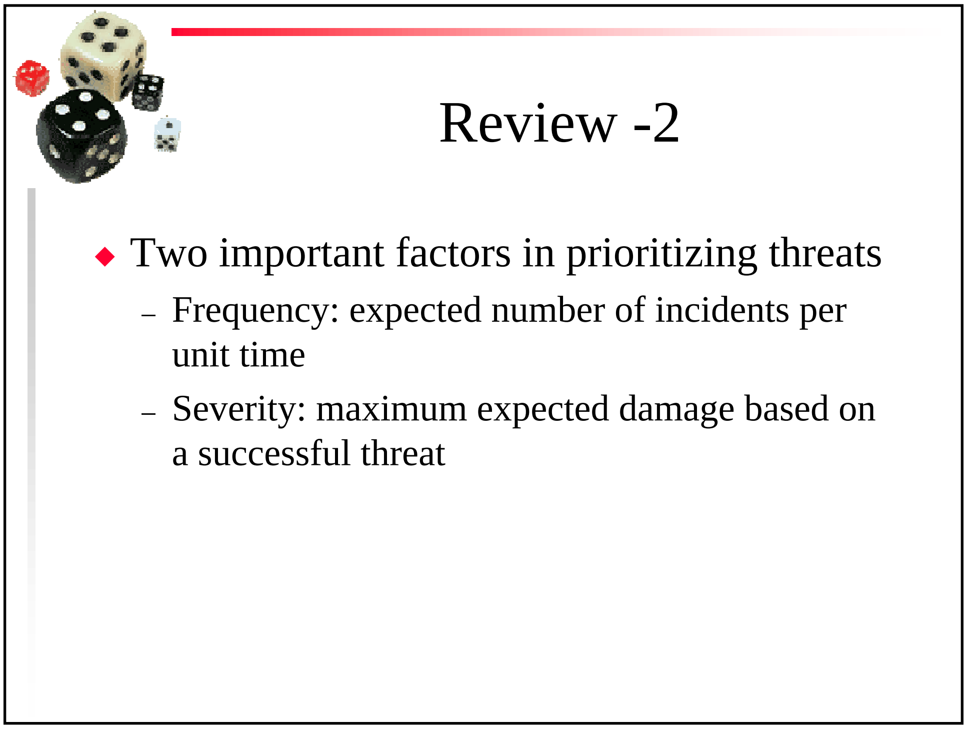
Threats and Survivability Architectures

Introduction to Security Architectures

21 Sept 2000

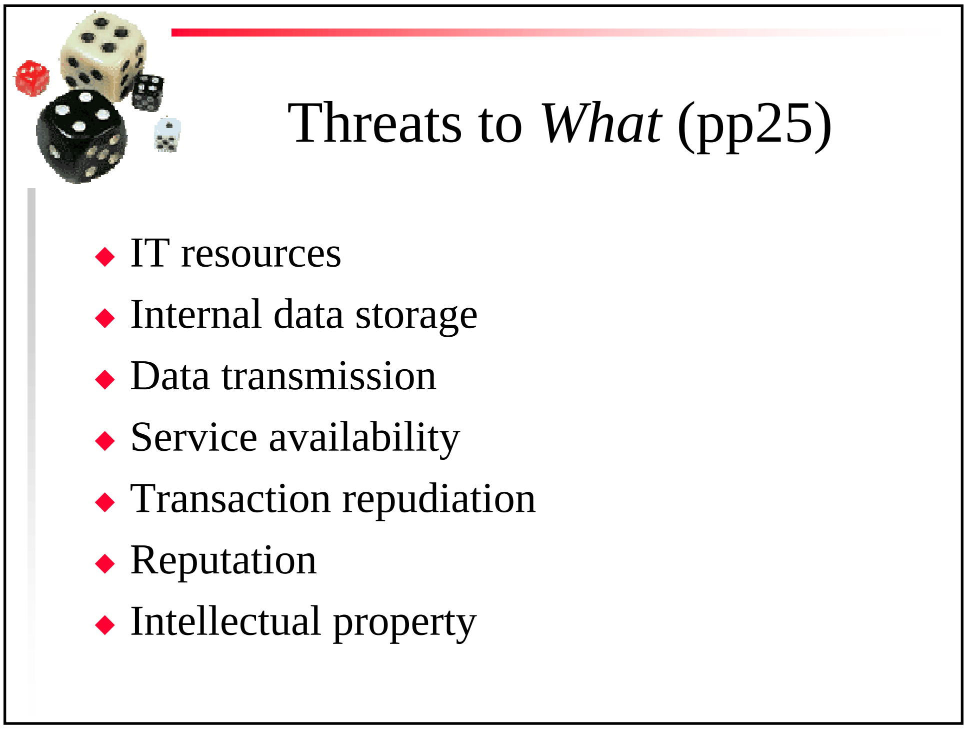
Review

- Threats to security and survivability
- Information Warfare threats
  - Nation states, terrorists, hacktivists, etc
