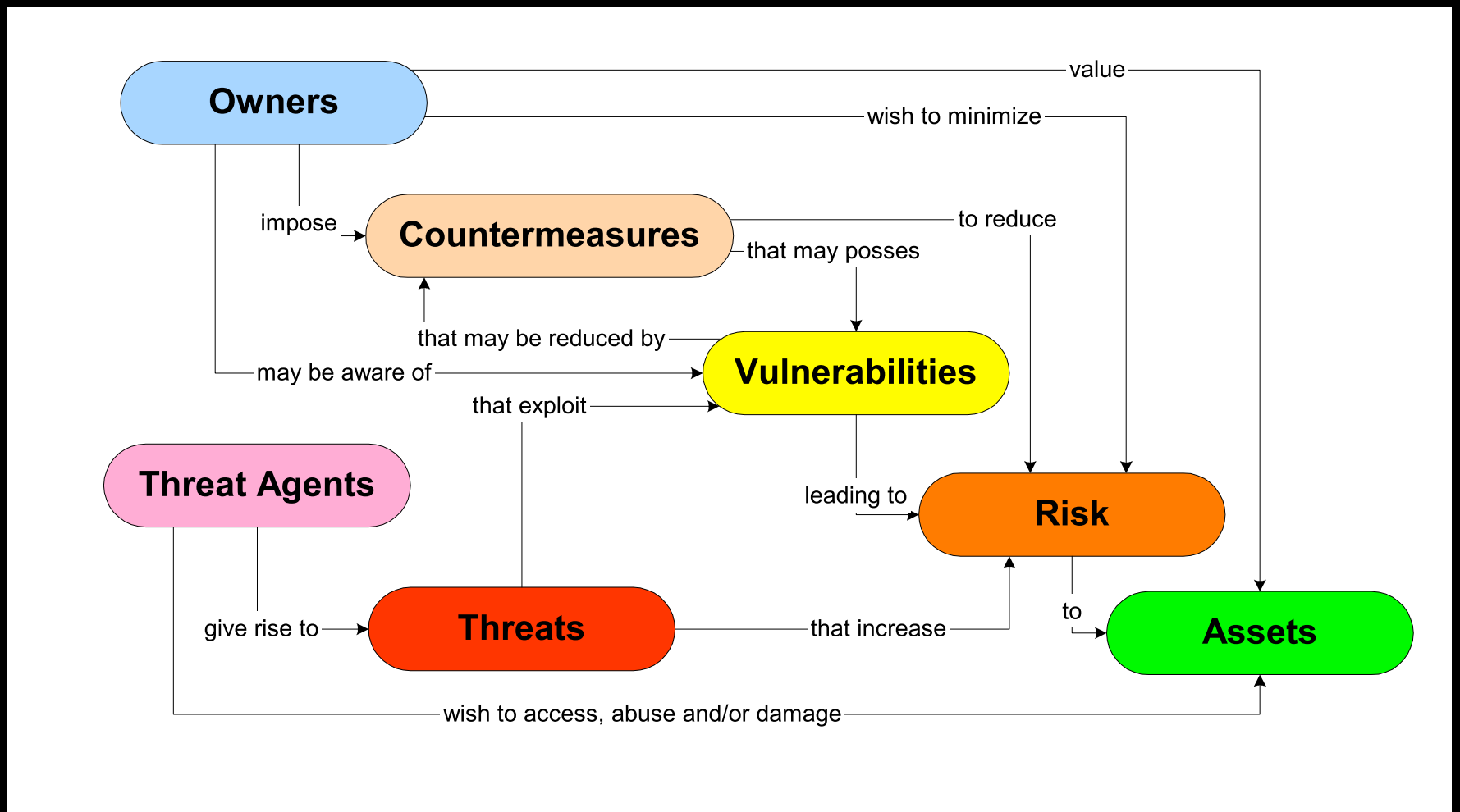
- security -- "safety, or freedom from worry"
- how can it be achieved?
  - Make computers too heavy to steal
  - Buy insurance
  - Create redundancy (disaster recovery services)



Risk = Asset * Vulnerability * Threat

What can be done about risk?

- Accept
- Avoid
- Transfer
- Reduce



Source: Common Criteria for Information Technology Security Evaluation. 1999

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

Goals of Security

- Deterrence
  - Deter attacks
- 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
- Investigation

Solovki Monastery, White Sea, Russia

Friday, September 5, 2008

Castle of Chillon

from www.picture-newsletter.com/chillon/

Conventional fortress-based security

Goal:

Prevent people from violating system's security policy

Means:

Fortification

- provides safety
- involves layering
- expensive

Some points about fortresses

- No absolute safety
- One weakness/error sufficient
- Extra layers at extra cost
- Important to understand threats
- Limited defender's resources
- Adjust to attacks
- Resource suppliers
- Distinguishing noncombatants from attackers
- Containment

