CSE 543
Information Assurance

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 flow of information*** between organization's internal trusted network and untrusted external internet
- Not much IA capabilities is allocated to secure ***internal*** system
- Examples: Firewalls, security access keys, access codes

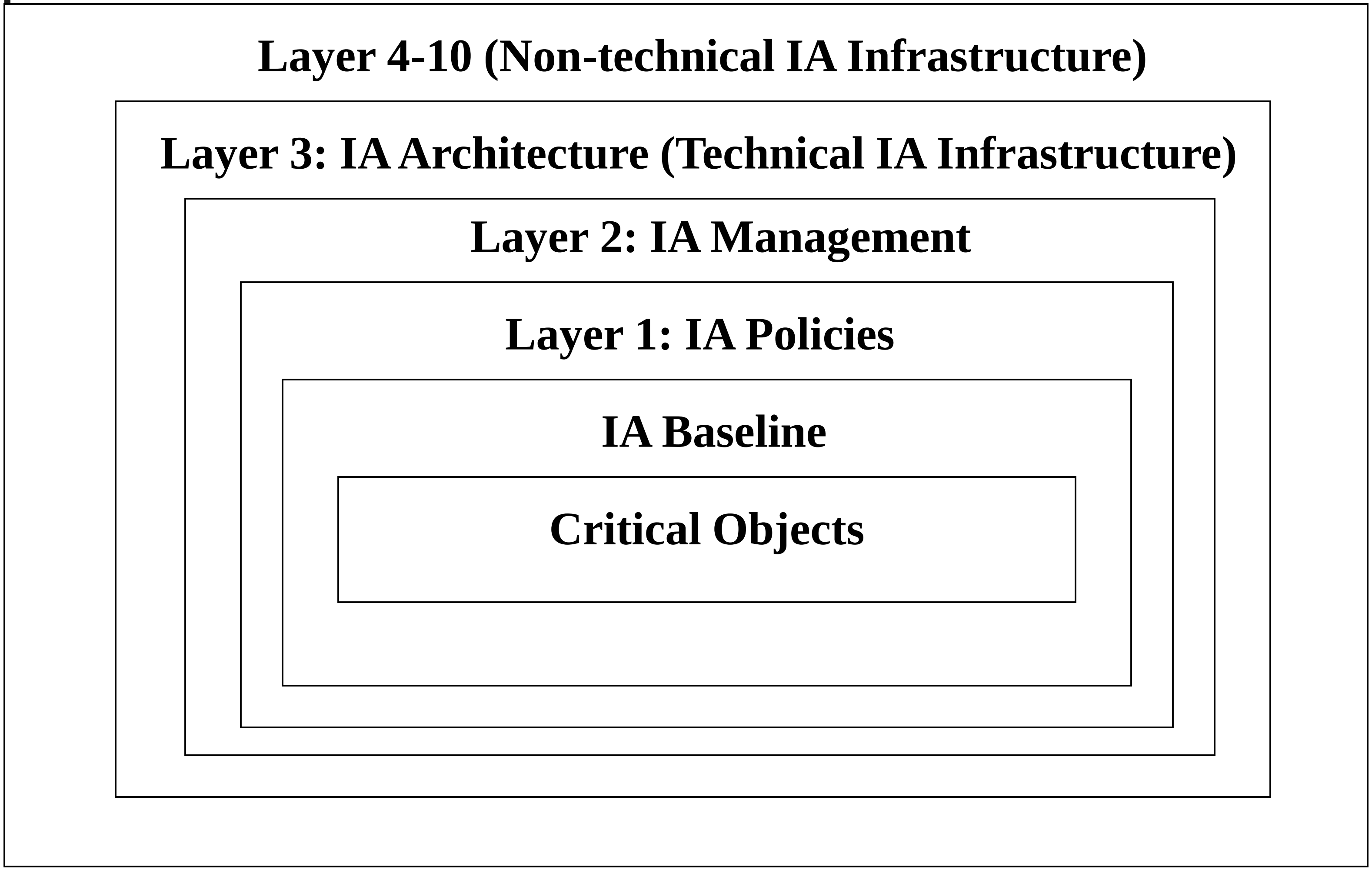
Perimeter Defense Strategy (cont.)

