Security Planning
Overview of CNSS/NSTISS
Physical Protection

Lecture 13

December 4, 2003

Courtesy of Professors
Chris Clifton & Matt Bishop

Security Planning

- A security plan
  - Document describing how an organization addresses its security needs
  - Periodically reviewed and revised
- Creating a security plan
  - What it should do
  - Who should write the plan
  - How to acquire support for the plan

Security Planning

- A security plan must address the following
  - *Policy*
  - *Current security state*
  - *Recommendations and the requirements* to meet the security goals
  - *Accountability*
    - Who is responsible for a each security activity
  - *Timetable*
    - For different security functions
  - *Continuing attention* for periodic update

Policy

- Should address
  - *Who* should be allowed to access *what* resources and *how* should the access be regulated
- Should specify
  - Organizational security goals
  - Where the responsibility lies (accountability policy); limits of responsibility
  - Organizational support for security
  - Legal and ethical aspects?

Current Security State

- Can be determined on the basis of risk analysis
- Indicates
  - Organizational assets
  - Security threats to these assets
  - Controls in place against these threats

Recommendation and requirements

- It is important to
  - Indicate what requirements are to be imposed in a plan, and over what period
  - Phase out implementation, and indicate elements of each phase and their time periods
- The plan
  - Must be extensible
  - Must include a procedure for change and growth
  - Should remain laregelyintact through change in the organization

Responsibility for implementation

- Identify people/groups responsible for implementation
  - A plan of accountability
- Some examples
  - Personal computer users are responsible for their own machine
  - Project leaders for data and computations
  - Database administrators – access and integrity of data in databases
  - Information officers for creation and use of data, and retention and disposal of data
  - Personnel staff members – responsible for security involving employees

Timetable and Continuing Attention

- Timetable
  - Expensive and complicated controls need gradual adoption
  - Training staff on new controls
- Continuing attention
  - Timely review and reevaluation
  - Update object inventory and list of controls
  - Review risk analysis to accommodate for parameters that may change

Planning Team

- Size
  - Depends on the complexity of organization and the degree of commitment to security
  - Organizational behavior studies show optimum size of a working committee: 5 – 9
  - Larger committee as oversight body
- Committee membership should be from each of the following
  - Hardware group
  - Systems/applications programmers
    - Encryption, protocols, security in OS and networks require systems programming staff
  - Data entry personnel
  - Physical security personnel
  - Representative users

Commitment to Plan

- Acceptance of plan
  - Needs a concise, well-organized report that includes a plan of implementation and justification of costs
    - Indicate accountability,
    - time for accomplishment,
    - continuing reevaluation, etc.
- Education and publicity to help people understand and accept security plan
- Management commitment depends on
  - Understanding cause and potential effects of lack of security (Risk analysis)
  - Cost-effectiveness of security plan
  - Presentation of the plan

Organizational Security Policies

- Purpose
  - A policy is written for several different groups
- Beneficiaries
  - Their needs should be captured in the policy
- Users
  - Policy should indicate acceptable use
- Owners
  - Policy should express the expectation of owners
- Balance
  - Needs of above groups may conflict
  - Balance the priorities of all affected communities

Attributes of good policies

- Purpose (of the computing facility)
  - E.g., “protect customers’ confidentiality”, “ensure continual usability”
- Protected resources
  - All computers? Networks? All data? Customers’ data? etc.
- Protection
  - What degree of protection to which resources
- Coverage
  - Must be comprehensive enough; general enough to apply to new cases
- Durability
  - Must grow and adapt well
- Realism
  - Protection requirements must be realizable with existing mechanisms
- Usefulness
  - Must be read, understood and followed by all

Examples

- Four levels S1 o S4 with increasing strength of protection
  - S1: is not designed to protect any specific resources or any specific level of protection to services
  - S2: designed to protect regular resources and to provide normal protection against threats
  - S3: important resources, high protection
  - S4: critical resources, very strong protection

Overview of CNSS/NSTISS

Courtesy of Professors
Chris Clifton & Matt Bishop

Committee on National Security Systems (CNSS).