- Other threats
  - Natural disasters, casual hackers, accidents, insiders, …



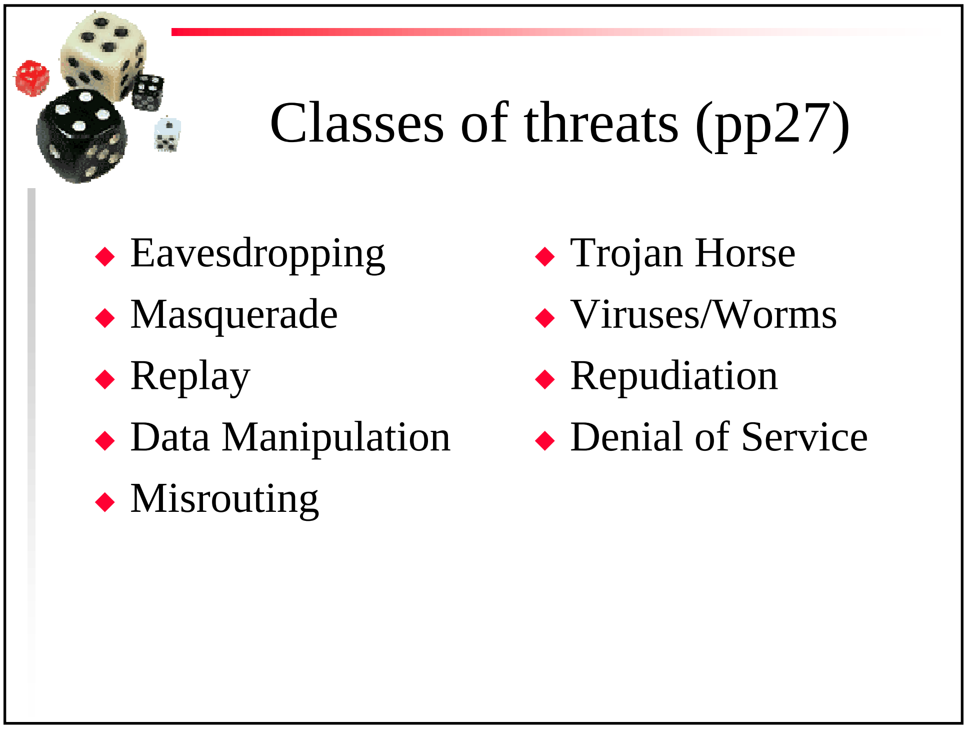
Review -2

- Two important factors in prioritizing threats
  - Frequency: expected number of incidents per unit time
  - Severity: maximum expected damage based on a successful threat



