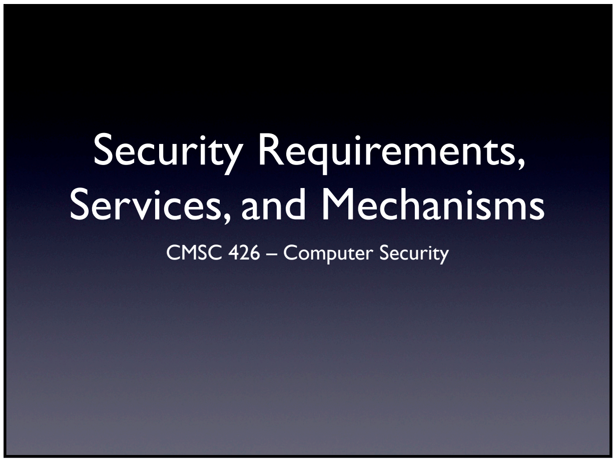
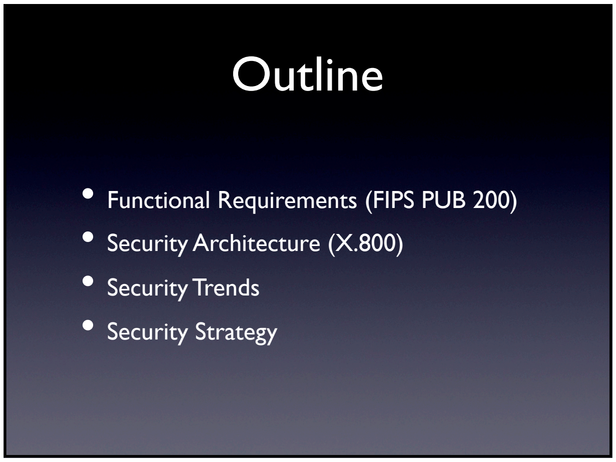


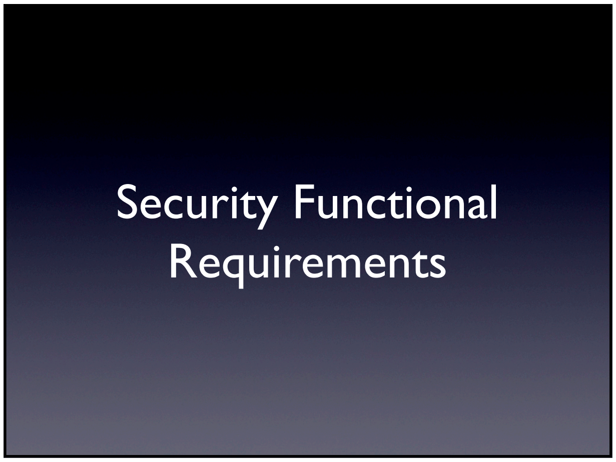
Security Requirements, Services, and Mechanisms

CMSC 426 – Computer Security

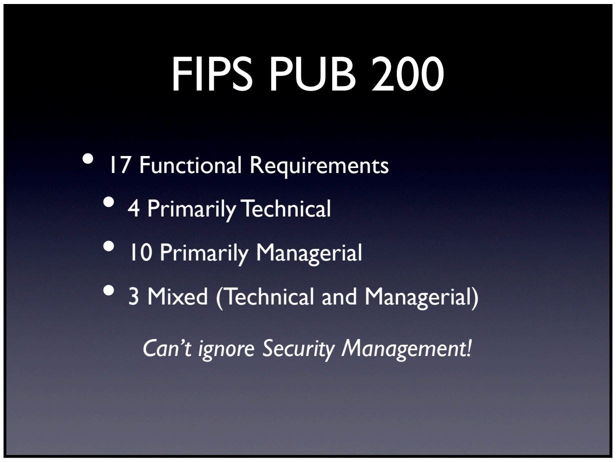


Outline

- Functional Requirements (FIPS PUB 200)
- Security Architecture (X.800)
- Security Trends
- Security Strategy