- National Security Telecommunications and Information Systems Security Committee (NSTISSC)
  - Re-designated as the Committee on National Security Systems (CNSS).
  - By the President, under executive Order (E.O.) 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age
  - The Department of Defense continues to chair the committee

CNSS function

- The primary functions of the CNSS include but are not limited to:
  - Develop and issue National policy and standards.
  - Develop and issue guidelines, instructions, advisory memoranda, technical bulletins and incident reports.
  - Assess the "health" of national security systems.
  - Approve release of INFOSEC products and information to foreign governments.
  - Create and maintain the National Issuance System.
  - Liaison / Partner with other security fora

National Security Telecommunications and Information Systems Security

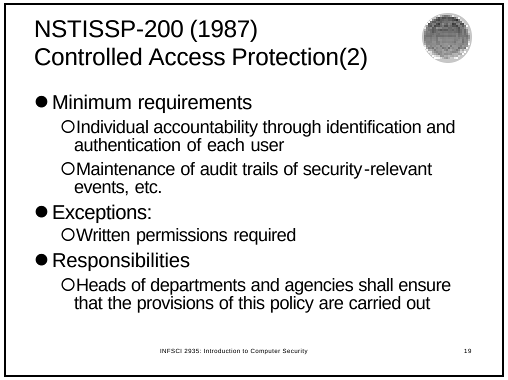
- NSTISSC Policy (NSTISSCP)
  - Addresses national security telecommunications and information systems security issues from a broad perspective
  - Establishes national goals and binds all US Government departments and agencies
- NSTISSC Directive (NSTISSCD)
  - Addresses national security telecommunications and information system security issues that go beyond the NSTISSCP
- NSTISSC Instruction (NSTISSCI)
  - Provides guidance and establishes technical criteria for specific national security telecomm. and info. sys. security issues
- NSTISSC Advisory/Info. Memorandum (NSTISSCAM)
  - Addresses ad hoc issues of a general nature leading to national security telecomm. and info. Sys. security

NSTISSP-200 (1987)
Controlled Access Protection (CAP)

- Policy:

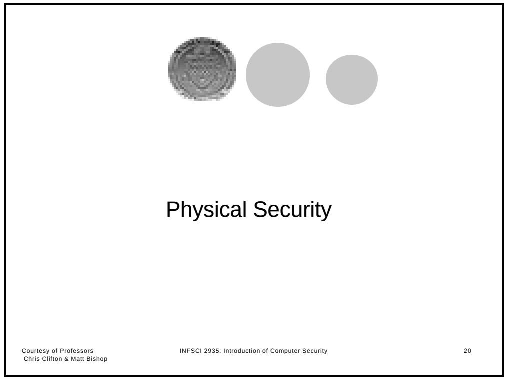
  All AIS which are accessed by more than one user, when those users do not have the same authorization to use all the classified or sensitive unclassified information processed or maintained by the AIS, shall provide automated CAP for all classified and sensitive unclassified information. This minimum protection shall be provided within five years of the promulgation of this policy

- Definitions: AIS, CAP (C2 of



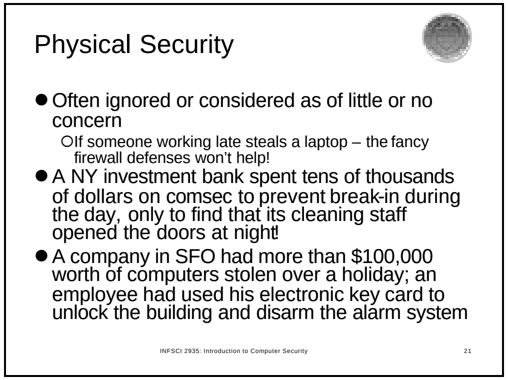
NSTISSP-200 (1987) Controlled Access Protection(2)

- Minimum requirements
  - Individual accountability through identification and authentication of each user
  - Maintenance of audit trails of security-relevant events, etc.
- Exceptions:
  - Written permissions required
- Responsibilities
  - Heads of departments and agencies shall ensure that the provisions of this policy are carried out