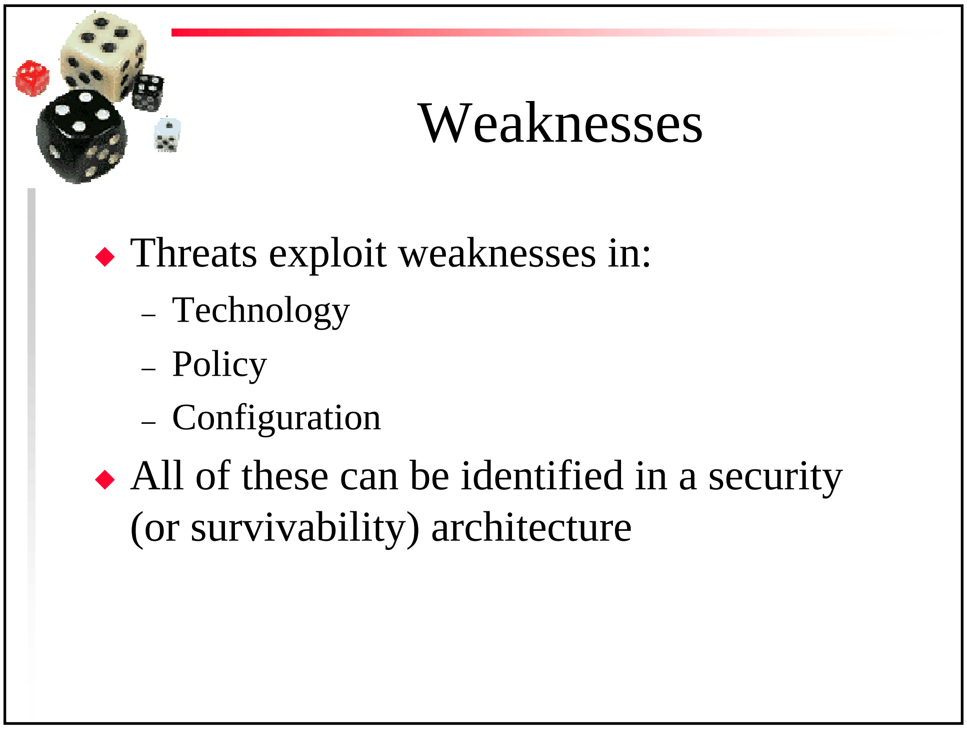
Threats to *What* (pp25)

- IT resources
- Internal data storage
- Data transmission
- Service availability
- Transaction repudiation
- Reputation
- Intellectual property



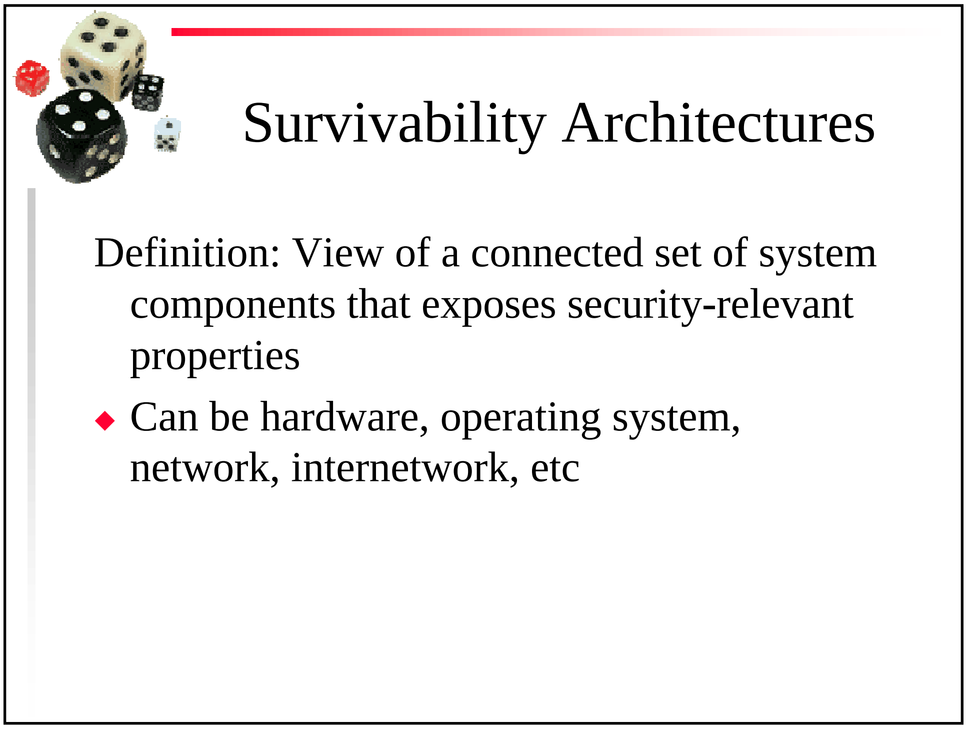
Classes of threats (pp27)

- Eavesdropping
- Masquerade
- Replay
- Data Manipulation
- Misrouting
- Trojan Horse
- Viruses/Worms
- Repudiation
- Denial of Service



