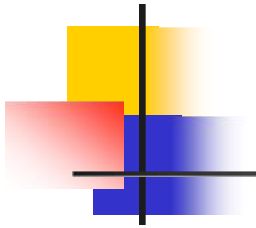

CSE 465
Information Assurance

Security Principles

Professor Stephen S. Yau

Information Assurance (IA)
Overview and Concepts

- Concepts
- Principles & strategies
- Techniques
- Guidelines, policies & laws

Information Forms and States

- **Information Forms**
  - Hard copy
  - Softcopy
  - Records of formal and informal meetings
  - Telephone conversations
  - Video teleconferences
  - ……. .
- **Information States**

  Transmitted, processed, and stored

Threats and Vulnerabilities

- A *threat* is a ***potential occurrence*** that can have an undesirable effect on the system assets or resources
- A *vulnerability* is a ***weakness*** that makes a threat to possibly occur

Four Categories of Threats

- ***Disclosure*:** Unauthorized access to information
  - Snooping
- ***Deception*:** Acceptance of false data
  - Alteration
  - Spoofing
  - Denial of receipt
- ***Disruption*:** Interruption or prevention of correct operations
  - Alteration
- ***Usurpation***: Unauthorized control of part of a system
  - Alteration
  - Spoofing
  - Delay
  - Denial of Service

Necessary Protection

- Protect ***working areas*** from outside intrusion or theft
- ***Keep equipment*** in secure rooms, and make sure it works properly
- Review ***programs*** carefully to detect potential malicious logic
- Keep track of all ***sensitive files, documents, conference records, experiment results***, which may be on printed papers. stored in storage media, CDs or DVDs.
  - ***Protect*** them from unauthorized access.
  - ***Backup*** this information periodically in case of system failure
- Encrypt ***sensitive information*** during storage or transmission
- Obfuscate ***sensitive data*** during processing
- Choose good ***passwords*** and change them periodically
- Report ***abnormal action***s immediately

Security Principles

1. Auditability and ***Accountability***

- ***Auditability*** is the ability to **verify** the activities of a ***contro***l
- ***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.

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. The measures include
  - 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 Additional 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

DoD Definition of Information Assurance

Information Assurance (IA) is information operations (IO) that protect and defend ***information and information systems*** by ensuring their ***availability***, ***integrity***, ***authentication***, ***confidentiality*** *and* ***nonrepudiation***.

Information Characteristics

***Availability*:**

Timely and reliable access to data and information services for authorized user.

***Integrity*:**

Protection against unauthorized modification or destruction of information

***Authentication*:**

Security measure designed to establish validity of transmission, message, or originator, or means of verifying an individual's authorization to receive specific categories of information

Information Characteristics (cont.)

***Confidentiality*:**

Assurance that information is not disclosed to ***unauthorized persons, processes, or devices.***

***Nonrepudiation*:**

Assurance that sender of data is provided with proof of delivery to recipient, and recipient is provided with proof of sender's identification.

***Privacy*:**

Ability and/or right to protect certain ***personal data***; extends ability and/or right to prevent invasion of ***personal information or space***.Extends to ***families***, but not to legal persons, such as corporations, organizations, schools

Information Characteristics (cont.)

***Secrecy*:**

Refers to the effect of mechanisms used to limit number of principals who can access information, such as cryptography or computer access control

***Denial of Service*:**

Mechanisms which prevent legitimate users from using the system.

Information System

- Information system consists of
  - Computer systems and networks
  - Information
  - Operating environments

INFOSEC

- ***INFOSEC*: *Information Systems Security***
  - Protection of information systems against ***unauthorized access* to**, or ***modification of, information***, whether in storage, processing or transit, and against ***denial of service to authorized users*** or ***provision of service to unauthorized users***, including those measures necessary to detect, document, and counter such threats.

OPSEC

- ***OPSEC*: *Operations Security***
  - A *process* that determines ***what information adversaries*** can obtain or piece together from observation and to provide ***measures*** for ***reducing such vulnerabilities*** to ***acceptable levels***

Other Important Terms

- ***Rainbow Series***
  - A series of computer security standards published by US government in 1980s and 1990s describing a process of evaluation for ***trusted systems***.
  - Originally published by DoD Computer Security Center, and then by the National Computer Security Center. Total 35 books have been published
  - Nicknames based on the colors of their covers. For example, the first book of the series and the most well-known book is The DoD Trusted Computer System Evaluation Criteria (DoD 5200.28-STD) in 1983, which is often referred to as ***"The Orange Book"***

Other Important Terms (Cont.)

- ***Indicators:***
  - ***Profile*** indicator – normal activities
  - ***Deviation*** indicator – different from normal activities
  - ***Tip-off*** indicator – drawing attention to information that otherwise might pass unnotices.

References

- M. E. Whitman and H. J. Mattord , *Principles of Information Security*, 5th edition, Thomson Course Technology, November 18, 2014
- "DoD Instruction 8500.2, Information Assurance (IA) Implementation, 2/6/2003". Department of Defense.