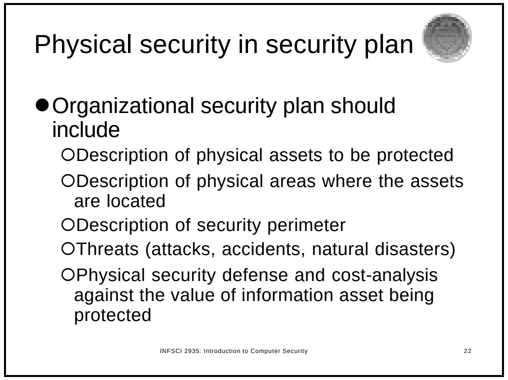
Physical Security

Courtesy of Professors
Chris Clifton & Matt Bishop



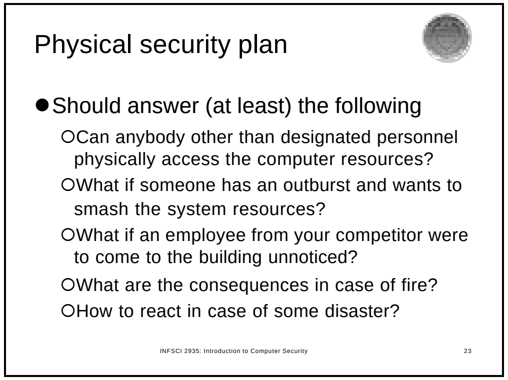
Physical Security

- Often ignored or considered as of little or no concern
  - If someone working late steals a laptop – the fancy firewall defenses won't help!
- A NY investment bank spent tens of thousands of dollars on comsec to prevent break-in during the day, only to find that its cleaning staff opened the doors at night!
- A company in SFO had more than $100,000 worth of computers stolen over a holiday; an employee had used his electronic key card to unlock the building and disarm the alarm system



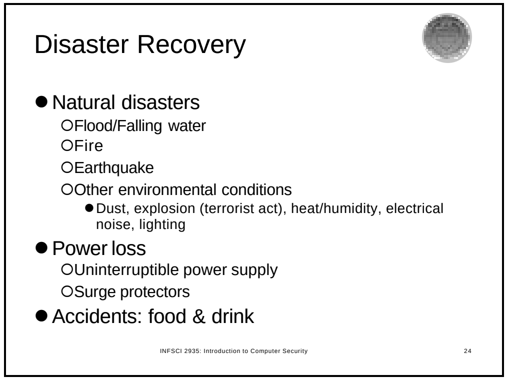
Physical security in security plan

- Organizational security plan should include
  - Description of physical assets to be protected
  - Description of physical areas where the assets are located
  - Description of security perimeter
  - Threats (attacks, accidents, natural disasters)
  - Physical security defense and cost-analysis against the value of information asset being protected



Physical security plan

- Should answer (at least) the following
  - Can anybody other than designated personnel physically access the computer resources?
  - What if someone has an outburst and wants to smash the system resources?
  - What if an employee from your competitor were to come to the building unnoticed?
  - What are the consequences in case of fire?
  - How to react in case of some disaster?



Disaster Recovery

- Natural disasters
  - Flood/Falling water
  - Fire
  - Earthquake
  - Other environmental conditions
    - Dust, explosion (terrorist act), heat/humidity, electrical noise, lighting
- Power loss
  - Uninterruptible power supply
  - Surge protectors
- Accidents: food & drink

Contingency planning

"key to successful recovery is adequate planning"

- Backup/off-site backup
- Cold-site/hot-site
  - Cold site: facility with power/cooling where computing system can be installed to begin immediate operation
  - Hot-site: facility with installed and ready to use computing system.
- Theft prevention
  - Prevent access: guards; locks; cards
  - prevent portability: locks, lockable cabinets
  - detect exit: like in library

Disposal of Sensitive Media

- Shredders
  - Mainly for paper; also used for diskettes, paper ribbons and some tapes
- Sanitizing media before disposal
  - Completely erase data
  - ERASE and DELETE may not be enough
  - Overwrite data several times
- Degaussers
  - Destroys magnetic fields
  - Fast way to neutralize a disk or tape

