Security

18-849b Dependable Embedded Systems

Kanaka Juvva

2/25/99

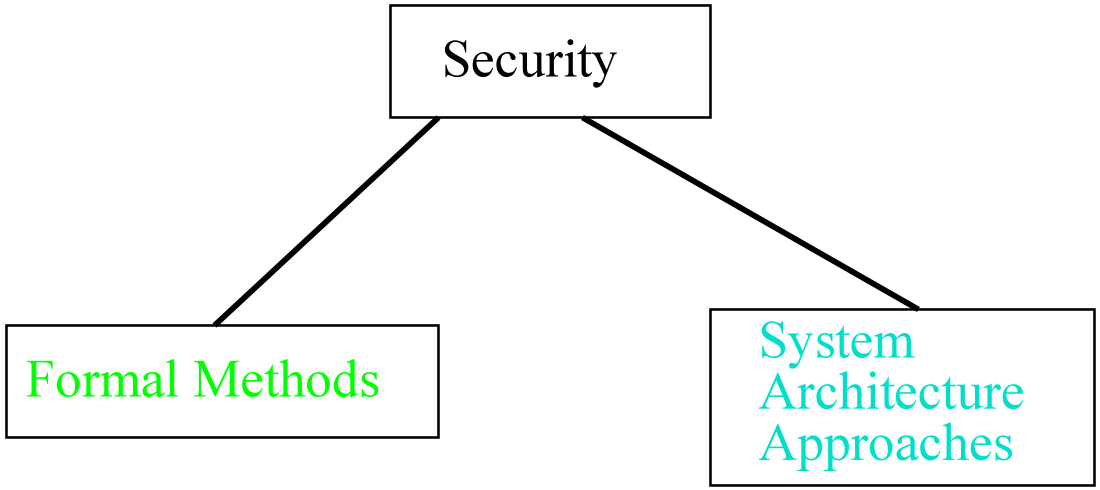
Required Reading:	**Security of the Internet, Marcel Dekker, In the Froehlich/Kent Encyclopedia of Telecommunications, vol. 15, pp. 231-255.**
Tutorial:	**Chapter 1 , Computer System and Network Security, Gregory B. White, Eric A. Fisch, Udo W. Pooch**
Authoritative Books:	**Computer System and Network Security, Gregory B. White, Eric A. Fisch, Udo W. Pooch**

