IS 2150 / TEL 2810
Introduction to Security

James Joshi

Assistant Professor, SIS

Lecture 1

August 30, 2007

Contact

- Instructor: James B. D. Joshi
  - 706A, IS Building
  - Phone: 412-624-9982
  - E-mail: jjoshi@mail.sis.pitt.edu
  - Web: http://www.sis.pitt.edu/~jjoshi/
  - Office Hours:
    - Tuesdays: 2.00 – 4.00 p.m.
    - By appointments
- GSA: TBD
- Lab help: Carlos E Caicedo Bastida

Course Goals

- to develop a broader understanding of the information security field,
  - *Recognize*, *analyze* and evaluate security problems and challenges in networks and systems.
  - *Apply* their knowledge to synthesize possible approaches to *solve* the problems in an integrated way.

Recognize the various security issues/terminologies related to software, networks and applications to *show* how they are interrelated and available techniques and approaches to solve/tackle security problems.

Analyze and *evaluate* the fundamentals of security policy models and mechanisms, and their need for different types of information systems and applications

Apply the basics of Cryptographic techniques and network security for ensuring the basic security goals of security of information systems.

Describe/identify the various basic social, legal and non-technical dimensions of security and its relation to technical counterparts.

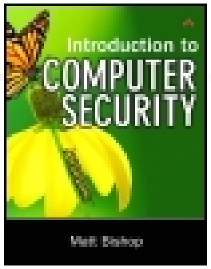
Certified for IA Standards

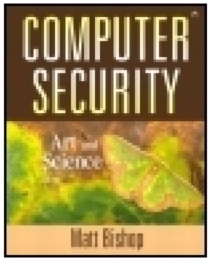
- SAIS Track is certified for 5 CNSS standards
  - This course accounts for about 85% of the first three CNSS standards
  - Hence CORE course for SAIS track
- Course webpage: http://www.sis.pitt.edu/~jjoshi/IS2150/Fall07/

Course Outline

- Security Basics
  - General overview and definitions
  - Security models and policy issues
- Basic Cryptography and Network security
  - Crypto systems, digital signature, authentication, PKI
  - IPSec, VPN, Firewalls
- Systems Design Issues and Information assurance
  - Design principles
  - Security Mechanisms
  - Auditing Systems
  - Risk analysis
  - System verification
- Intrusion Detection and Response
  - Attack Classification and Vulnerability Analysis
  - Detection, Containment and Response/Recovery
- Legal, Ethical, Social Issues
- Evaluation, Certification Standards
- Miscellaneous Issues
  - Malicious code, Mobile code
  - Digital Rights Management, Forensics
  - Watermarking,
  - E/M-commerce security, Multidomain Security
  - Identity/Trust Management

Course Material





- Textbook
  - Introduction to Computer Security, Matt Bishop,
    - Errata URL: http://nob.cs.ucdavis.edu/~bishop/
  - Computer Security: Art and Science, Matt Bishop – is fine too
- Other Recommended
  - Security in Computing, Charles P. Pfleeger, Prentice Hall
  - Inside Java 2 Platform Security, 2nd Edition, L. Gong, G. Ellision, M. Dageforde
  - Security Engineering: A Guide to Building Dependable Distributed Systems, Ross Anderson, Wiley, John & Sons, Incorporated, 2001
- Additional readings will be provided
  - Required or Optional

Prerequisites

- Assumes the following background
  - Programming skill
    - Some assignments in Java
  - Working knowledge of
    - Operating systems, algorithms and data structures, database systems, and networks
  - Basic Mathematics
    - Set, logic, induction techniques, data structure/algorithms
- Not sure?   SEE ME

Grading

- Lab + Homework/Quiz/Paper review 50%
- Exams 30% includes
  - Midterm: 15%
  - Final: 15%
- Paper/Project 20%
  - List of suggested topics will be posted;
  - Encouraged to think of a project/topic of your interest
- Some other
  - Seminar (LERSAIS) and participation
    - Borderline cases will be helped

Course Policies

- Your work MUST be your own
  - Zero tolerance for cheating/plagiarism
  - You get an F for the course if you cheat in anything however small – NO DISCUSSION
  - Discussing the problem is encouraged
- Homework
  - Penalty for late assignments (15% each day)
    - Occasionally you can seek extension under pressing circumstances
  - Ensure clarity in your answers – no credit will be given for vague answers
  - Sample solutions will be provided
- Check webpage for everything!
  - You are responsible for checking the webpage for updates

LERSAIS

LABORATORY OF EDUCATION AND RESEARCH ON

Security Assured Information Systems

LERSAIS

UNIVERSITY OF PITTSBURGH

SCHOOL OF INFORMATION SCIENCE

LERSAIS

- Laboratory of Education and Research in Security Assured Information Systems
  - Established in 2003
  - National Center of Academic Excellence in Information Assurance Education Program
    - A US National Security Agency program initiated in 1998 through a presidential directive to SECURE the Cyberspace
    - Partnered by Department of Homeland Security since 2003
    - There are 80+ such centers now
  - LERSAIS is Pitt’s representative center
- Website: http://www.sis.pitt.edu/~lersais/
  - Check out for Friday Seminars:
    - 2:00PM Welcome Coffee/Cake
    - 2:30-3:30PM Talk

A Word on SAIS Track

- Pitt’s IA curriculum has been certified for
  - Committee on National Security Systems IA Standards
    - CNSS 4011: Information Security Professionals
    - CNSS 4012: Designated Approving Authority
    - CNSS 4013: System Administrator in Information Systems Security
    - CNSS 4014: Information Systems Security Officer
    - CNSS 4015: System Certifiers
- Pitt is one among 13 Institutions in the US and only one in the State of Pennsylvania to have all certifications
- Website: http://www.sis.pitt.edu/~sais/

What is Information Security?

Overview of Computer Security

Information Systems Security

- Deals with
  - Security of (end) systems
    - Examples: Operating system, files in a host, records, databases, accounting information, logs, etc.
  - Security of information in transit over a network
    - Examples: e-commerce transactions, online banking, confidential e-mails, file transfers, record transfers, authorization messages, etc.

