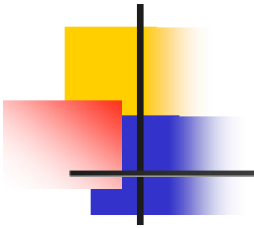


CSE 543
Information Assurance and Security

Security Principles

Professor Stephen S. Yau

Fall 2022

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

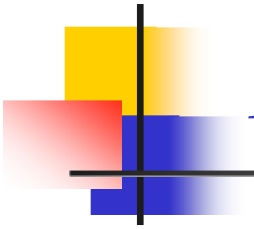
- A ***threat*** is a ***potential occurrence*** that can have an undesirable effect on the system assets or resources
- A ***vulnerability*** is a ***weakness*** that makes a threat to possibly occur

Four Categories of Threats

- ***Disclosure*:** Unauthorized access to information
  - Snooping
- ***Deception*:** Acceptance of false data
  - Alteration
  - Spoofing
  - Denial of receipt

Four Categories of Threats (cont.)

- ***Disruption*:** Interruption or prevention of correct operations
- ***Usurpation***: Unauthorized control of part of a system
  - Alteration
  - Spoofing
  - Delay
  - Denial of Service



Possible Protection

- Protect ***working areas***
- ***Keep equipment*** in ***secure environment*** and ensure it ***works properly.***
- Review ***software*** carefully to detect potential ***malicious logic.***

Possible Protection (cont.)

- Keep ***track*** of all ***sensitive files, documents, conference records, experiment results***, on printed papers or in any types of storage media.
  - ***Protect*** them from ***unauthorized access.***
  - ***Backup*** this information periodically

Possible Protection (cont.)

- ***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 ***control***
- ***Accountability*** is to hold ***individuals answerable, responsible or liable f***or specific activities
- ***Security control*** must produce ***reliable, indisputable evidence***
  - Evidence can take forms of **audit trails**, **system logs**, **alarms**, other overt or covert notifications

Security Principles (cont.)

2. Access Control

- ***Prevent reading modification disclosure or use*** of ***unauthorized information***

Security Principles (cont.)

2. Access Control (cont.)

- **Access control principles:**

  ***a) Separation of functions*:**

  - No one owns all the processes, controls all security features, or possesses ***unrestricted access to all information***

Security Principles (cont.)

2. Access Control (cont.)

- **Access control principles** (cont.):

b) Independence of control and subjects

c) Least privilege

d) Control

  - All access to the system must be regulated

Security Principles (cont.)

- **Access control types**

a) Discretionary Access Control (DAC)

b) Mandatory Access Control (MAC)

c) Role-Based Access Control (RBAC)

d) Situation-Aware Control (SAC)

Security Principles (cont.)

3. Confidentiality

- ***Protect*** information from ***unauthorized disclosure*** to persons, processes, or devices
- ***Confidentiality principles*** include:
  - ***1)Need to know:*** Possess combination of clearance, privilege of access, and need-to-know before being authorized access
  - ***2) Data separation***
  - ***3) Compartmentalization***

Security Principles (cont.)

3. Confidentiality (cont.)

4) Classification

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

Corporation

- Public Use
- Internal Use Only
- Confidential
- Confidential-Restricted
- Registered-Confidential

US Government

- Unclassified
- Official Use Only
- Confidential
- Secret
- Top Secret

Security Principles (cont.)

3. Confidentiality (cont.)

5) Encryption

- A reversible process of transforming plain text into enciphered text using an encryption algorithm.

4. Integrity:

- Protection against ***unauthorized modification or destruction*** of information

Security Principles (cont.)

5. Asset Availability

- Possible mechanisms
  - Backup procedures
  - Data recovery procedures
  - Preventive maintenance plan
  - Continuity of operations plan

Security Principles (cont.)

6. Cost Effectiveness

7. Risk Management

- Risk is an expected loss of accountability, access control, confidentiality, integrity, or availability due to an attack or incident

Security Principles (cont.)

8. Comprehensive and Integrated Approach

- Measures, practices and procedures should address ***all relevant security considerations and security interdependencies***.

9. Life-cycle Management

Security Principles (cont.)

10. Training and Awareness

- Everyone in organization should understand his/her ***security responsibility***

11. Continuous Reassessment

12. Respect of Ethical and Democratic Rights

13. Legal Issues

Additional Definitions

- ***Choke point***
  - ***Funneling activities through a narrow channel*** improves ability to control and monitor activities
- ***Consistency***
- ***Defense in depth***
  - Multiple, overlapping layers of control provides better protection

Additional Definitions (cont.)

- ***Deny upon failure***
  - Failed control default to denial of access or service
- ***Diversity of defense***

Additional Definitions (cont.)

- ***Interdependency***
  - Security depends on other services to achieve IA
- ***Override***
  - Permit proper authorities to stop operation of control only in special circumstances

Additional Definitions (cont.)

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

Additional Definitions (cont.)

Nonrepudiation:

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

Additional Definitions (cont.)

Secrecy:

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

Additional Definitions (cont.)

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 and organizations.

Additional Definitions (cont.)

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

Additional Definitions (cont.)

- ***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.

Additional Definitions (cont.)

- ***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

Additional Definitions (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*, 7th edition, Thomson Course Technology, June 27, 2021. ISBN-10: 035750643X, ISBN-13 : 978-0357506431
- "DoD Instruction 8580.1, Information Assurance (IA) Implementation, 9/7/2004". Department of Defense. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/858001p.pdf