Weaknesses

- Threats exploit weaknesses in:
  - Technology
  - Policy
  - Configuration
- All of these can be identified in a security (or survivability) architecture



Survivability Architectures

Definition: View of a connected set of system components that exposes security-relevant properties

- Can be hardware, operating system, network, internetwork, etc

Security features include but are not limited to:

- Integrity
- Availability
- Confidentiality

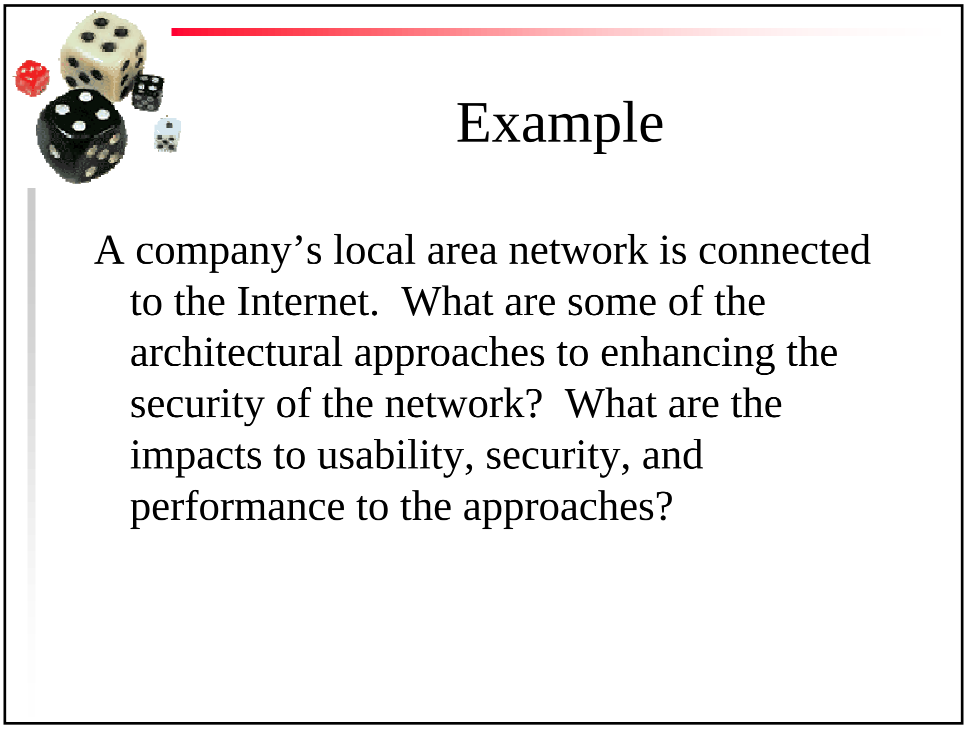
Survivability features add performance, dependability, fitness, responsiveness, etc

Flaws and Vulnerabilities

- Flaws: system component does not implement specification or maintain required system attributes
- Security flaw: a flaw that fails to impmenent the security properties of a system
- Vulnerability: a security flaw that may be exploited by a threat