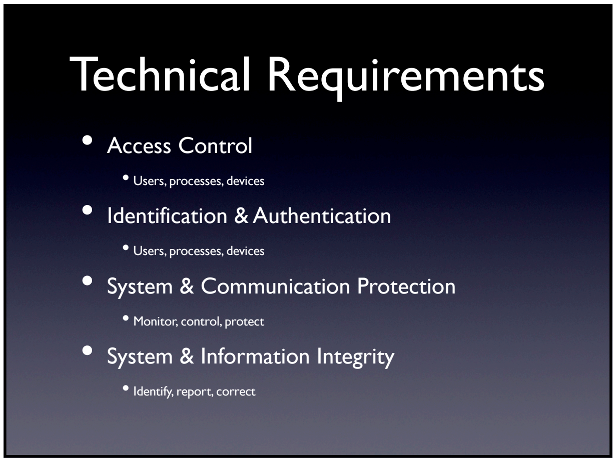
Security Functional Requirements



FIPS PUB 200

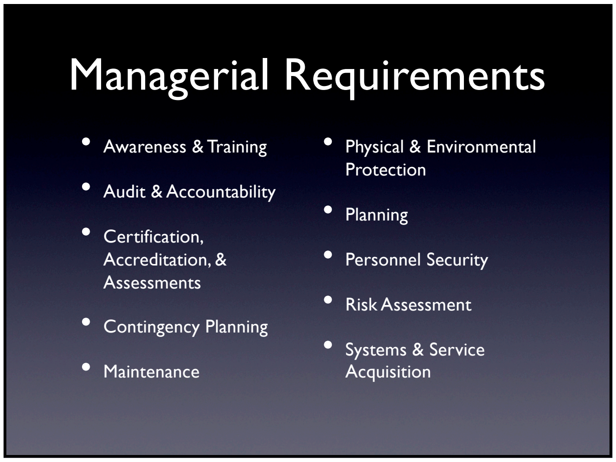
- 17 Functional Requirements
  - 4 Primarily Technical
  - 10 Primarily Managerial
  - 3 Mixed (Technical and Managerial)

Can't ignore Security Management!



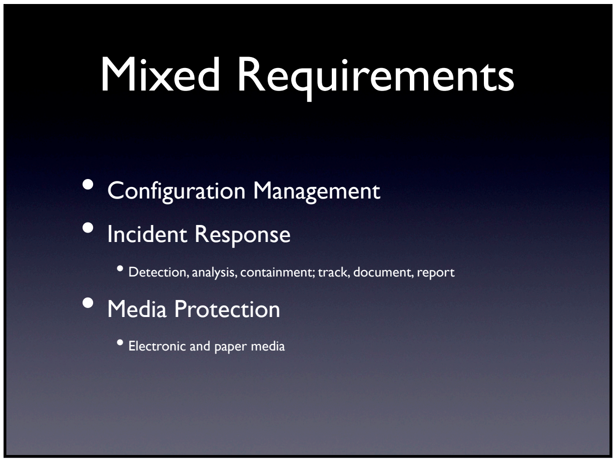
Technical Requirements

- Access Control
  - Users, processes, devices
- Identification & Authentication
  - Users, processes, devices
- System & Communication Protection
  - Monitor, control, protect
- System & Information Integrity
  - Identify, report, correct



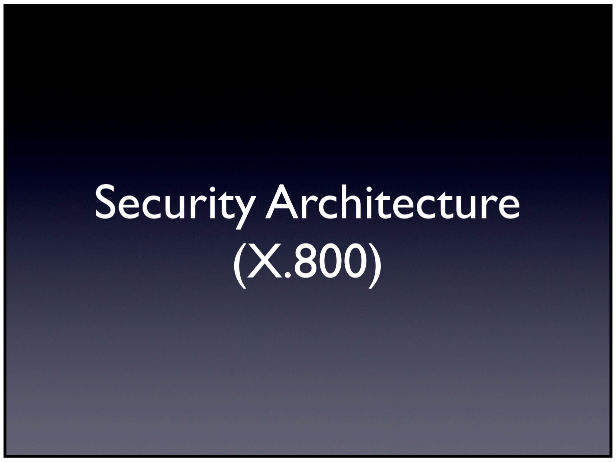
Managerial Requirements

- Awareness & Training
- Audit & Accountability
- Certification, Accreditation, & Assessments
- Contingency Planning
- Maintenance
- Physical & Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- Systems & Service Acquisition