"Using encryption on the internet is the equivalent of arranging an armored car to deliver credit card information from someone living in a cardboard box to someone living on a park bench" –

Gene Spafford

Basic Components of Security

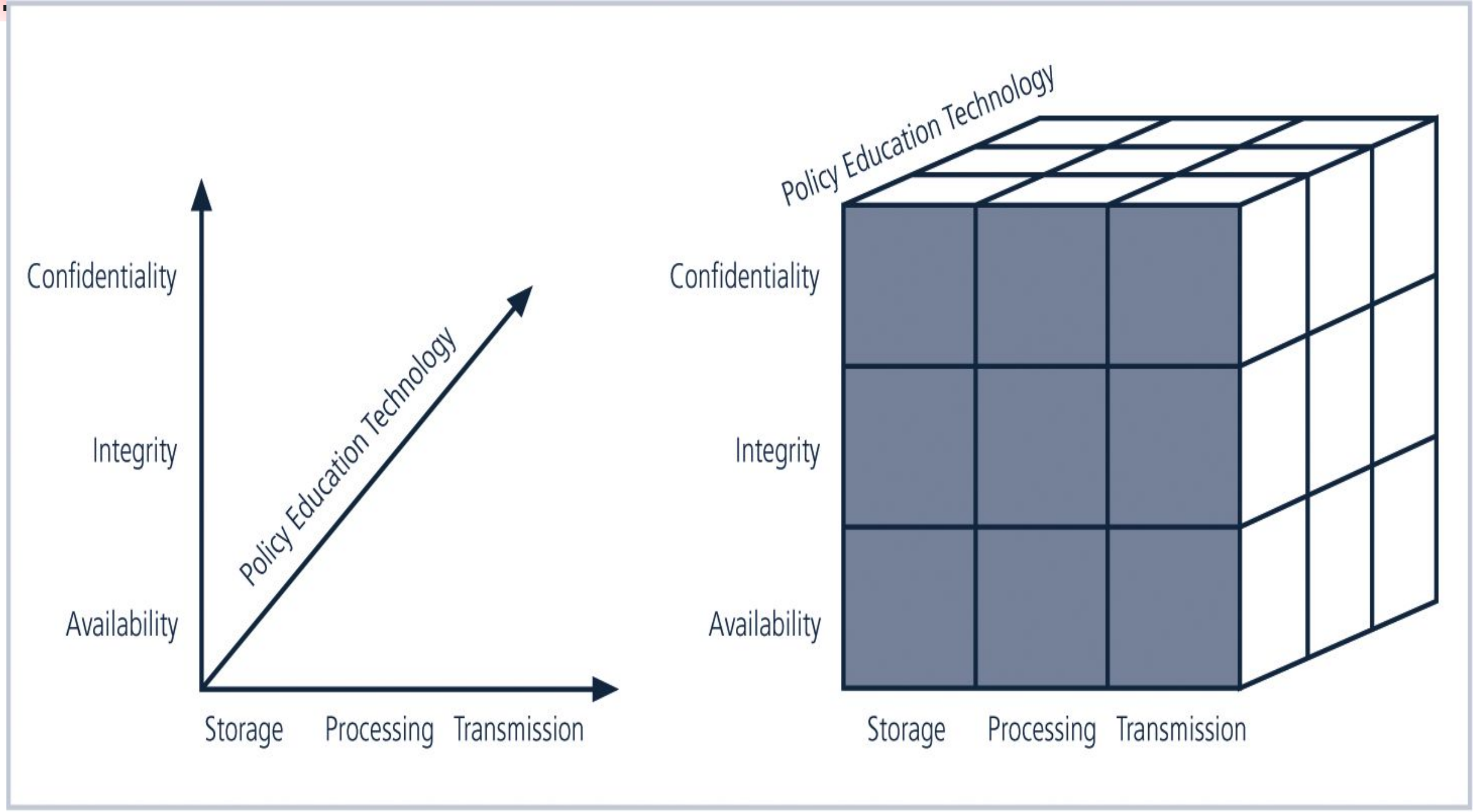
CIA

- Confidentiality
  - Keeping data and resources secret or hidden
  - Conceal existence of data
- Integrity
  - Refers to correctness and trustworthiness
  - Ensuring authorized modifications;
  - May refer to
    - Data integrity
    - Origin integrity (Authentication)
- Availability
  - Ensuring authorized access to data and resources when *desired*
    - *Often assume a statistical model for pattern of use – which can be distorted*

- Prevention
- Detection

Trust Management
(Emerging Challenge)

