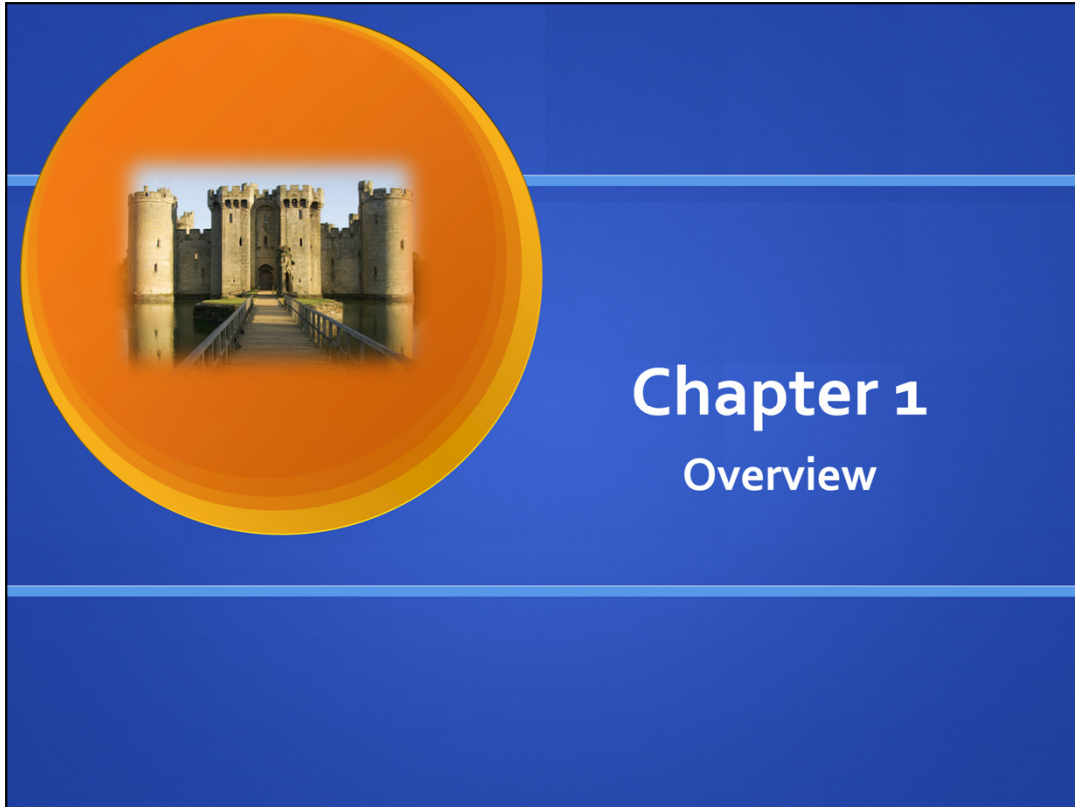


Lecture slides prepared for “Computer Security: Principles and Practice”, 2/e, by William Stallings and Lawrie Brown, Chapter 1 “Overview”.



This chapter provides an overview of computer security. We begin with a discussion of what we mean by computer security. In essence, computer security deals with computer-related assets that are subject to a variety of threats and for which various measures are taken to protect those assets. Accordingly, the next section of this chapter provides a brief overview of the categories of computer-related assets that users and system managers wish to preserve and protect, and a look at the various threats and attacks that can be made on those assets. Then, we survey the measures that can be taken to deal with such threats and attacks. This we do from three different viewpoints, in Sections 1.3 through 1.5 . We then look at some recent trends in computer security and lay out in general terms a computer security strategy.

The focus of this chapter, and indeed this book, is on three fundamental questions:

- 1. What assets do we need to protect?**
- 2. How are those assets threatened?**
- 3. What can we do to counter those threats?**

# Computer Security Overview

The NIST Computer Security Handbook defines the term Computer Security as:

“The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources” (includes hardware, software, firmware, information/data, and telecommunications).



The NIST Computer Security Handbook [NIST95] defines the term *computer security* as follows:

**Computer Security: The protection afforded to an automated information**

system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

This definition introduces three key objectives that are at the heart of computer security:

- **Confidentiality: This term covers two related concepts:**



— **Data confidentiality : 1 Assures that private or confidential information is**

not made available or disclosed to unauthorized individuals.

— **Privacy : Assures 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.