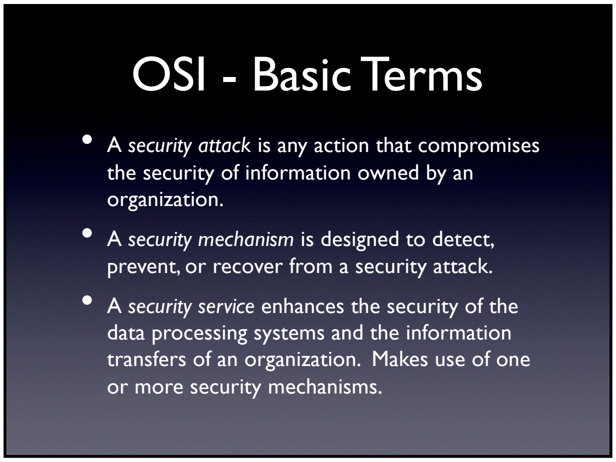


Mixed Requirements

- Configuration Management
- Incident Response
  - Detection, analysis, containment; track, document, report
- Media Protection
  - Electronic and paper media

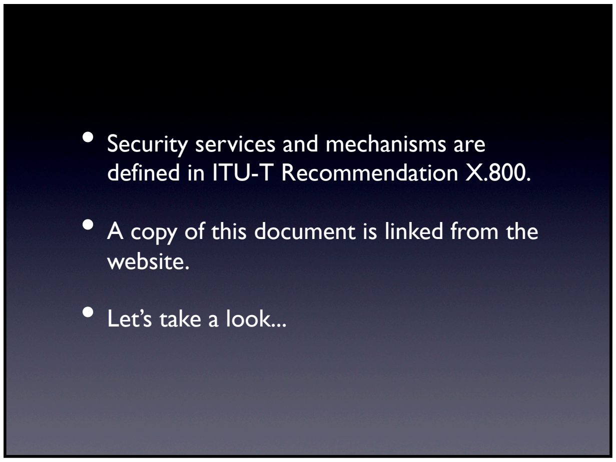


Security Architecture (X.800)



OSI - Basic Terms

- A *security attack* is any action that compromises the security of information owned by an organization.
- A *security mechanism* is designed to detect, prevent, or recover from a security attack.
- A *security service* enhances the security of the data processing systems and the information transfers of an organization. Makes use of one or more security mechanisms.



- Security services and mechanisms are defined in ITU-T Recommendation X.800.
- A copy of this document is linked from the website.
- Let’s take a look...

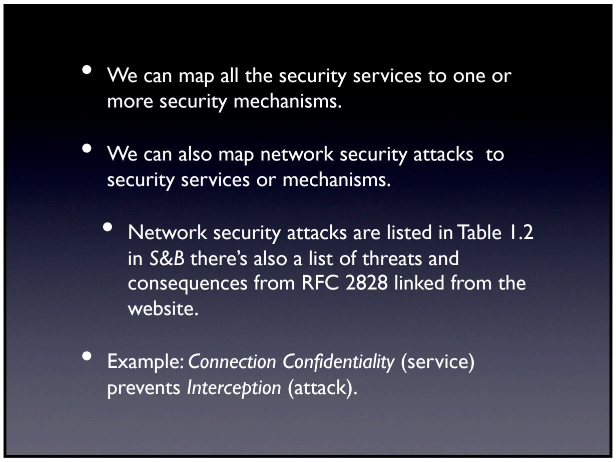
Example: Access Control

- *Access Control* is a security service. For a networked system, it will require one or more of the following mechanisms:
  - Access Control (mechanisms)
  - Authentication Exchange
  - Security Audit Trail