Fortress Analogy Limitations

Fortress

- Against external attackers
- Protects only insiders
- Defenses cannot change

Computer security

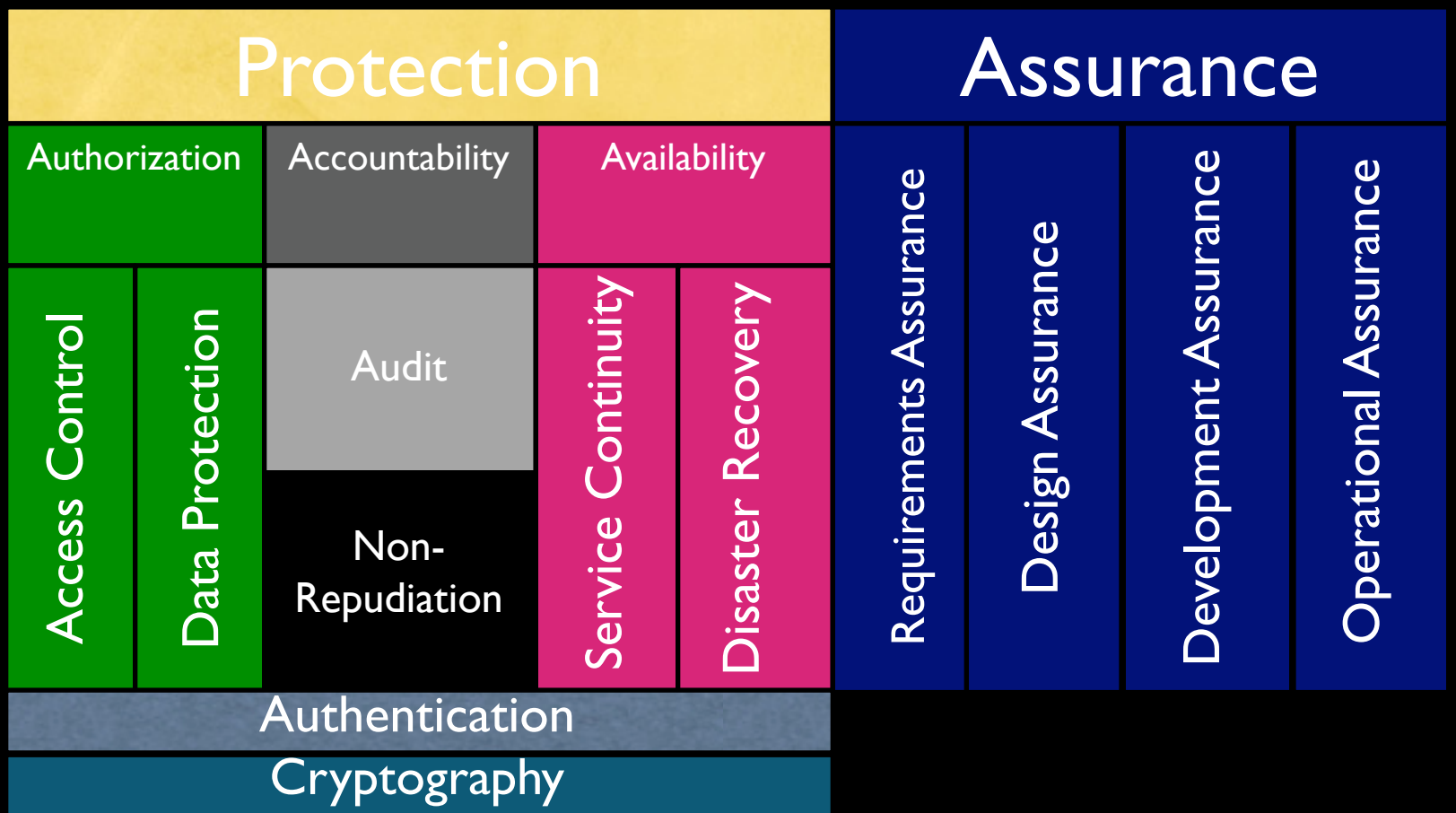
- Control of insiders
- Has to keep system usable
- Has to protect from new types of attacks