Carnegie Mellon

Overview: Security

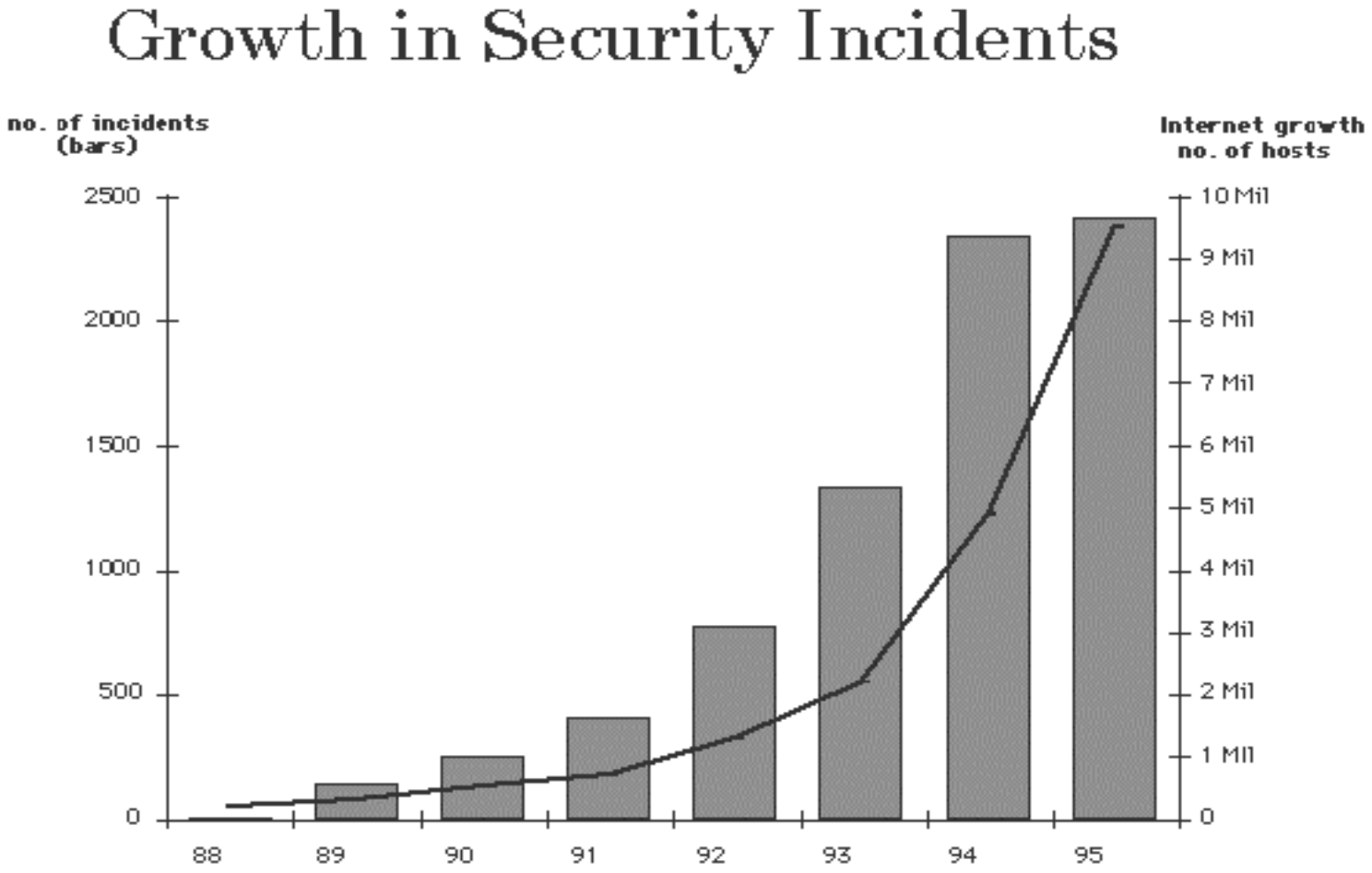
- **Introduction**
  - Why Computer Security ?
- **Key concepts**
  - Security Issues
  - Security Models
  - Cryptography
- **Metrics**
  - Unconditional Security
  - Computational Security
- **Relationship to other topics**
  - Formal Methods
  - System Architecture Approaches
- **Conclusions & future work**

YOU ARE HERE



Why Security ?

– "Undetected Theft of a Credit-Card Data Raises Concern About On-Line Security" The Wall Street Journal, Friday, February 17, 1995.