CIA-based Model

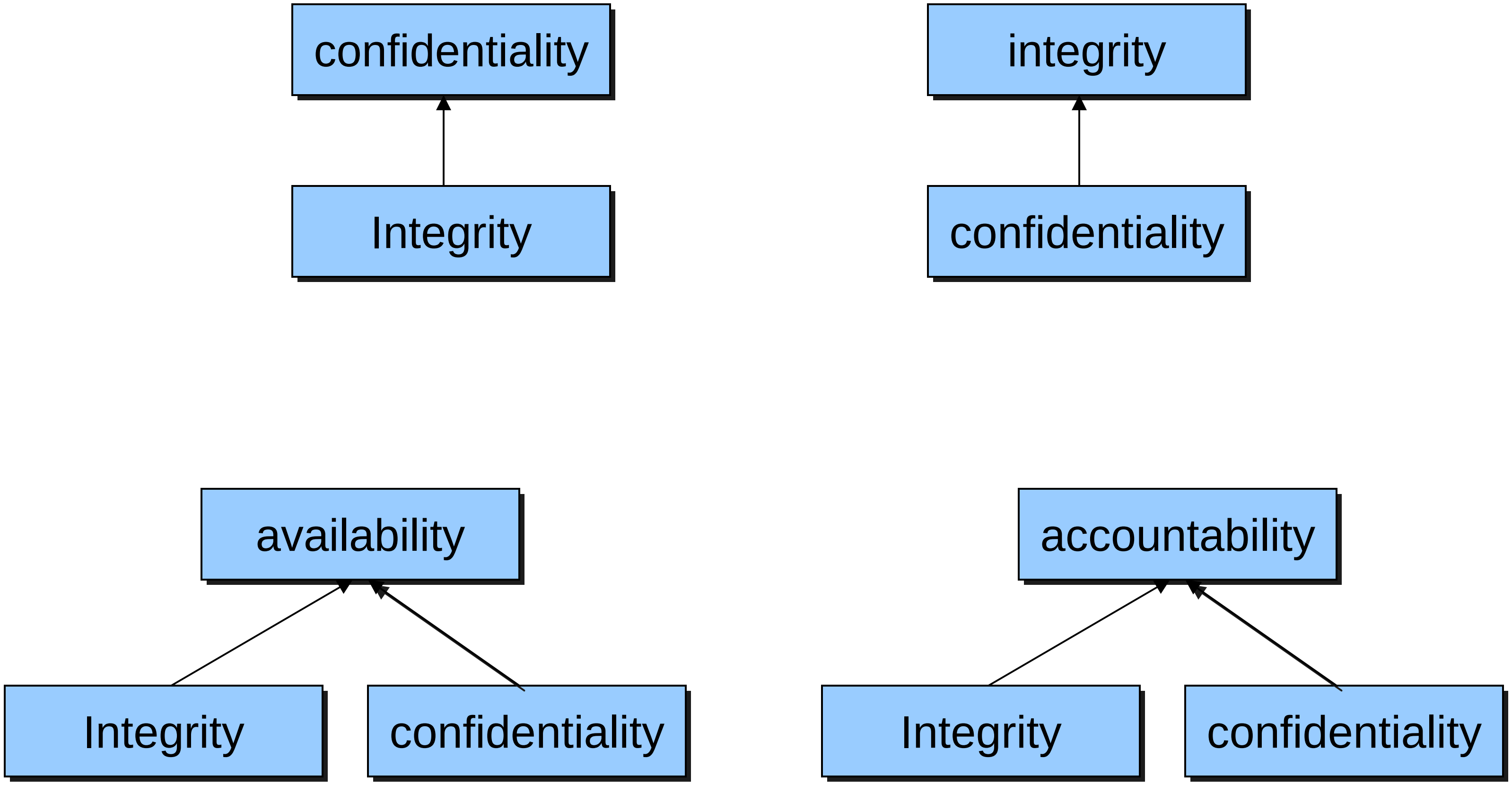


NSTISSC 4011 Security Model (CNSS 4011)

Basic Components of Security

- Additional from NIST (National Institute of Standards and Technology
    - Accountability
        - Ensuring that an entity’s action is traceable uniquely to that entity
    - [Security] assurance
        - Assurance that all four objectives are met
- Other
    - Non-repudiation:
        - false denial of an act

Interdependencies



confidentiality

Integrity

integrity

confidentiality

availability

Integrity

confidentiality

accountability

Integrity

confidentiality

Security - Years back

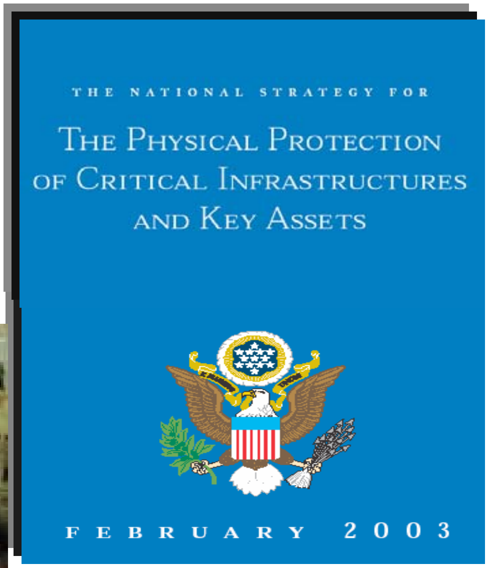
- Physical security
  - Information was primarily on paper
  - Lock and key
  - Safe transmission
- Administrative security
  - Control access to materials
  - Personnel screening
  - Auditing

Information security today

- Emergence of the Internet and distributed systems
  - Increasing system complexity
  - Open environment with previously unknown entities interacting
- Digital information needs to be kept secure
  - Competitive advantage
  - Protection of assets
  - Liability and responsibility

Information security today

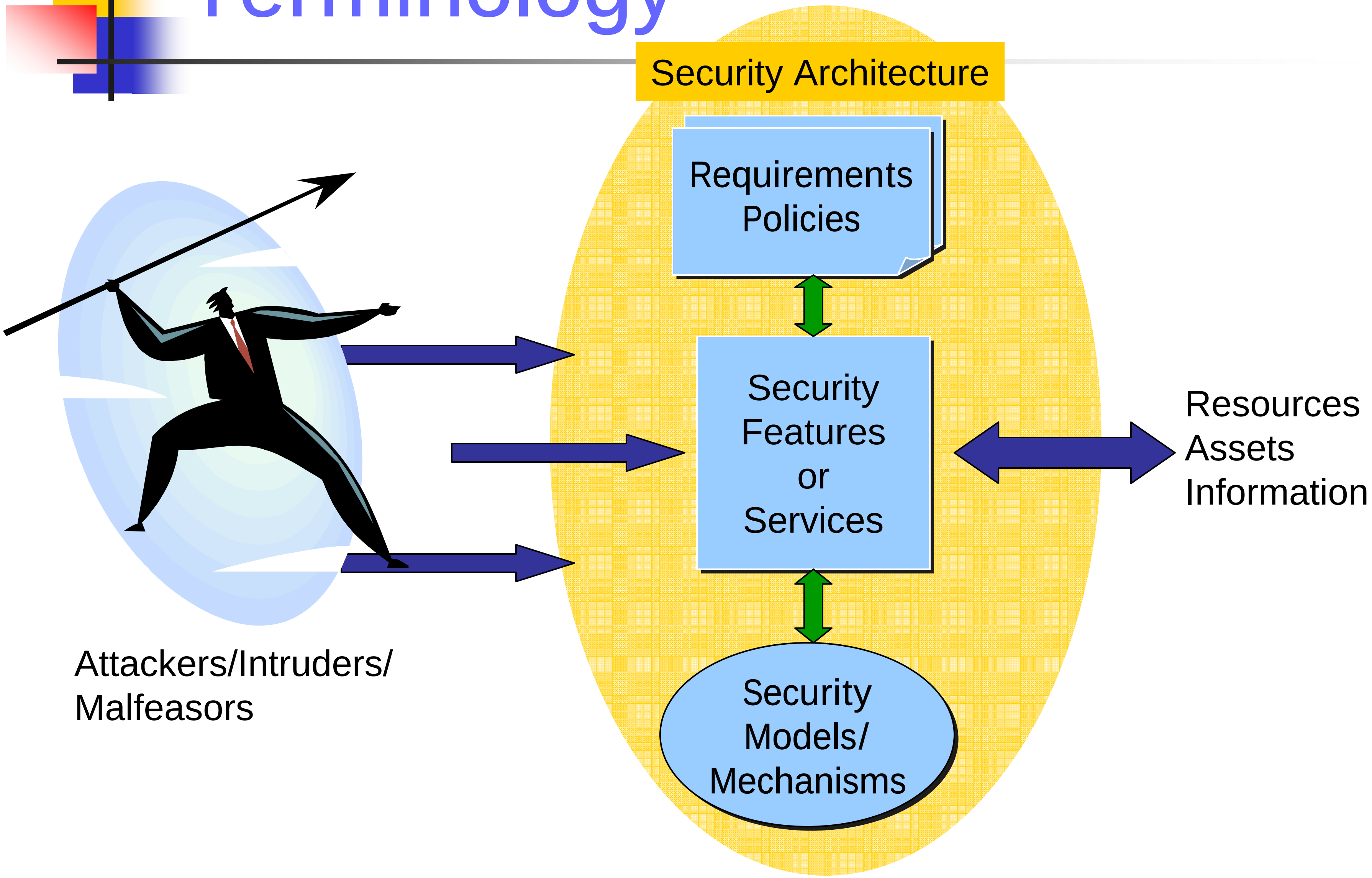
- Financial losses
  - The FBI estimates that an insider attack results in an average loss of $2.8 million
  - Reports indicate annual financial loss due to information security breaches of $5 - 45 billion
- National defense
  - Protection of critical infrastructures:
    - Power Grid; Air transportation; SCADA
  - Interlinked government agencies
    - Bad Grade for many agencies (GAO Reports)
    - DHS gets a failing grade (2005) !!


