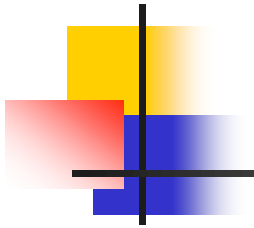
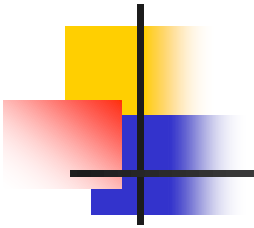


CSE 543
Information Assurance and Security

Security Strategies

Professor Stephen S. Yau



Security Strategies

- Obscurity Strategy
- Perimeter Defense Strategy
- Defense in Depth Strategy

Security by Obscurity Strategy (Stealth)

- If the existence of an organization's IA baseline and critical objects is ***unknown***, the organization might not be subject to threats
- Intent to secure the system by ***hiding*** the details of security mechanisms
- IA involves use of obscurity strategy to a certain extent

Perimeter Defense Strategy

- Focus on threats from ***outsiders***
- Intent to ***control the flow of information*** between organization's internal trusted network and the un-trusted external internet
- Not much IA capabilities is allocated to secure the ***internal*** system
- Examples: Firewall, security access keys, access codes

Perimeter Defense Strategy (cont.)

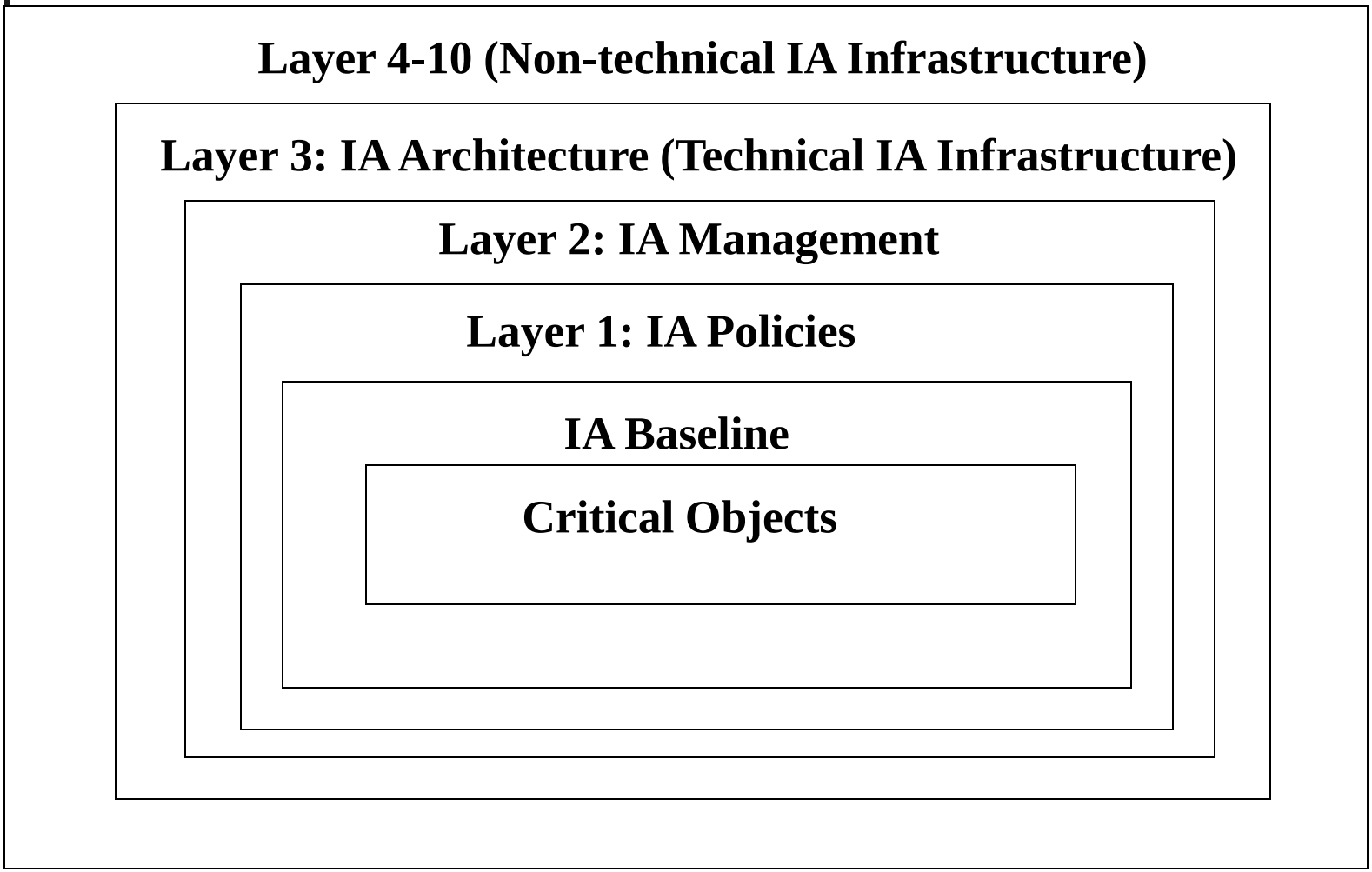
- Two critical weaknesses:
  - Very little or nothing to protect against attacks by an inside user
  - If the perimeter defenses fail, then the internal systems are open to attack