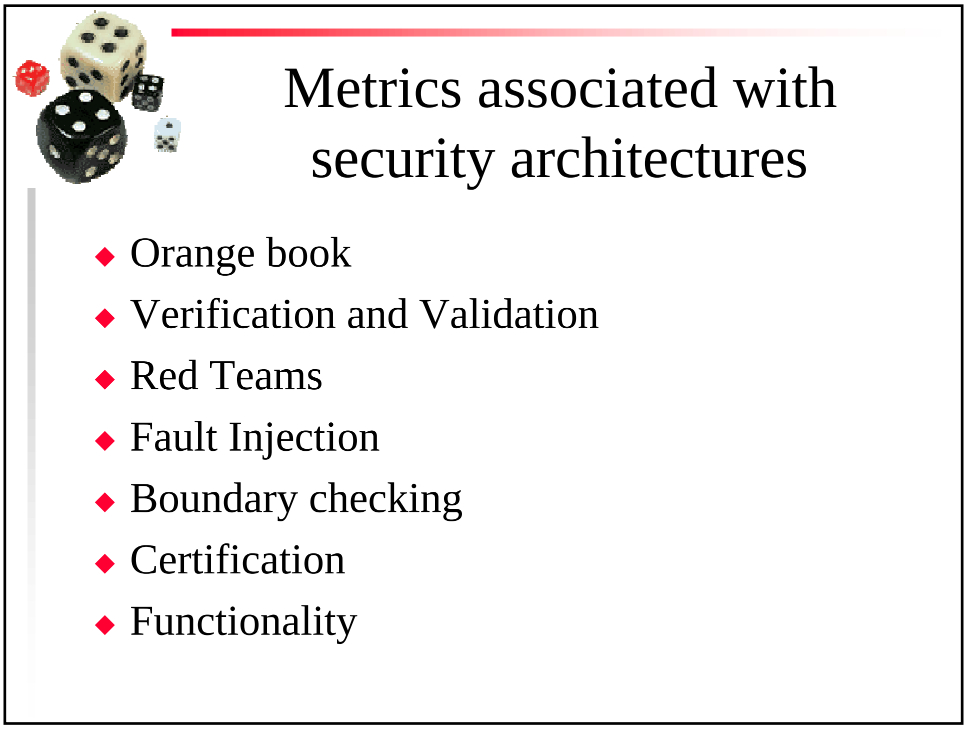
Security Architecture

- Attempts to limit the impact of vulnerabilities through the application of an architectural abstraction
- Identified elements in a security architecture should support the security attributes
- All security-relevant elements evident at the specific level of abstraction should be included



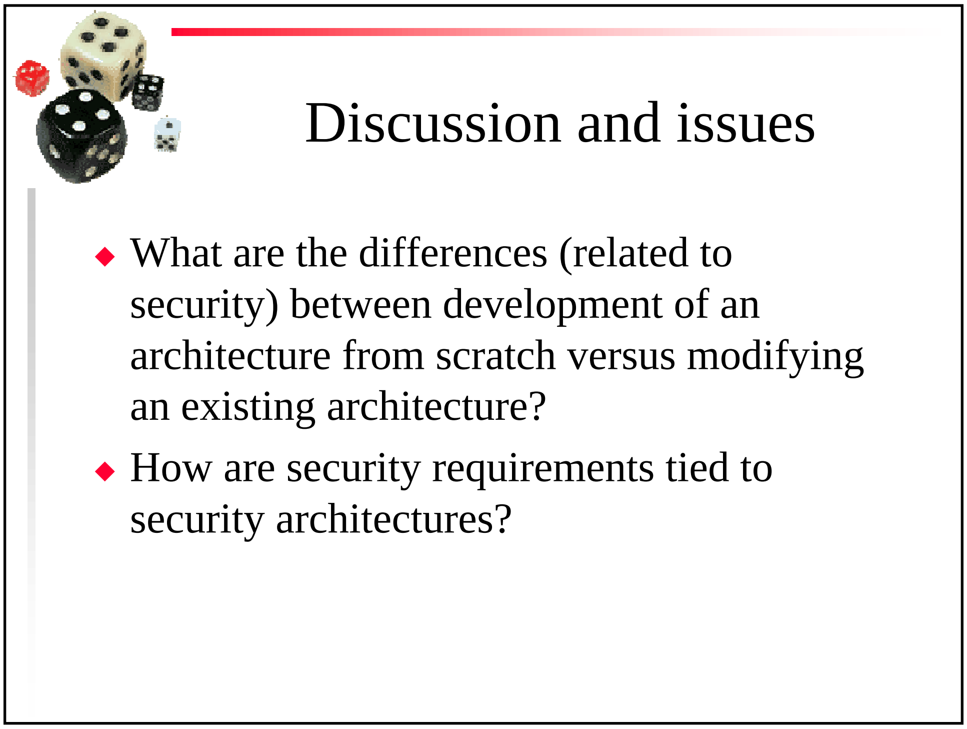
Example

A company’s local area network is connected to the Internet. What are some of the architectural approaches to enhancing the security of the network? What are the impacts to usability, security, and performance to the approaches?



Metrics associated with security architectures

- Orange book
- Verification and Validation
- Red Teams
- Fault Injection
- Boundary checking
- Certification
- Functionality



Discussion and issues

- What are the differences (related to security) between development of an architecture from scratch versus modifying an existing architecture?
- How are security requirements tied to security architectures?