THE NATIONAL STRATEGY FOR

THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURES AND KEY ASSETS

FEBRUARY 2003

Terminology



Security Architecture

Requirements
Policies

Security
Features
or
Services

Security
Models/
Mechanisms

Resources
Assets
Information

Attackers/Intruders/
Malfeasors

Attack Vs Threat

- A threat is a “potential” violation of security
  - The violation need not actually occur
  - The fact that the violation *might* occur makes it a threat
  - It is important to guard against threats and be prepared for the actual violation
- The actual violation of security is called an attack

Common security threats/attacks

- Interruption, delay, denial of receipt or denial of service
  - System assets or information become unavailable or are rendered unavailable
- Interception or snooping
  - Unauthorized party gains access to information by browsing through files or reading communications
- Modification or alteration
  - Unauthorized party changes information in transit or information stored for subsequent access
- Fabrication, masquerade, or spoofing
  - Spurious information is inserted into the system or network by making it appear as if it is from a legitimate entity
- Repudiation of origin
  - False denial that an entity did (send/create) something

Classes of Threats (Shirley)

- Disclosure: *unauthorized access to information*
  - Snooping
- Deception: *acceptance of false data*
  - Modification, masquerading/spoofing, repudiation of origin, denial of receipt
- Disruption: *interruption/prevention of correct operation*
  - Modification
- Usurpation: *unauthorized control of a system component*
  - Modification, masquerading/spoofing, delay, denial of service

Policies and Mechanisms

- A security policy states what is, and is not, allowed
  - This defines “security” for the site/system/*etc*.
  - Policy definition: Informal? Formal?
- Mechanisms enforce policies
- Composition of policies
  - If policies conflict, discrepancies may create security vulnerabilities

Goals of Security

- Prevention
  - To prevent someone from violating a security policy
- Detection
  - To detect activities in violation of a security policy
  - Verify the efficacy of the prevention mechanism
- (Response &) Recovery
  - Stop policy violations (attacks)
  - Assess and repair damage
  - Ensure availability in presence of an ongoing attack
  - Fix vulnerabilities for preventing future attack
  - Retaliation against the attacker

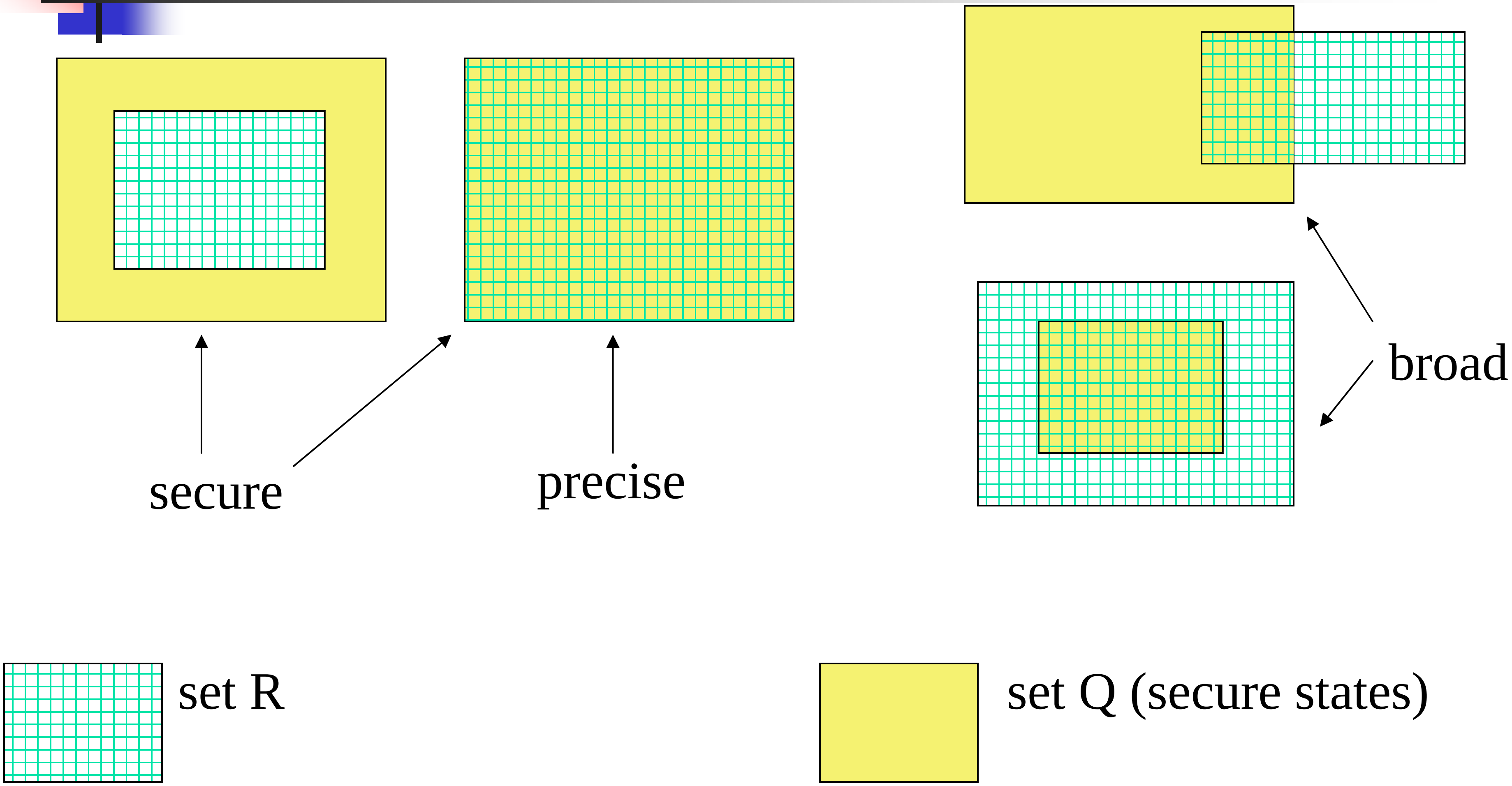
Assumptions and Trust

- Policies and mechanisms have implicit assumptions
- Assumptions regarding policies
  - Unambiguously partition system states into “secure” and “nonsecure” states
  - Correctly capture security requirements
- Mechanisms
  - Assumed to enforce policy; i.e., ensure that the system does not enter “nonsecure” state
  - Support mechanisms work correctly