TEMPEST: Emanations protections

- All electronic and electromechanical info. processing equipment can produce unintentional data-related or intelligence-bearing emanations which, if intercepted and analyzed, disclose the info. transmitted, received, handled or otherwise processed (NSTISSAM 1-00)
- TEMPEST program certifies an equipment as not emitting detectable signals
  - Enclosure
    - Completely cover a tempest device
      - Shielded cable
      - Copper shielding a computer?
  - Emanation modification
    - Similar to generating noise

Review

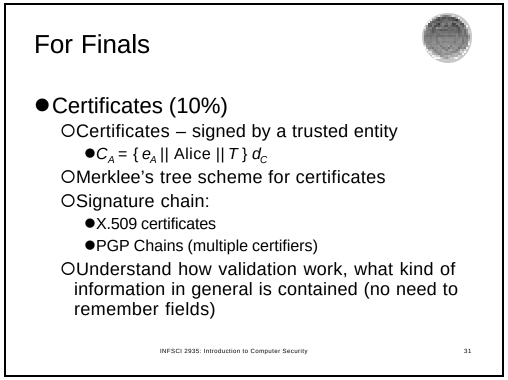
Courtesy of Professors
Chris Clifton & Matt Bishop

Before Mid-term

- Security Models
  - HRU
  - Take-grant
  - Schematic Protection/Typed access
- Policy Issues
  - Confidentiality policies:
    - Bell-LaPadula,
  - Integrity policies
    - Biba, Lipner,Clark-wilson
  - Hybrid
    - Chinese wall, RBAC

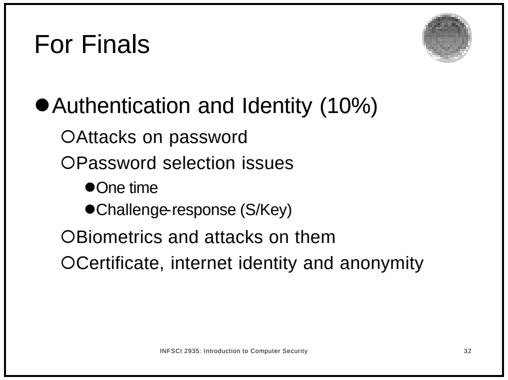
Before Midterm

- Cryptographic basics
  - Classical
    - Transposition, Substitution
  - Public-key cryptography
    - Diffie-hellman, RSA
  - Key Management (key exchange protocols)
  - Digital Signature



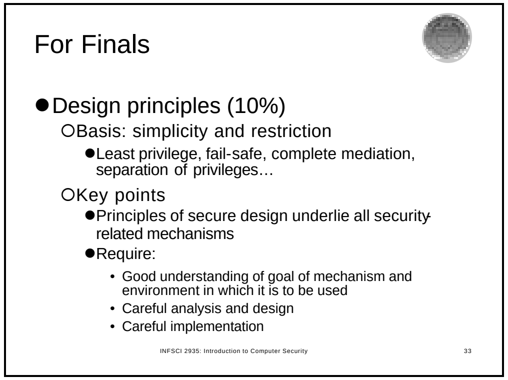
For Finals

- Certificates (10%)
  - Certificates – signed by a trusted entity
    - $C_A = \{ e_A \| \text{Alice} \| T \}\, d_C$
  - Merklee's tree scheme for certificates
  - Signature chain:
    - X.509 certificates
    - PGP Chains (multiple certifiers)
  - Understand how validation work, what kind of information in general is contained (no need to remember fields)



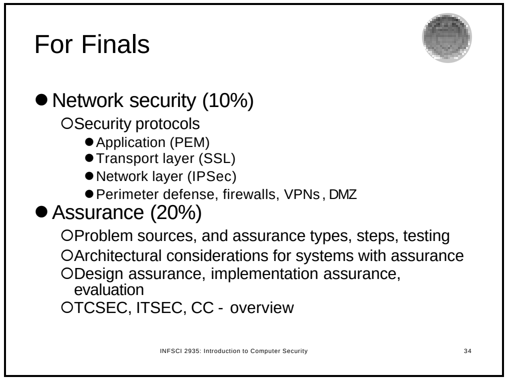
For Finals

- Authentication and Identity (10%)
  - Attacks on password
  - Password selection issues
    - One time
    - Challenge-response (S/Key)
  - Biometrics and attacks on them
  - Certificate, internet identity and anonymity



