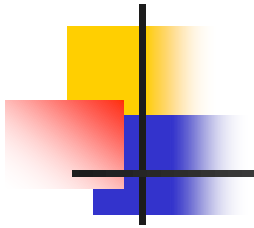

CSE 543
Information Assurance and Security

Security Principles

Professor Stephen S. Yau

Security Principles

1. ***Auditability*** and ***Accountability***
   - ***Auditability*** is the ability to **verify** the activity of a control
   - ***Accountability*** is to hold individuals **answerable, responsible or liable** for specific activities
   - Security control must produce **reliable, indisputable evidence**
     - Evidence can take forms of **audit trails**, **system logs**, **alarms**, other overt or covert notifications
     - With feedback, management can determine whether control is functioning properly

Security Principles (cont.)

2. ***Access Control***

- Prevent any user from seeing or using unauthorized information
- Prevent unauthorized modification or disclosure of that information.
- Access control principles include

  1) ***Separation of functions****:*
  - No one owns all the processes, controls all security features, or possesses unrestricted access to all information

  2) ***Independence of control and subjects****:*
  - The person charged with security control and the persons subject to such control should be independent

Security Principles (cont.)

2. *Access Control (cont.)*

3) Least privilege:

- User given only needed access or privilege to do the assigned job

4) Control

- All access to the system must be regulated

5) *Discretionary Access Control (DAC)*

- Restricting access to objects based on identity of subjects and/or groups to which they belong
- Controls are ***discretionary*** in the sense that user or process given discretionary access to information is capable of passing that information to another subject

Security Principles (cont.)

2. *Access Control (cont.)*

6) Mandatory Access Control (MAC)

- Restrict access to objects based on ***sensitivity*** (as represented by a label) of the ***information*** contained in the objects and the formal authorization (*i.e.* clearance) of subjects to access information of such sensitivity.

7) Role-Based Access Control (RBAC)

- Associate ***roles*** with each ***individual.***
- Each role defines a specific set of operations that the individual acting in that role may perform.
- Individual needs to be authenticated, chooses a role that has been assigned to individual, and accesses information according to operations needed for the role.

Security Principles (cont.)

3. ***Confidentiality***

- Protect information from unauthorized disclosure
- Confidentiality principles include:

1) Need to know

- A individual should possess combination of clearance, privilege of access, **and need-to-know** before being authorized access to the information

2) Data separation

- Physically separating data and filtering

3) Compartmentalization

- Individual has pieces of information based on need-to-know
- Too much information increases possibilities that a whole picture may be constructed and used illicitly

Security Principles (cont.)

3. ***Confidentiality (cont.)***

4) Classification

- Assign labels to information in order to identify the appropriate level of protection, handling and control of the information.

Corporation	***US Government***
Public Use	Unclassified
Internal Use Only	Official Use Only
Confidential	Confidential
Confidential-Restricted	Secret
Registered-Confidential	Top Secret

Security Principles (cont.)

3. *Confidentiality (cont.)*

5) Encryption

- A reversible process of transforming plain text into enciphered text using an encryption algorithm.
- Public key infrastructure (PKI) includes
  - Digital certificates
  - Certificate authorities (CA)
  - Registration authorities
  - Certificate revocation
  - Policies and procedures
  - Nonrepudiation support
  - Time-stamping
  - Lightweight Directory Access Protocol (LDAP)
  - Security–enabled applications

Security Principles (cont.)

4. ***Integrity***
   - Calculating the data being transmitted and binding the value to the original data. Recalculating the received data to match the one sent to ensure that no modification occurred during transmission.
5. ***Asset Availability***
   - Applying measures for access control, integrity and confidentiality
   - Closing known security holes in OS and network
   - Backup procedures
   - Data recovery procedures
   - Preventive maintenance plan
   - Continuity of operations plan
   - Emergency action plan

Security Principles (cont.)

7. ***Cost Effectiveness***
8. ***Risk Management***
   - Risk is an expected loss of accountability, access control, confidentiality, integrity, or availability which may cause an attack or incident
   - Risks should be identified and analyzed to assess impact of each of them. Management determines whether certain risks are ***tolerable*** or whether some measures are ***required to mitigate a risk to a tolerable level***
   - Risk management includes measures required to maintain a level of tolerable risks

Security Principles (cont.)

9. ***Comprehensive and Integrated Approach***
   - Measures, practices and procedures should take account of and address all relevant security considerations, security disciplines, and security interdependencies.
10. ***Life-cycle Management***
   - Information system acquisition, integration, configuration, testing, implementation, operation, and disposal are controlled and managed

Security Principles (cont.)

11. ***Training and Awareness***
    - Everyone in organization should know and understand his/her ***security and responsibility***
12. ***Continuous Reassessment***
    - Organization and its information, facilities, system/network, environment are dynamic
    - Security safeguards must be constantly re-evaluated for applicability and effectiveness
13. ***Respect of Ethical and Democratic Rights***
14. ***Legal Issues***

Some Definitions

- ***Choke point***
  - ***Funneling activities through a narrow channel*** improves ability to control and monitor activities
- ***Consistency***
  - System behaves in same manner each time according to its configuration regardless who accesses it; and there is ***no unplanned variation*** in system's behavior; for instance, system can be configured to no response for all unauthorized accesses
- ***Control of periphery***
  - To deny entry to intruders at choke points
- ***Defense in depth***
  - Multiple, overlapping layers of control provides better protection

Other Security Principles

- ***Deny upon failure***
  - Failed control default to denial of access or service
- ***Diversity of defense***
  - Additional security is derived from having more than one type or brand of same control.
  - Trade-offs in additional acquisition, operation, maintenance costs
- ***Interdependency***
  - Security depends on other services to achieve IA
- ***Override***
  - Permit proper authorities to stop operation of control only in special circumstances

Other Security Principles (cont.)

- ***Reliability***
  - System behaves as expected
- ***Simplicity***
  - Simpler the control, easier to implement, test and verify
- ***Timeliness***
  - Prevention and response to breaches ***timely***
- ***Weakest link***
  - A chain is only as strong as its weakest link
  - Security of a network is only as effective as the least protected or weakest point

Mission Assurance

- **Mission Assurance**
  - A life-cycle engineering ***process*** to identify and mitigate the mission requirements, design, production, test, and field support deficiencies of 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 the 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) focus 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 (1) protecting the infrastructure and data, and (2) 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 III 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 the 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

- M. E. Whitman and H. J. Mattord , *Principles of Information Security*, 4th edition, Thomson Course Technology, January 2011
- "DoD Instruction 8500.2, Information Assurance (IA) Implementation, 2/6/2003". Department of Defense.
- "The Need for Mission Assurance". RAHUL GUPTA, PRTM, 2006.