Types of Mechanisms

- Let P be the set of all the reachable states
- Let Q be a set of secure states identified by a policy: $Q \subseteq P$
- Let the set of states that an enforcement mechanism restricts a system to be R
- The enforcement mechanism is
  - Secure if $R \subseteq Q$
  - Precise if $R = Q$
  - Broad if there are some states in R that are not in Q

Types of Mechanisms



secure

precise

broad

set R

set Q (secure states)

Information Assurance

- *Information Assurance Advisory Council (IAAC)*:

  "Operations undertaken to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation"

- National Institute of Standards Technology

  "Assurance is the basis for confidence that the security measures, both technical and operational, work as intended to protect the system and the information it processes"

Assurance

- Assurance is to indicate “how much” to trust a system and is achieved by ensuring that
  - The required functionality is present and correctly implemented
  - There is sufficient protection against unintentional errors
  - There is sufficient resistance to intentional penetration or by-pass
- Basis for determining this aspect of trust
  - Specification
    - Requirements analysis
    - Statement of desired functionality
  - Design
    - Translate specification into components that satisfy the specification
  - Implementation
    - Programs/systems that satisfy a design

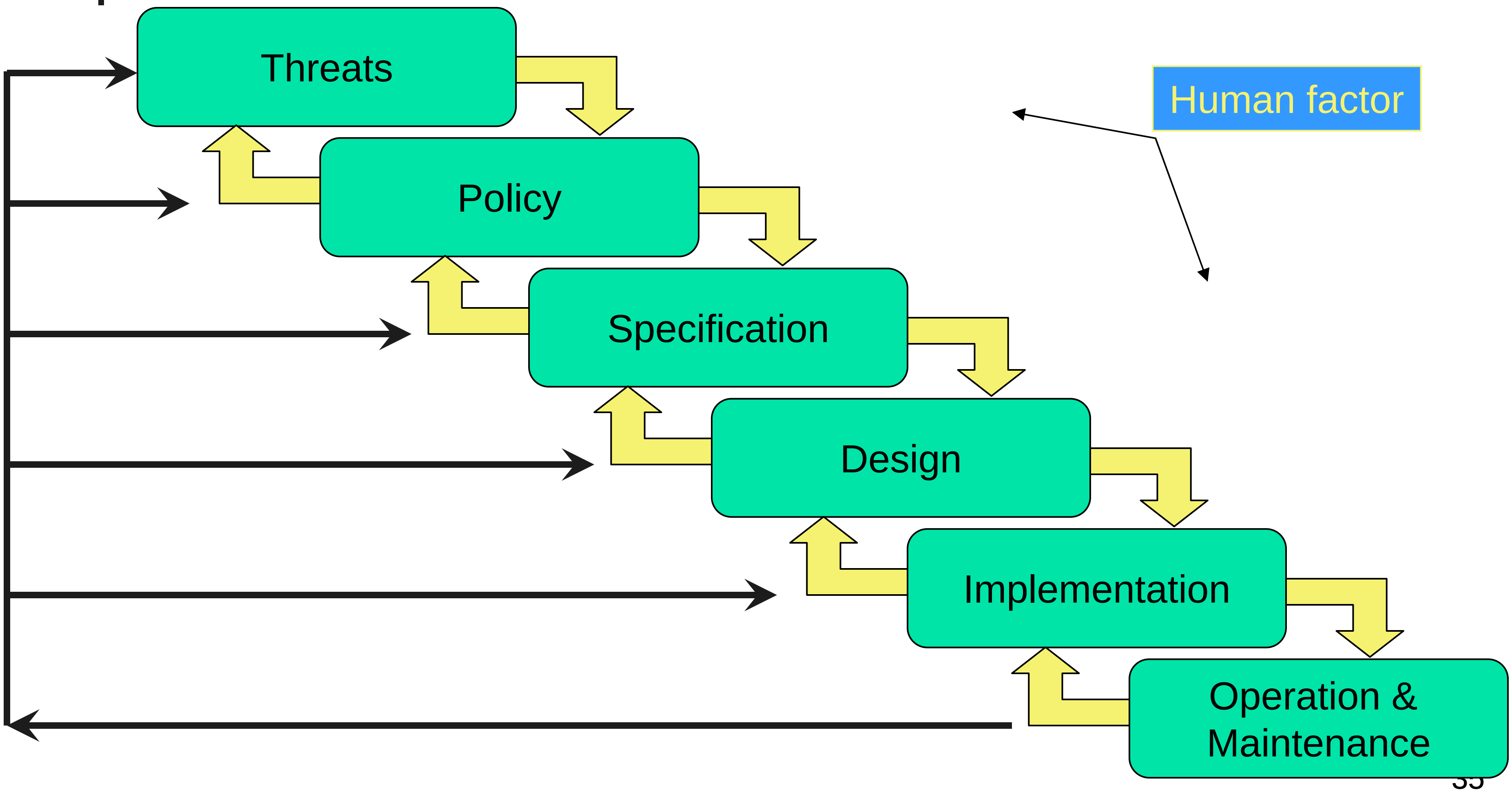
Operational Issues

- Designing secure systems has operational issues
- Cost-Benefit Analysis
  - Benefits vs. total cost
  - Is it cheaper to prevent or recover?
- Risk Analysis
  - Should we protect something?
  - How much should we protect this thing?
  - Risk depends on environment and change with time
- Laws and Customs
  - Are desired security measures illegal?
  - Will people do them?
  - Affects availability and use of technology

Human Issues

- Organizational Problems
  - Power and responsibility
  - Financial benefits
- People problems
  - Outsiders and insiders
    - *Which do you think is the real threat?*
  - Social engineering

