Information hiding

Security

Applications

Negotiation

Privacy

Integrity

Access control

Threats

Data provenance

Biometrics

Semantic web security

Fraud

Trust

POLICY MAKING

Encryption

Computer epidemic

Data mining

Anonymity

Formal models

System monitoring

Vulnerabilities

Network security

[cf. Csilla Farkas, University of South Carolina]

Examples – Security in Practice

Barbara Edicott-Popovsky and Deborah Frincke, CSSE592/492, U. Washington]

From CSI/FBI Report 2002

- 90% detected computer security breaches within the last year

- 80% acknowledged financial losses

- 44% were willing and/or able to quantify their financial losses.
These 223 respondents reported $455M in financial losses.

- The most serious financial losses occurred through theft of proprietary information and financial fraud:

  26 respondents: $170M
  25 respondents: $115M

- For the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).

- 34% reported the intrusions to law enforcement. (In 1996, only 16% acknowledged reporting intrusions to law enforcement.)

More from CSI/FBI 2002

- 40% detected external penetration
- 40% detected denial of service attacks.
- 78% detected employee abuse of Internet access privileges
- 85% percent detected computer viruses.
- 38% suffered unauthorized access or misuse on their Web sites within the last twelve months. 21% didn't know.
  [includes insider attacks]
- 12% reported theft of transaction information.
- 6% percent reported financial fraud (only 3% in 2000).

[Barbara Edicott-Popovsky and Deborah Frincke, CSSE592/492, U. Washington]

Critical Infrastructure Areas

- Include:
  - Telecommunications
  - Electrical power systems
  - Water supply systems
  - Gas and oil pipelines
  - Transportation
  - Government services
  - Emergency services
  - Banking and finance
  - …

What is a "Secure" Computer System?

To decide whether a computer system is "secure", you must first decide what "secure" *means to you*, then identify the threats you care about.

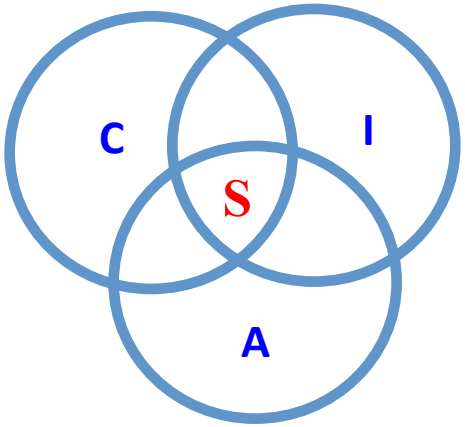
You Will Never Own a Perfectly Secure System!

You Will Never Own a Perfectly Secure System!

You Will Never Own a Perfectly Secure System!

Basic Components of Security: Confidentiality, Integrity, Availability (CIA)

- CIA
  - Confidentiality: Who is authorized to use data?
  - Integrity: Is data „good?"
  - Availability: Can access data whenever need it?



S = Secure

- CIA or CIAAAN… ☺

  (other security components added to CIA)
  - Authentication
  - Authorization
  - Non-repudiation
  - …

Need to Balance CIA

- Example 1: C vs. I+A
  - Disconnect computer from Internet to increase confidentiality
  - Availability suffers, integrity suffers due to lost updates

Need to Balance CIA(1)

- Example 2: I vs. C+A
  - Have extensive data checks by different people/systems to increase integrity
  - Confidentiality suffers as more people see data, availability suffers due to locks on data under verification)