• **Integrity: This term covers two related concepts:**

— **Data integrity : Assures that information and programs are changed only**

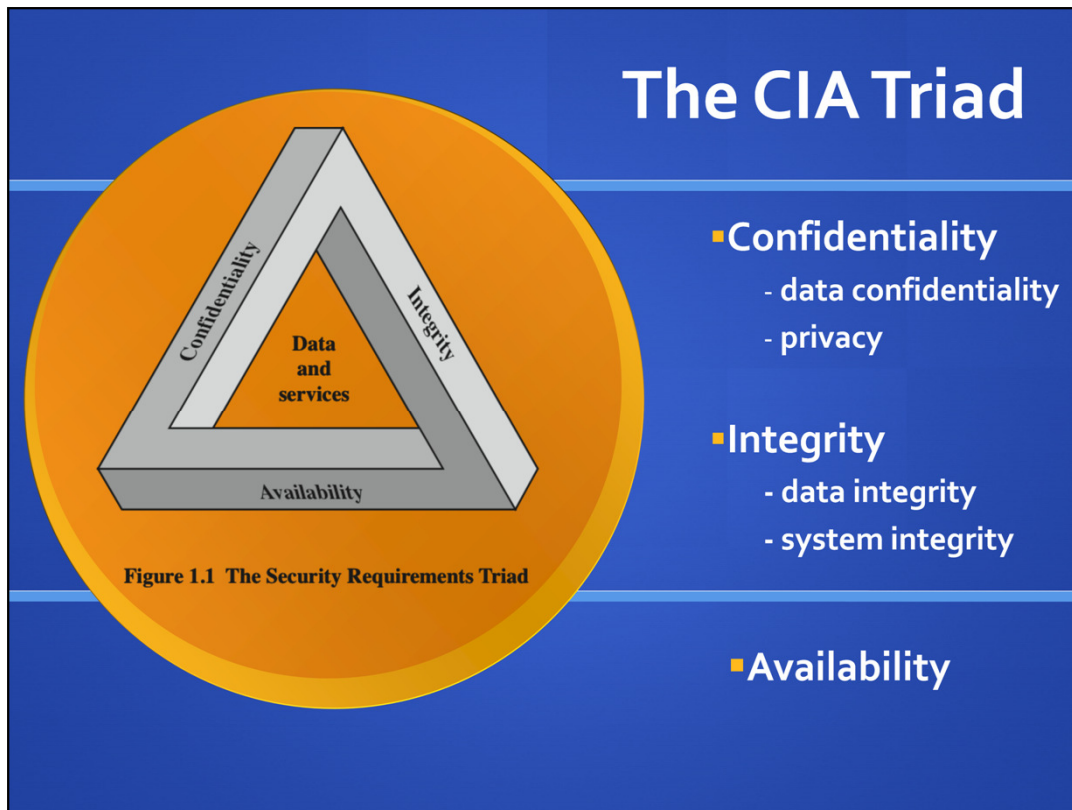
in a specified and authorized manner.

— **System integrity : Assures that a system performs its intended function in**

an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

• **Availability: Assures that systems work promptly and service is not denied to**

authorized users.



These three concepts form what is often referred to as the **CIA triad** ( Figure 1.1 ). The three concepts embody the fundamental security objectives for both data and for information and computing services.

For example, the NIST standard FIPS 199 ( *Standards for Security Categorization of Federal Information and Information Systems* ) lists confidentiality, integrity, and availability as the three security objectives for information and for information systems.

# Key Security Concepts



FIPS PUB 199

provides a useful characterization of these three objectives in terms of requirements

and the definition of a loss of security in each category:

- **Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.** A loss of confidentiality is the unauthorized disclosure of information.

- **Integrity: Guarding against improper information modification or destruction,** including ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

- **Availability: Ensuring timely and reliable access to and use of information.** A loss of availability is the disruption of access to or use of information or an information system.

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are as follows:

- **Authenticity: The property of being genuine and being able to be verified and**

trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

- **Accountability: The security goal that generates the requirement for actions**

of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems aren't yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.


Note that FIPS PUB 199 includes authenticity under integrity.

# Computer Security Challenges

- computer security is not as simple as it might first appear to the novice
- potential attacks on the security features must be considered
- procedures used to provide particular services are often counterintuitive
- physical and logical placement needs to be determined
- additional algorithms or protocols may be involved
- attackers only need to find a single weakness, the developer needs to find all weaknesses
- users and system managers tend to not see the benefits of security until a failure occurs
- security requires regular and constant monitoring
- is often an afterthought to be incorporated into a system after the design is complete
- thought of as an impediment to efficient and user-friendly operation

Computer security is both fascinating and complex. Some of the reasons follow:

1. Computer security is not as simple as it might first appear to the novice. The requirements seem to be straightforward, but the mechanisms used to meet those requirements can be quite complex and subtle.
2. In developing a particular security mechanism or algorithm, one must always consider potential attacks (often unexpected) on those security features.
3. Hence procedures used to provide particular services are often counterintuitive.
4. Having designed various security mechanisms, it is necessary to decide where to use them.
5. Security mechanisms typically involve more than a particular algorithm or protocol, but also require participants to have secret information, leading to issues of creation, distribution, and protection of that secret information.
6. Computer security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them.
7. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.
8. Security requires regular monitoring, difficult in today's short-term environment.
9. Security is still too often an afterthought - incorporated after the design is complete.
10. Many users / security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