Tying all together: The Life Cycle

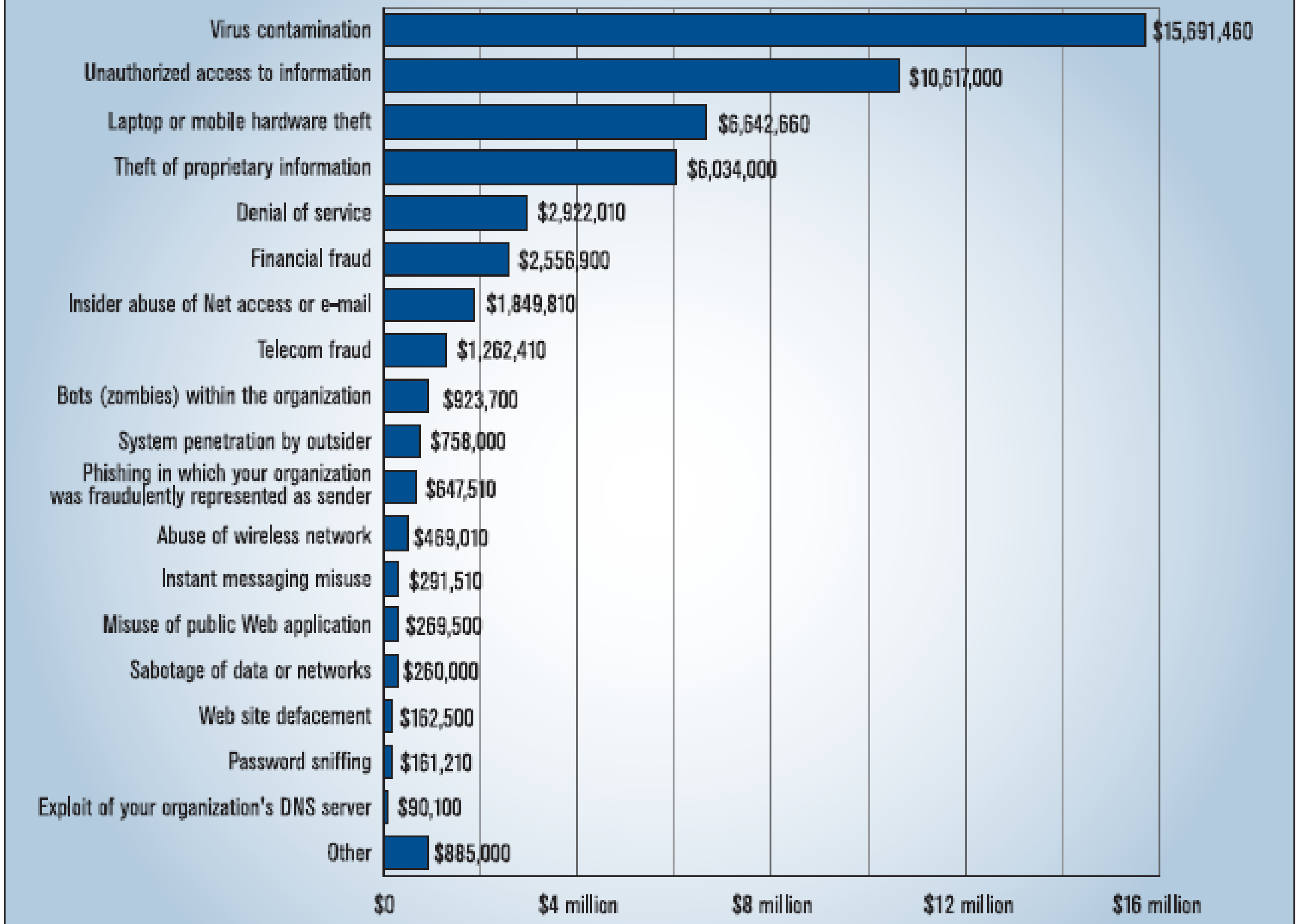


Summary

- Course outline
- Overview of security
  - Basic components:
    - CIA, Assurance
  - Policy/Mechanisms
  - Operational and human issues