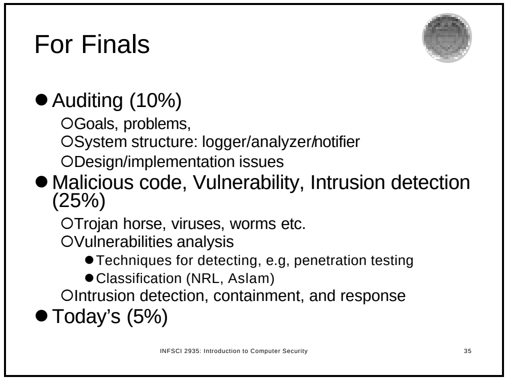
For Finals

- Design principles (10%)
  - Basis: simplicity and restriction
    - Least privilege, fail-safe, complete mediation, separation of privileges…
  - Key points
    - Principles of secure design underlie all security-related mechanisms
    - Require:
      - Good understanding of goal of mechanism and environment in which it is to be used
      - Careful analysis and design
      - Careful implementation



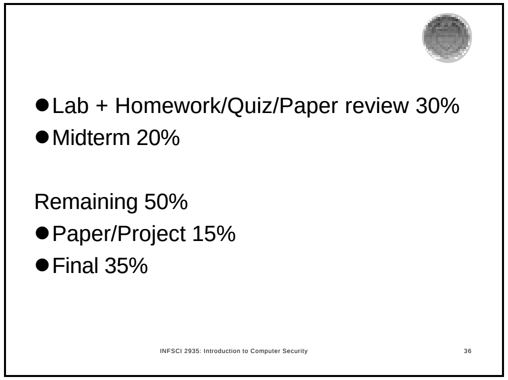
For Finals

- Network security (10%)
  - Security protocols
    - Application (PEM)
    - Transport layer (SSL)
    - Network layer (IPSec)
    - Perimeter defense, firewalls, VPNs, DMZ
- Assurance (20%)
  - Problem sources, and assurance types, steps, testing
  - Architectural considerations for systems with assurance
  - Design assurance, implementation assurance, evaluation
  - TCSEC, ITSEC, CC - overview



For Finals

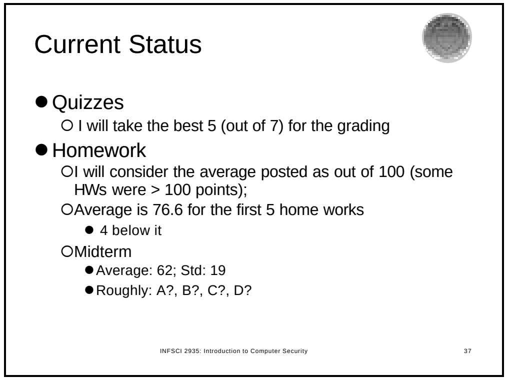
- Auditing (10%)
  - Goals, problems,
  - System structure: logger/analyzer/notifier
  - Design/implementation issues
- Malicious code, Vulnerability, Intrusion detection (25%)
  - Trojan horse, viruses, worms etc.
  - Vulnerabilities analysis
    - Techniques for detecting, e.g, penetration testing
    - Classification (NRL, Aslam)
  - Intrusion detection, containment, and response
- Today's (5%)



- Lab + Homework/Quiz/Paper review 30%
- Midterm 20%

Remaining 50%

- Paper/Project 15%
- Final 35%



Current Status

- Quizzes
  - I will take the best 5 (out of 7) for the grading
- Homework
  - I will consider the average posted as out of 100 (some HWs were > 100 points);
  - Average is 76.6 for the first 5 home works
    - 4 below it
  - Midterm
    - Average: 62; Std: 19
    - Roughly: A?, B?, C?, D?