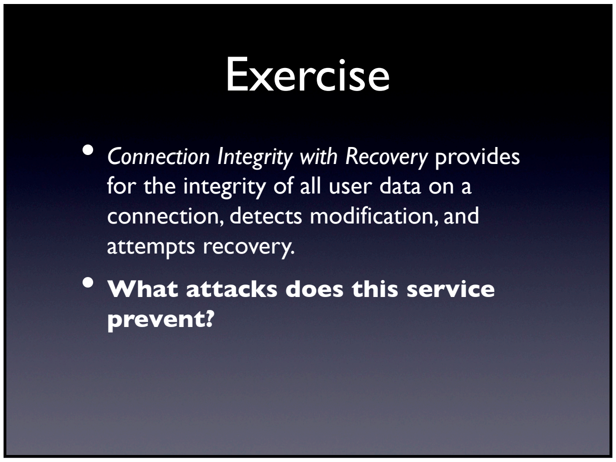
Exercise

- *Connection Confidentiality* is a service that provides confidentiality of all user data on a connection.
- **What security mechanisms may be required to provide this service?**

See the list of security mechanisms in section 5.3 of the X.800 document.



- We can map all the security services to one or more security mechanisms.
- We can also map network security attacks to security services or mechanisms.
  - Network security attacks are listed in Table 1.2 in *S&B* there's also a list of threats and consequences from RFC 2828 linked from the website.
- Example: *Connection Confidentiality* (service) prevents *Interception* (attack).



Exercise

- *Connection Integrity with Recovery* provides for the integrity of all user data on a connection, detects modification, and attempts recovery.
- **What attacks does this service prevent?**

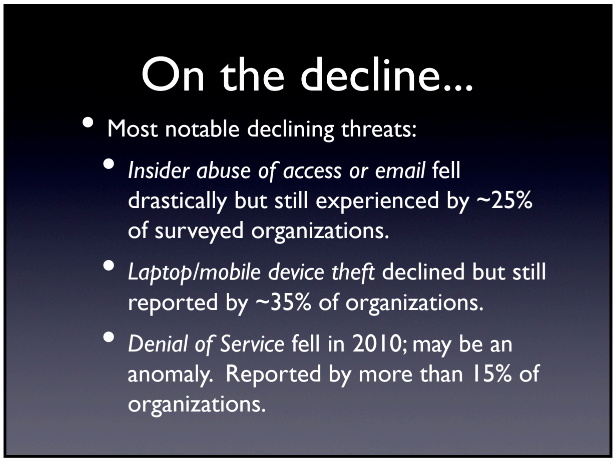
Security Trends

Threat Trends

- Trends for 2005 - 2010; from Computer Security Institute Survey 2010/2011.
- 350 companies, non-profits, and public sector organizations.

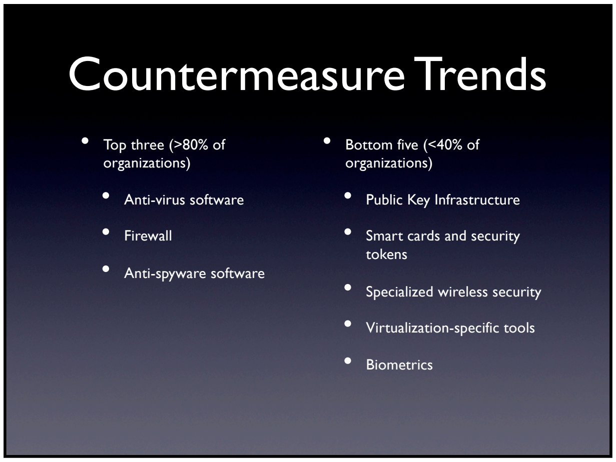
On the rise...

- Three categories of threat on the rise:
  - Malware infections experienced by more than 65% of surveyed organizations.
  - Phishing attacks experienced by nearly 40% of surveyed organizations.
  - Bots on network experienced by nearly 30% of surveyed organizations.



On the decline...