2006 CSI/FBI Report

Figure 16. Dollar Amount Losses by Type



Total Losses for 2006 = $52,494,290

CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 313 Respondents

2006
CSI/FBI
Report

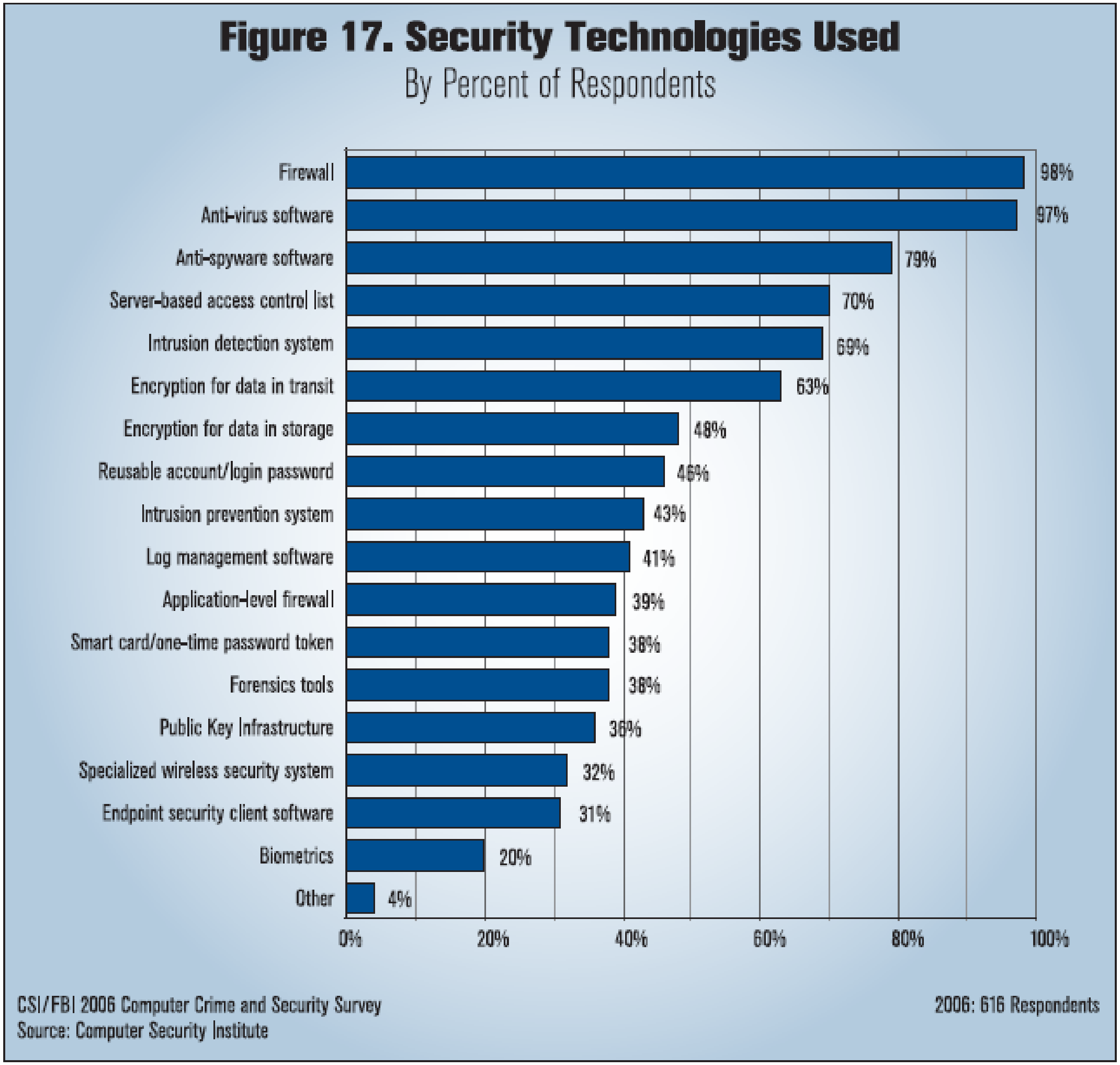


Figure 17. Security Technologies Used
By Percent of Respondents

CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 616 Respondents

2006
CSI/FBI
Report

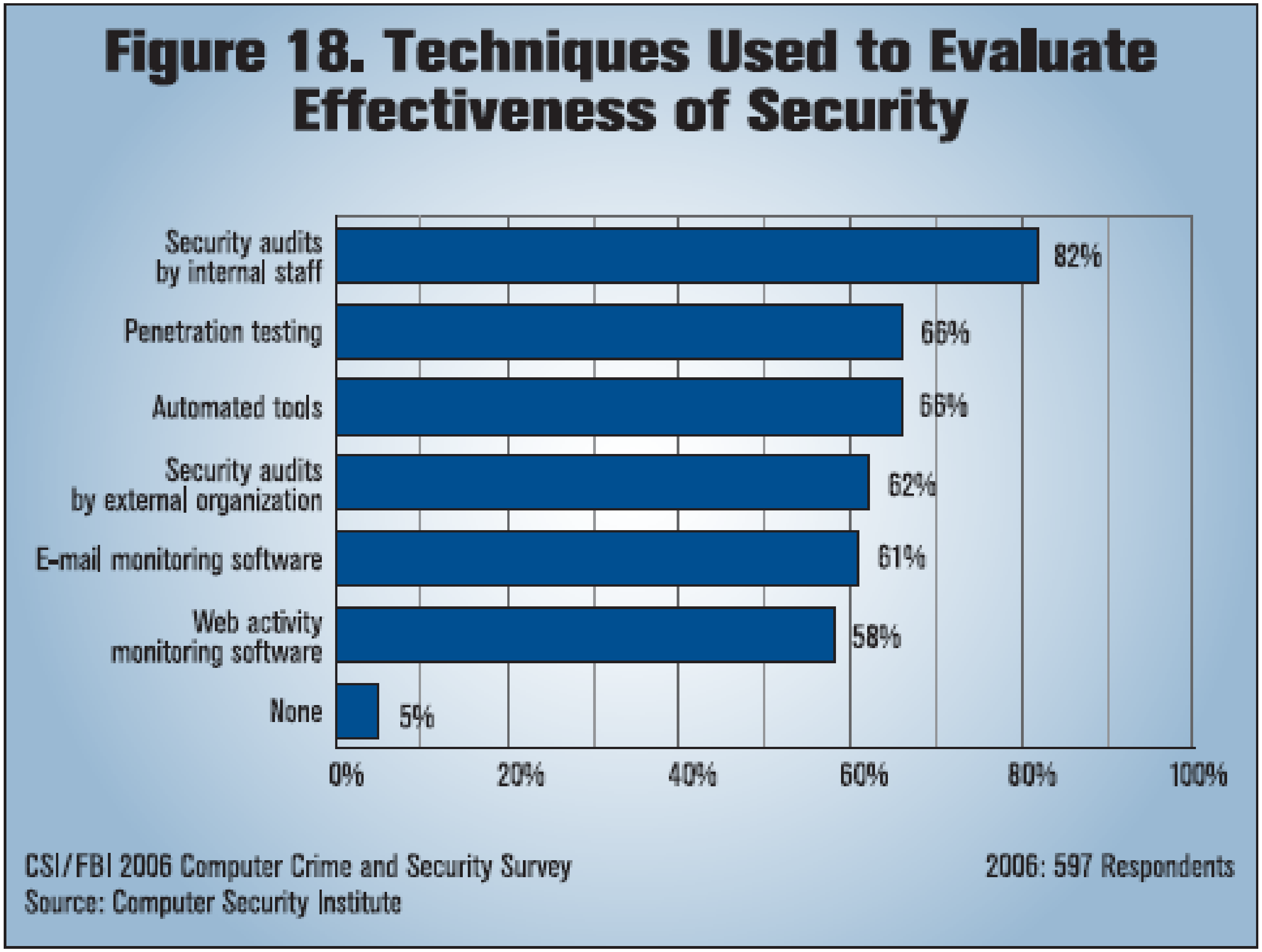
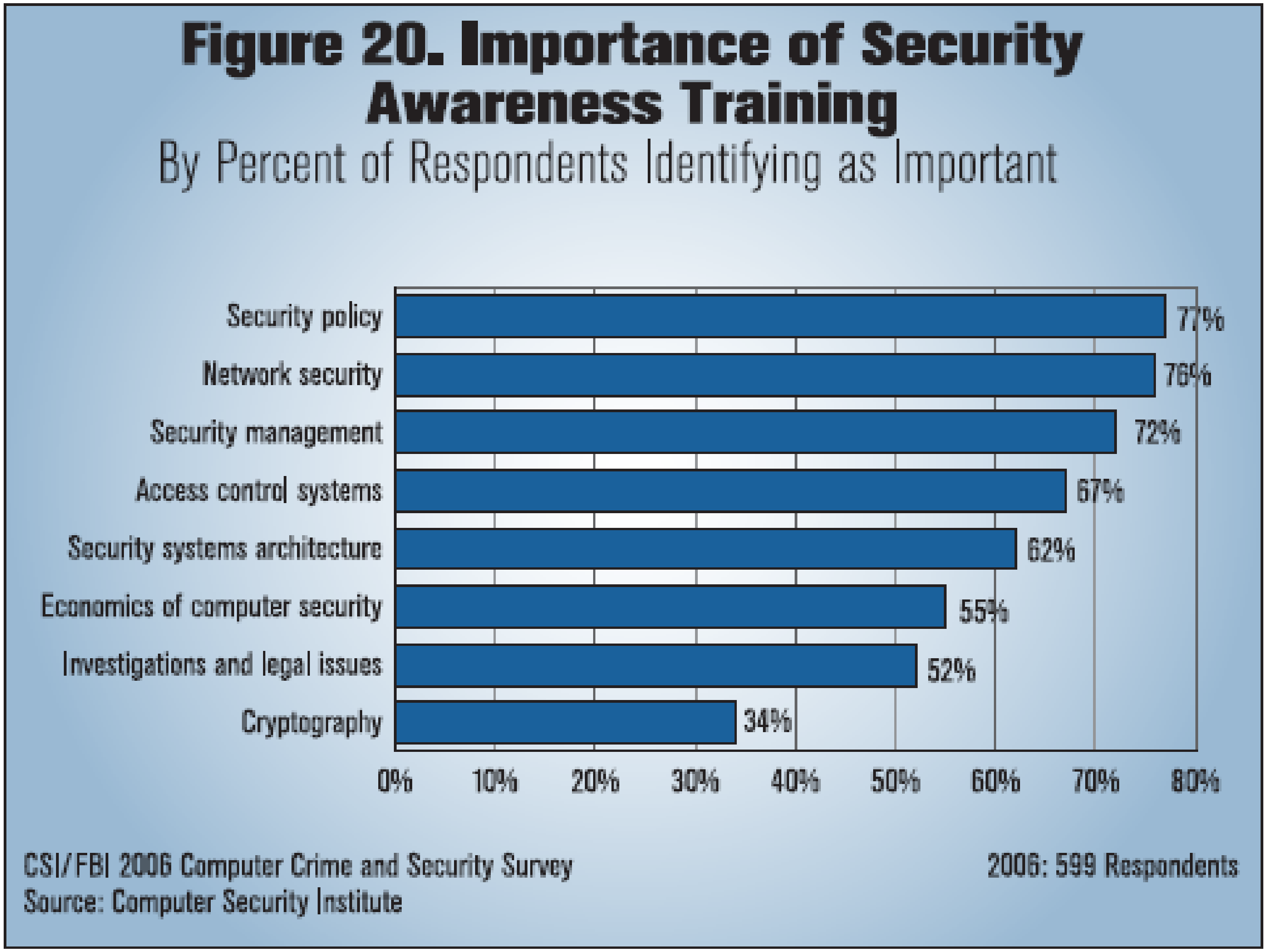