- Two critical weaknesses:
  - Very little or nothing to protect against attacks by inside users
  - 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’s 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



Layer 4-10 (Non-technical IA Infrastructure)

Layer 3: IA Architecture (Technical IA Infrastructure)

Layer 2: IA Management

Layer 1: IA Policies

IA Baseline

Critical Objects

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

- Ensures 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 levels 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

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 plan/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
  - Virus detectors
  - 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:
  1. Determine appropriate response
  2. Collect and safeguard relevant information
  3. Contain the situation
  4. Assemble the incident management team
  5. Create evidence disks and printouts
  6. Eradicate/clean up/recover
  7. Prepare preliminary status report for management and other authorities
  8. Document and report all activities
  9. Lesson learned: make improvements

Mission Assurance

- ***Mission Assurance***
  - A ***life-cycle engineering process*** to ***identify and mitigate*** the ***deficiencies of mission requirements, design, production, test, and field support for mission success***
- ***Goal*** of Mission Assurance
  - To create a ***state of resilience*** that supports the ***continuation*** of an entity's ***critical business processes and protects its employees, assets, services, and functions.***

Mission Assurance (cont.)

- Includes ***disciplined application*** of ***system engineering, risk management, quality and management principles*** to achieve ***success*** of the following,
  - ***Requirement analysis***
  - ***Design***
  - ***Development***
  - ***Testing***
  - ***Deployment***
  - ***Operations process***
- Mission assurance also covers the ***enterprise, supply base, business partners, and customer base*** to enable ***mission success***.

Mission Assurance (cont.)

- In practice, information assurance (IA) focuses on protection of data and systems often conflicts with the “get the job done” attitude of mission assurance.
- This conflict is largely eliminated when the focus of information assurance is bifurcated into
  - ***protecting the infrastructure and data***, and
  - ***securely sharing information with authorized recipients.***

Mission Assurance Use Cases

- The US Department of Defense 8500-series of policies has defined three mission assurance categories (MACs) that form the basis for ***availability and integrity requirements***
    - ***MAC I*** systems handle information ***vital*** to the ***operational readiness or effectiveness of deployed or contingency forces***.
        - Loss of MAC I data would cause ***severe damage*** to the successful completion of a DoD mission.
        - MAC I systems must maintain the highest levels of both ***integrity and availability*** and ***use the most rigorous measure of protection.***

Mission Assurance Use Cases (cont.)

- ***MAC II*** systems handle information ***important*** to ***the support*** of ***deployed and contingency forces***.
  - The loss of MAC II systems could have a ***significant negative impact*** ***on the success of the mission or operational readiness***.
  - MAC II systems must maintain the highest level of ***Integrity***.
  - The loss of availability of MAC II data can be ***tolerated*** ***only for a short period of time***, so MAC II systems must maintain a ***medium level of availability***.
  - MAC II systems require ***protective measures above industry best practices*** to ensure ***adequate integrity and availability of data.***

Mission Assurance Use Cases (cont.)

- ***MAC II***I systems handle information that is ***necessary*** for ***day-to-day operations***, but not directly related to the support of deployed or contingency forces.
  - Loss of MAC III data would ***not have a significant immediate impact*** on mission effectiveness or operational readiness in short term
  - MAC III systems are required to maintain ***basic levels of integrity and availability.*** MAC III systems must be protected by measures considered as ***industry best practices***.

References

- J. G. Boyce, D. W. Jennings, *Information Assurance*: *Managing Organizational IT Security Risks*. Butterworth Heineman, 2002, ISBN 0-7506-7327-3
- M. E. Whitman and H. J. Mattord , Principles of Information Security, 5th edition, Thomson Course Technology, November 2014
- Rahul Gupta, "The Need for Mission Assurance". *PRTM Magazine*, 2006.