THE UNIVERSITY OF BRITISH COLUMBIA

Introduction into Computer Security

1

what is "computer security"?

- security -- "safety, or freedom from worry"
- thesaurus: peace of mind, feeling of safety, stability, certainty, happiness, confidence.

2

Buddhist chant of metta (loving-kindness)

in Pali	in English
• Aham avero homi	• May I be safe, free from enmity and danger.
• Abyapajjho homi	• May I be at peace, free from mental suffering.
• Anigha homi	• May I be safe, free from physical suffering.
• Sukhi attanam pariharami	• May I take care of myself, and live happily.

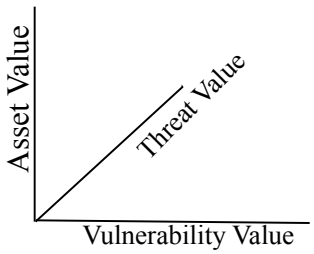
3

what is "computer security"?

- security -- "safety, or freedom from worry"
- thesaurus: peace of mind, feeling of safety, stability, certainty, happiness, confidence.
  - where does it come from?
- how can it be achieved?
  - make computers too heavy to steal
  - buy insurance
  - create redundancy (disaster recovery services)

4

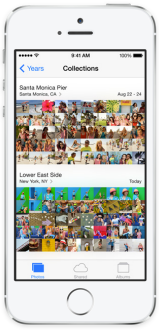
it's all about risk management



Risk = Asset x Vulnerability x Threat

5

example (photos on a smartphone)



from www.apple.com/ca/ios/whats-new/

6

what can be done about risk?

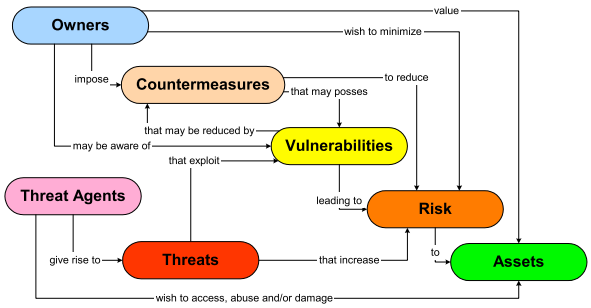
avoid

transfer

reduce

accept

7



Source: Common Criteria for Information Technology Security Evaluation. 1999

8

example: food for thought

analyze and suggest

- assets at risk and their value
- threats to these assets
- threat agents
- risk management

9

10

goals of computer 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**
  - Find out how the attack was executed: forensics
  - Decide what to change in the future to minimize the risk

11

Solovki Monastery, White Sea, Russia

12

13

Castle of Chillon

from www.picture-newsletter.com/chillon/

14

conventional fortress-based security

Goal: Prevent people from violating system's security policy

Means:

Fortification

- provides safety
- involves layering
- expensive
- requires maintenance
- eventually compromised

15

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

16

limitations of the fortress analogy

fortress

- against external attackers
- protects only insiders
- defences cannot change

computer security

- control of insiders
- has to keep system usable
- has to protect from new types of attacks

17

what computer security policies are concerned with?

Confidentiality

keeping data and resources hidden

Integrity

data integrity (integrity)

origin integrity (authentication)

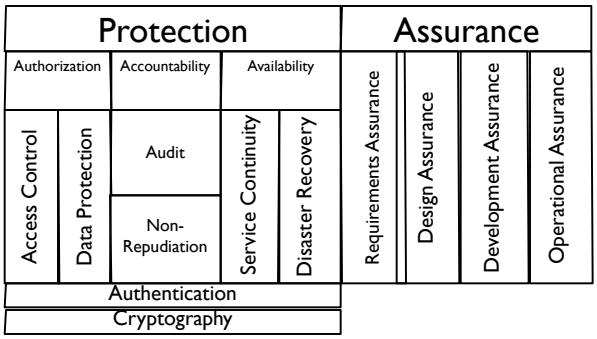
Availability

enabling access to data and resources

CIA

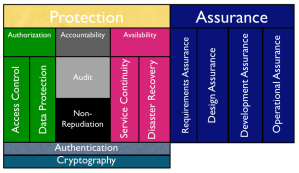
18

conventional approach to computer security



Protection

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

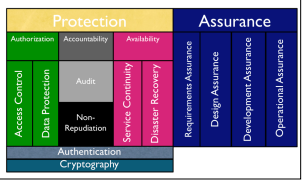


Authorization

protection against breaking rules

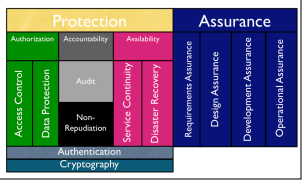
Rule examples:

- 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

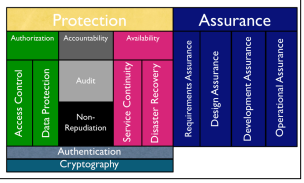
- No way to check the rules
  - e.g. telephone wire or wireless networks
- No trust to enforce the rules
  - e.g., mobile devices



Accountability

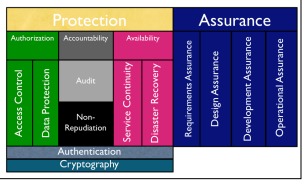
You can tell who did what when

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

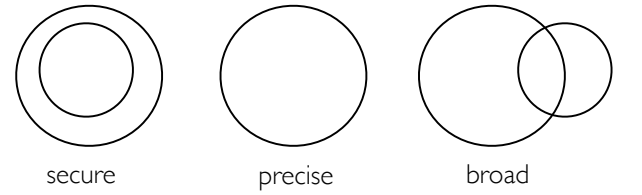


Availability

- 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



set of reachable states

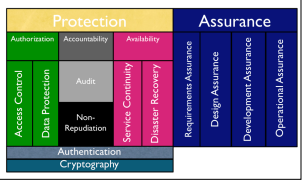
set of secure states

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

in the following scenario, analyze

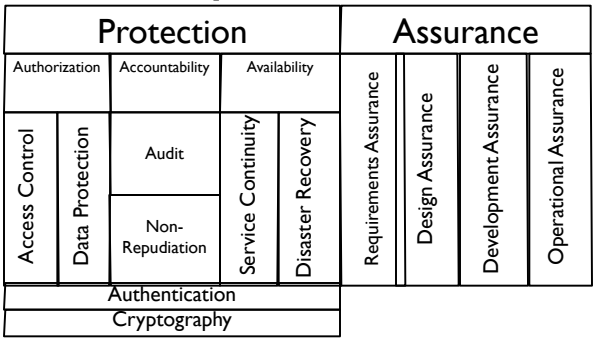
Assets at risk and their value

Threats to these assets

Threat agents

Ways to manage risk

Key Points



key points (cont-ed)

secure, precise, and broad mechanisms

Risk = Asset × Vulnerability × Threat

steps of improving security

classes of threats

- disclosure
- deception
- disruption
- usurpation