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

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

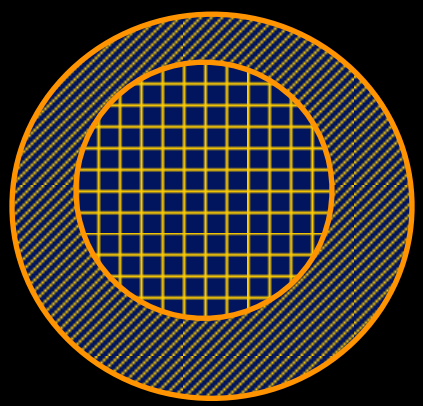
You can tell who did what when

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

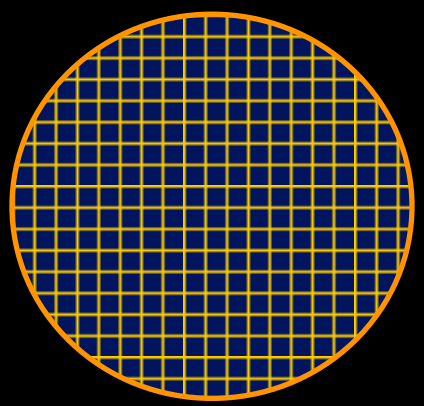
Availability

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

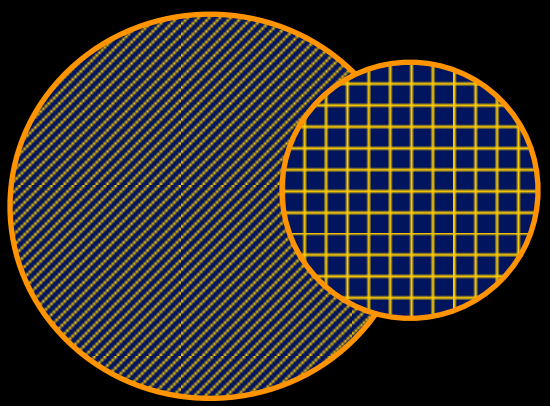
Types of Mechanisms



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.

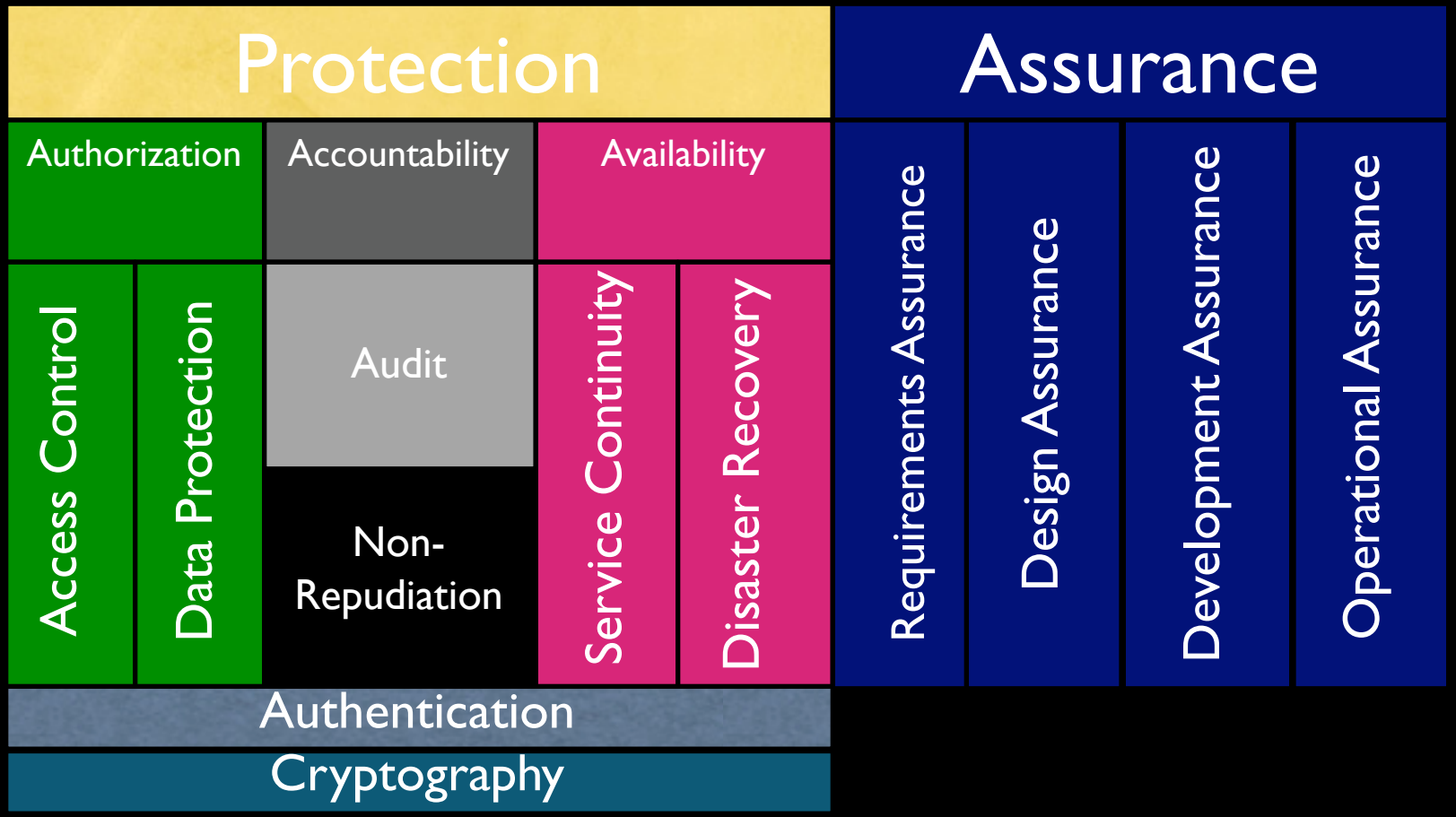
- the system can enforce the policy you are interested in, and
- the system works as intended

Securing Systems

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

Key Points


Protection
Assurance
Authorization
Accountability
Availability
Access Control
Data Protection
Audit
Non-Repudiation
Service Continuity
Disaster Recovery
Requirements Assurance
Design Assurance
Development Assurance
Operational Assurance
Authentication
Cryptography

Key Points (cont-ed)

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