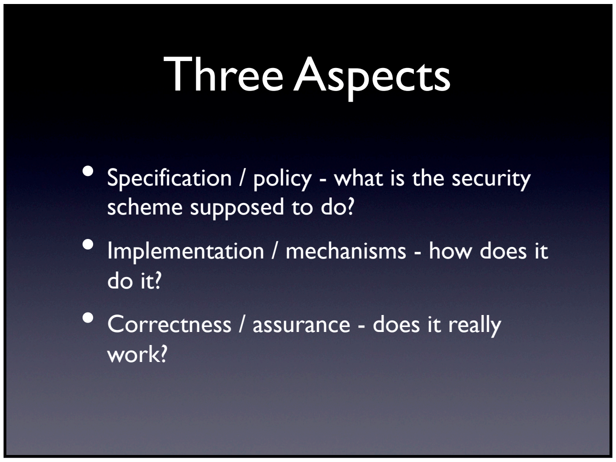
- Most notable declining threats:
  - *Insider abuse of access or email* fell drastically but still experienced by ~25% of surveyed organizations.
  - *Laptop/mobile device theft* declined but still reported by ~35% of organizations.
  - *Denial of Service* fell in 2010; may be an anomaly. Reported by more than 15% of organizations.



Countermeasure Trends

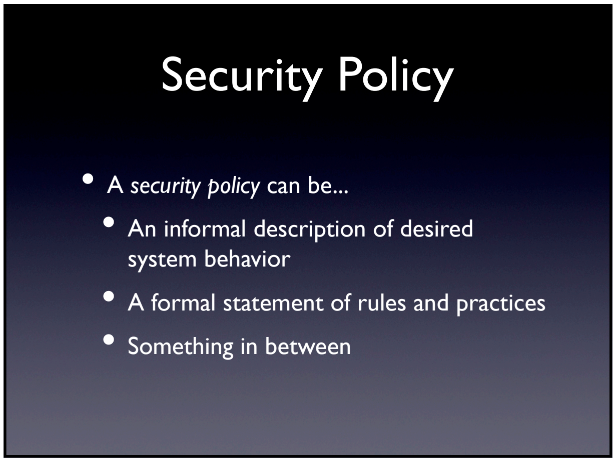
- Top three (>80% of organizations)
  - Anti-virus software
  - Firewall
  - Anti-spyware software
- Bottom five (<40% of organizations)
  - Public Key Infrastructure
  - Smart cards and security tokens
  - Specialized wireless security
  - Virtualization-specific tools
  - Biometrics

Security Strategy



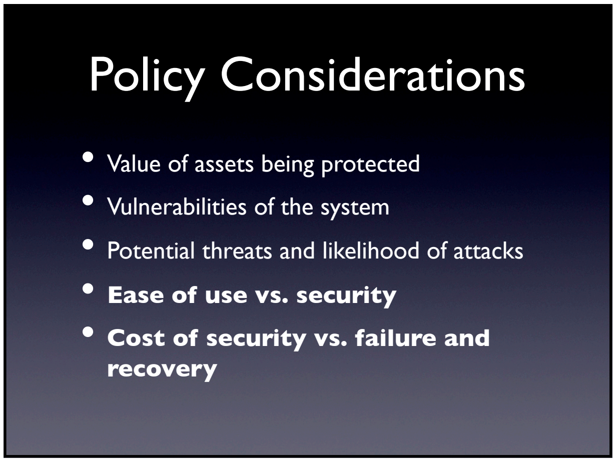
Three Aspects

- Specification / policy - what is the security scheme supposed to do?
- Implementation / mechanisms - how does it do it?
- Correctness / assurance - does it really work?



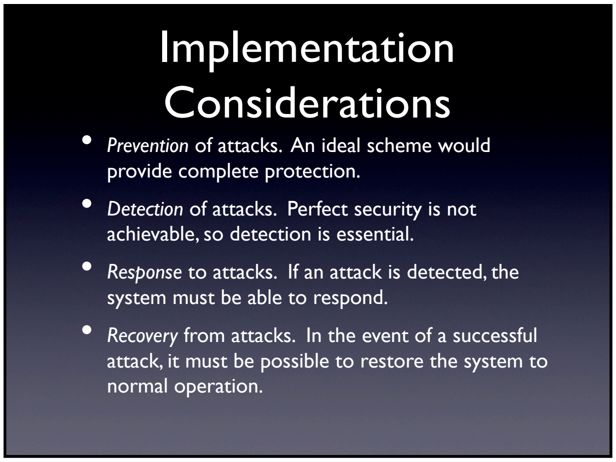
Security Policy

- A *security policy* can be…
  - An informal description of desired system behavior
  - A formal statement of rules and practices
  - Something in between