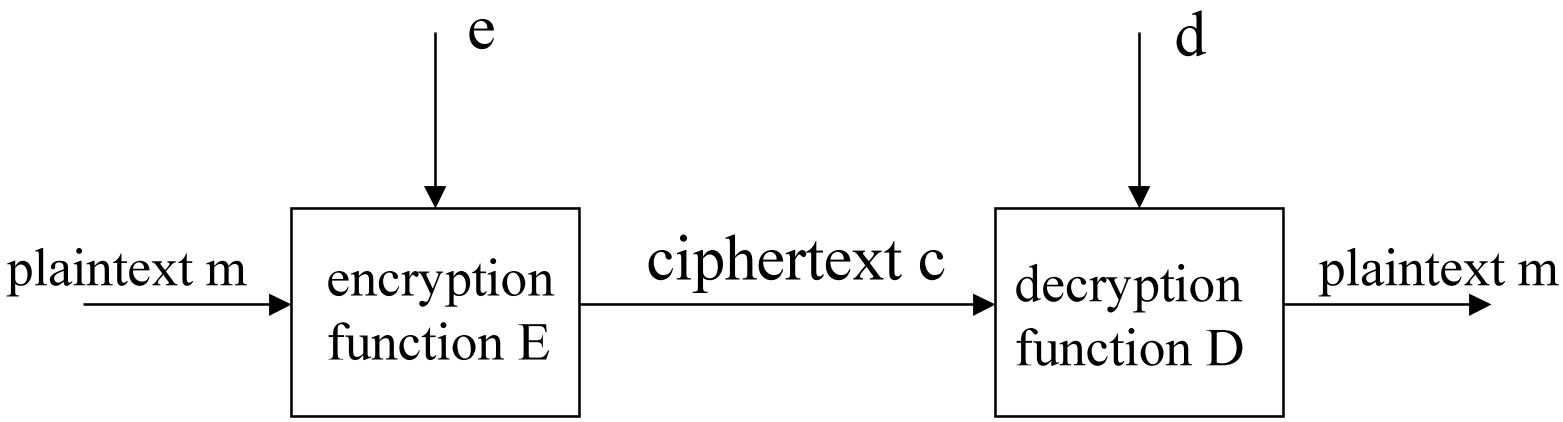
Issues Involved in Security

- **Security Policies**
  - Used to be just physical protection - Not any longer
  - Confidentiality
  - Integrity
  - Availability
- **Secure Operating Systems**
- **Other Issues**
  - Security is often not included in the originally designed or implemented system but is added later in the project
  - Security costs and often "gets in the way"
  - Very often the problem lies with the people who use the system and not in the technology
- **Risk Analysis**

Security Models

- **Precisely expresses the system's security requirements**
- **Bell and LaPadula (for military)**
  - Finite State Machine model
  - Secure Transitions lead to secure states
  - Users are constrained by the data they can acess
- **Clark-Wilson (Commercial)**
  - Integrity policies are more important than disclosure policies
  - Well-formed transactions eg Auditing
  - Users are constrained by the programs they can execute
- **TCSEC (DoD Orange book)**
  - Provides requirements and specific criteria to develop a system
  - Discretionary access controls and Mandatory access controls

Cryptography



- **Data Encryption Standard (DES)**
  - Scrambling of data
- **International Data Encryption Algorithm (IDEA)**
  - Larger keys and complex breaking scheme
- **Public Key Cryptography**
  - Correspondents never have to exchange secret keys

Tools / Techniques

- **Monitoring Tools**
  - Network Monitors
- **Security Analysis Tools**
  - Vulnerability Identification Tools
- **Cryptography**
- **Intrusion Detection**

Metrics

- **Unconditional security**
  - Adversaries have unlimited computational power.
- **Computational security**
  - Adversaries have limited computational power. Breaking system requires at least N operations where N is some specified, very large number.. Complexity-theoretic security
    - Adversaries are modeled as having polynomial computational power.
      - » » Asymptotic and worse-case analysis used => results may be impractical. E.g., polynomial attacks in model may be computationally infeasible in practice.
- **Provable security**
  - The difficulty of defeating cryptosystem can be shown to be essentially as difficult as solving a well-known and supposedly difficult (typically number-theoretic problem.
- **Practical security**
  - Perceived level of computation to defeat it using best known attacks exceeds ``by a comfortable margin'' the assumed computational resources of adversary.

Connections

- **System Architecture Approaches**
  - Software Engineering
- **Formal Methods**
- **OS**
- **Languages**

Conclusions & Future Work

- Security issues
- Security Models
- Cryptography
- Security Monitoring Tools
- OS and Language Support
- Intrusion Detection

Internet Security:

- Overview of Internet Security
- Types of Incidents
- Types of vulnerabilities
- Improving Security