Defense in Depth Strategy

- Define a number of operationally interoperable and complementary technical and non-technical IA ***layers*** of defense
- Separate organization network into ***enclaves***
  - An ***enclave*** is an environment under control of a single authority with personnel and physical security measures.
- ***Perimeter defense*** for each enclave
- Complicated and multiple ***connections*** among enclaves and between an enclave and outside
- Need ***multiple layers*** and ***different solution for each connection***

Defense in Depth Strategy

--- Layered Architecture Model



Defense in Depth Strategy (cont.)
--- Layered Architecture Model

-Core consists of ***critical objects*** and ***IA baseline*** that collect, input, process, store, output, and communicate with any element in core.

-IA Policies (Layer 1) define the actions and behavior required to accomplish the organization's IA needs.

-IA Management (Layer 2) monitors and controls implementation of the IA policies.

-IA Architecture (Layer 3) provides a means to allocate and integrate technical and non-technical controls

Defense in Depth Strategy (cont.)
--- Layered Architecture Model

- ***Layers 4 to 10*** involve non-technical implementations of IA policies, and provide ***infrastructure*** in support of IA Architecture
  - Layer 4 Operational security administration
  - Layer 5 Configuration management
  - Layer 6 Life-cycle security
  - Layer 7 Contingency planning
  - Layer 8 IA education, training, awareness
  - Layer 9 IA policy Compliance Oversight
  - Layer 10 IA incident response and reporting

Layer 3: IA Architecture

- Ensure that at least the minimum level of interoperability and services is available to authorized users to perform their tasks, to coordinate with other users, and to exchange information securely
- Integrates three types of security:
  - Physical security
  - Procedure security
  - Logical security

Layer 4: Operational Security Administration

- People:
  - Users: general and privileged
  - Separation of roles
  - Prevention
  - Limitation
  - Accountability
  - Detection
  - Deterrence
  - Outsourcing
- Security operations, such as encryption, hashing, access control, auditing

Layer 5: Configuration Management

- Provide a mechanism to ensure ***documentation of all changes***
- Identify anticipated ***effects of changes*** on cost/schedule as a basis for approving or disapproving proposed changes
- Maintain ***integrity of schedule***
- Maintain updated ***documentation on status of each proposed change***
- Ensure ***all changes communicated to appropriate personnel***

Layer 6: Life-Cycle Security

- Security is involved in each state of the system's life cycle:
  - Initiation
  - Definition
  - Design
  - Acquisition
  - Development and implementation
  - Operation and maintenance
  - Destruction and disposal

Layer 7: Contingency Plan

- Planning for the worst
  - Backups
  - Power outage
  - Emergency action and disaster recovery plan
  - Continuity of operations plan

Layer 8: IA Education, Training, and Awareness

- IA support services
- IA awareness programs
- IA curriculum development, certification and accreditation
- IA compliance inspection and validation
- Workshop, conference and symposia support

Layer 9: IA Policy Compliance Oversight

- Provide a means of ***detecting, reporting, and correcting noncompliance*** with the ***IA policies***
- Implementation can be performed both internally and by external parties
- Mechanisms
  - Intrusion detection systems
  - Scanners
    - Probing vulnerabilities of network to prevent attacks
    - Specifying IP addresses to check origins of communication (OS, servers, routers, firewalls,…)
  - Automated auditing
  - Malware detection tools
  - Periodic assessments of IA management and vulnerabilities

Layer 10: IA Incident Response & Reporting

- No perfect prevention systems, and incidents are expected
- General incident handling procedures:
  - Determine appropriate response
  - Collect and safeguard the information
  - Contain the situation
  - Assemble the incident management team
  - Create evidence disks and printouts
  - Eradicate/clean up/recover
  - Prepare preliminary status report for management and other authorities
  - Document and report all activities
  - Lesson learned: make improvements