Figure 18. Techniques Used to Evaluate Effectiveness of Security

CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 597 Respondents

2006
CSI/FBI
Report



2006
CSI/FBI
Report

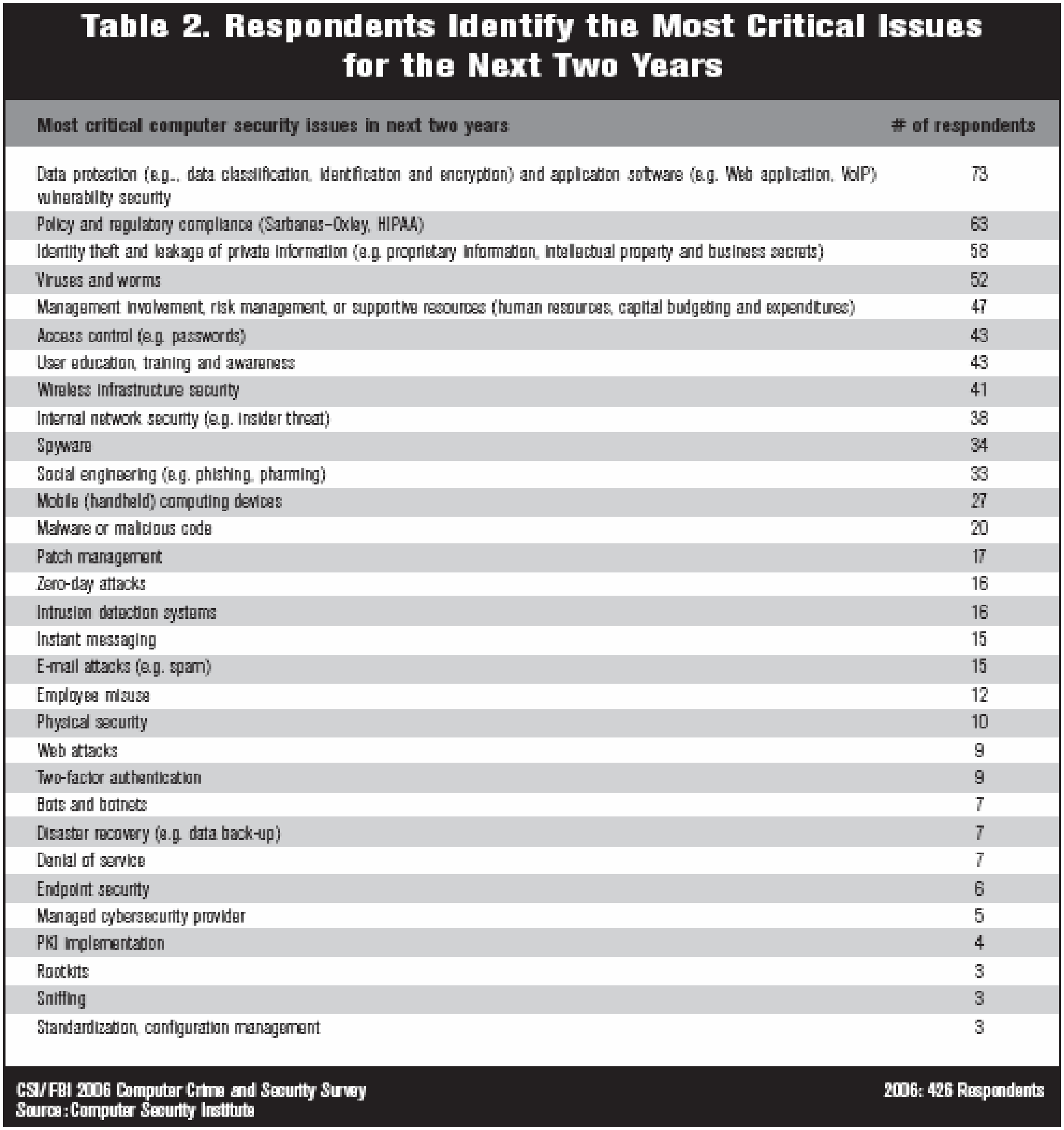


Table 2. Respondents Identify the Most Critical Issues for the Next Two Years

Most critical computer security issues in next two years	# of respondents
Data protection (e.g., data classification, identification and encryption) and application software (e.g. Web application, VoIP) vulnerability security	73
Policy and regulatory compliance (Sarbanes-Oxley, HIPAA)	63
Identity theft and leakage of private information (e.g. proprietary information, intellectual property and business secrets)	58
Viruses and worms	52
Management involvement, risk management, or supportive resources (human resources, capital budgeting and expenditures)	47
Access control (e.g. passwords)	43
User education, training and awareness	43
Wireless infrastructure security	41
Internal network security (e.g. insider threat)	38
Spyware	34
Social engineering (e.g. phishing, pharming)	33
Mobile (handheld) computing devices	27
Malware or malicious code	20
Patch management	17
Zero-day attacks	16
Intrusion detection systems	16
Instant messaging	15
E-mail attacks (e.g. spam)	15
Employee misuse	12
Physical security	10
Web attacks	9
Two-factor authentication	9
Bots and botnets	7
Disaster recovery (e.g. data back-up)	7
Denial of service	7
Endpoint security	6
Managed cybersecurity provider	5
PKI implementation	4
Rootkits	3
Sniffing	3
Standardization, configuration management	3

CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 426 Respondents