

The Pillars

There are thus three basic pillars on which security rests:

1. Confidentiality
2. Integrity
3. Availability

Maintaining the above constitute the three security objectives for all information systems

Confidentiality

Confidentiality covers both:

1. **Confidentiality** ensures that private or confidential information is not made available or disclosed to unauthorised individuals
2. **Privacy** ensures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Confidentiality

- Confidentiality covers both the concealment of information **and** resources
- Knowledge of a resource may lead to inappropriate or unauthorised usage
- Related to confidentiality is **cryptography** which typically protects data during transmission over an insecure channel
- Also related to confidentiality are **access control mechanisms** that typically provide a host-based defence against unauthorised access to data

Integrity

- Integrity refers to the trustworthiness of the data or resources and generally refers to preventing unauthorised modification and covers both:
 1. **Data integrity** or the information content
 2. **Origin integrity** or the source of the information

Integrity

- Integrity is maintained by blocking:
 1. Any unauthorised attempts to modify the data
 2. Any attempts to modify the data in authorised ways
- This distinction is an important one: authentication and access control mechanisms can prevent unauthorised users modifying the data but additional mechanisms are required to limit how authorised users may modify with that data

Availability

- Availability is the ability to access the desired information or use the desired resources
- Maintaining availability ensures that systems work promptly and that service is not denied to authorised users

Example

- During risk assessment assets are assigned a label of low, moderate or high under the headings of confidentiality, integrity and availability
- Student grade information in the US is an asset of **high** confidentiality and its disclosure is regulated by law
- Enrolment information might have a **moderate** confidentiality rating as university staff may require regular access to such information
- Classlist information could be assigned a **low** confidentiality rating as disclosure carries little risk

Threats

- A **threat** is a potential violation of our security objectives
- The violation need not occur but must still be guarded against
- The actions that realise a threat constitute an **attack** of which there are four broad classes:
 1. **Disclosure**: reveals data to unauthorised entity
 2. **Deception**: an authorised entity believes false data true
 3. **Disruption**: correct operation is prevented
 4. **Usurption**: system service controlled by unauthorised entity

Disclosure

- A threat to confidentiality
- **Exposure**: sensitive data is directly released to an unauthorised entity
- **Interception**: an unauthorised entity directly accesses sensitive data travelling between authorised sources and destinations
- **Inference**: an unauthorised entity indirectly accesses sensitive data through reasoning based on behavioural characteristics
- **Intrusion**: an unauthorised entity gains access to sensitive data through circumventing defences

Deception

- A threat to system or data integrity
- **Masquerade**: an unauthorised entity gains access to a system or performs a malicious act by posing as an authorised entity
- **Falsification**: the altering or replacing of valid data or the introduction of false data
- **Repudiation**: a user denies sending data or denies receiving or possessing the data

Disruption

- A threat to availability or system integrity
- **Incapacitation**: physical destruction of hardware or the disabling of system services
- **Corruption**: modification of system resources to cause them to function in an unintended manner
- **Obstruction**: interfering with system operation through disabling communication or causing excessive consumption of resources

Usurption

- A threat to system integrity
- **Misappropriation**: using system resources for unintended purposes e.g. launching a DDoS attack
- **Misuse**: causing a system component to perform some function that is detrimental to system security

Security Concepts and Relationships

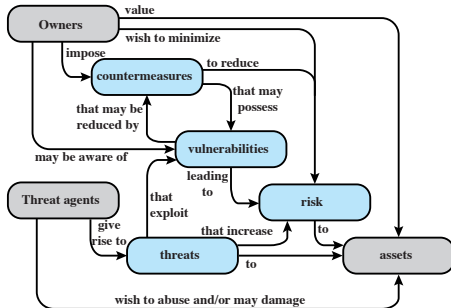


Figure 1.2 Security Concepts and Relationships

Security Requirements

- Security requirements dictate countermeasures
- *Minimum Security Requirements for Federal Information Systems* lists 17 countermeasures for protecting CIA
- Each of these areas may involve computer security or management measures or both
- **Computer security:** access control, secure communication
- **Management issues:** Security assessment, contingency planning, personnel security, awareness and training
- **Both:** Incident response
- Interestingly, the majority of countermeasures are purely managerial

Security Strategy

A comprehensive security strategy involves:

1. Policy
2. Mechanism
3. Assurance

Security Policy

- Security models and mechanisms are devised in order to satisfy a **security policy**
- A security policy is a statement of what is and what is not allowed
- A formal statement that defines the allowed/secure states and the disallowed/insecure states
- An informal textual document that describes what the users are and are not allowed to do

Security Mechanism

- A **security mechanism** is a method, tool or procedure for enforcing a security policy
- Implementing security involves putting in place mechanisms in the following areas:
 1. **Prevention**: use encryption to prevent interception
 2. **Detection**: monitor for DDoS attacks
 3. **Response**: take action to minimise attack damage
 4. **Recovery**: use backup systems to alleviate integrity risks
- Mechanisms may be non-technical e.g. requiring proof of ID before password resetting

Security Assurance

- Consumers of security mechanisms require that the chosen mechanisms enforce the security policy by correctly implementing its requirements
- Assurance is the degree of trust that can be placed in:
 - **Specification**: does the policy partition the system into secure and non-secure states?
 - **Design**: model the system, does it satisfy the specification?
Can we prove things?
 - **Implementation**: is the implementation bug free?
- **Assurance** is a degree of confidence and not a proof
- **Evaluation** is the process of determining a measure of assurance