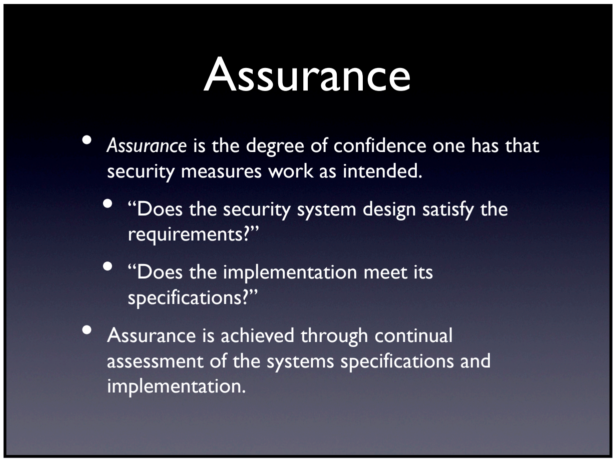
Policy Considerations

- Value of assets being protected
- Vulnerabilities of the system
- Potential threats and likelihood of attacks
- **Ease of use vs. security**
- **Cost of security vs. failure and recovery**



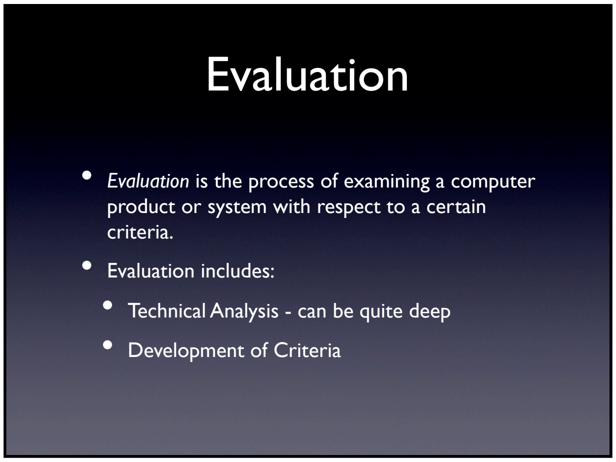
Implementation Considerations

- *Prevention* of attacks. An ideal scheme would provide complete protection.
- *Detection* of attacks. Perfect security is not achievable, so detection is essential.
- *Response* to attacks. If an attack is detected, the system must be able to respond.
- *Recovery* from attacks. In the event of a successful attack, it must be possible to restore the system to normal operation.



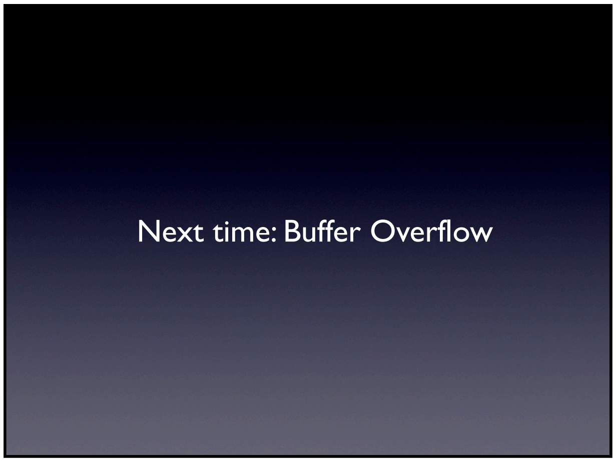
Assurance

- *Assurance* is the degree of confidence one has that security measures work as intended.
  - “Does the security system design satisfy the requirements?”
  - “Does the implementation meet its specifications?”
- Assurance is achieved through continual assessment of the systems specifications and implementation.



Evaluation

- *Evaluation* is the process of examining a computer product or system with respect to a certain criteria.
- Evaluation includes:
  - Technical Analysis - can be quite deep
  - Development of Criteria



Next time: Buffer Overflow