<p><b>Adversary (threat agent)</b> An entity that attacks, or is a threat to, a system.</p> <p><b>Attack</b> An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.</p> <p><b>Countermeasure</b> An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.</p> <p><b>Risk</b> An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.</p> <p><b>Security Policy</b> A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.</p> <p><b>System Resource (Asset)</b> Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.</p> <p><b>Threat</b> A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.</p> <p><b>Vulnerability</b> A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.</p>	<p><b>Table 1.1</b></p> <p><b>Computer Security Terminology</b></p> <p><i>RFC 2828, Internet Security Glossary, May 2000</i></p> 
--	---

We now introduce some terminology that will be useful throughout the book, relying on RFC 2828, *Internet Security Glossary*. 3 Table 1.1 defines terms and Figure 1.2 [CCPS09a] shows the relationship among some of these terms.

## Figure 1.2 Security Concepts and Relationships

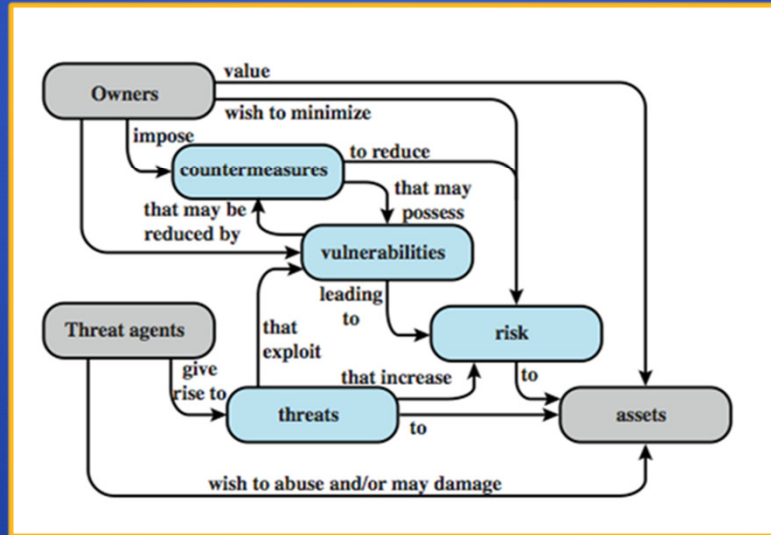


Figure 1.2 [CCPS04a] shows the relationship among some terminology that will be useful throughout the book, drawn from RFC 2828, *Internet Security Glossary*:

**Adversary (threat agent)** - An entity that attacks, or is a threat to, a system.

**Attack** -An assault on system security that derives from an intelligent threat; a deliberate attempt to evade security services and violate security policy of a system.

**Countermeasure** - An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

**Risk** - An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

**Security Policy** - A set of rules and practices that specify how a system or org provides security services to protect sensitive and critical system resources.

**System Resource (Asset)** - Data; a service provided by a system; a system capability; an item of system equipment; a facility that houses system operations and equipment.

**Threat** - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

**Vulnerability** - Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.



# Vulnerabilities, Threats and Attacks

- categories of vulnerabilities
  - corrupted (loss of integrity)
  - leaky (loss of confidentiality)
  - unavailable or very slow (loss of availability)
- threats
  - capable of exploiting vulnerabilities
  - represent potential security harm to an asset
- attacks (threats carried out)
  - passive – does not affect system resources
  - active – attempt to alter system resources or affect their operation
  - insider – initiated by an entity inside the security parameter
  - outsider – initiated from outside the perimeter



In the context of security, our concern is with the **vulnerabilities of system**

resources. [NRC02] lists the following general categories of vulnerabilities of a

computer system or network asset:

- It can be **corrupted** , so that it does the wrong thing or gives wrong answers.

For example, stored data values may differ from what they should be because

they have been improperly modified.

- It can become **leaky** . For example, someone who should not have access to

some or all of the information available through the network obtains such access.

- It can become **unavailable or very slow**. That is, using the system or network

becomes impossible or impractical.

These three general types of vulnerability correspond to the concepts of integrity, confidentiality, and availability, enumerated earlier in this section.

Corresponding to the various types of vulnerabilities to a system resource are

**threats that are capable of exploiting those vulnerabilities. A threat represents a**

potential security harm to an asset. An **attack is a threat that is carried out (threat**

action) and, if successful, leads to an undesirable violation of security, or threat

consequence. The agent carrying out the attack is referred to as an attacker, or

**threat agent . We can distinguish two types of attacks:**

- **Active attack: An attempt to alter system resources or affect their operation.**

- **Passive attack: An attempt to learn or make use of information from the**

system that does not affect system resources.

We can also classify attacks based on the origin of the attack:

- **Inside attack: Initiated by an entity inside the security perimeter (an “insider”).**

The insider is authorized to access system resources but uses them in a way not

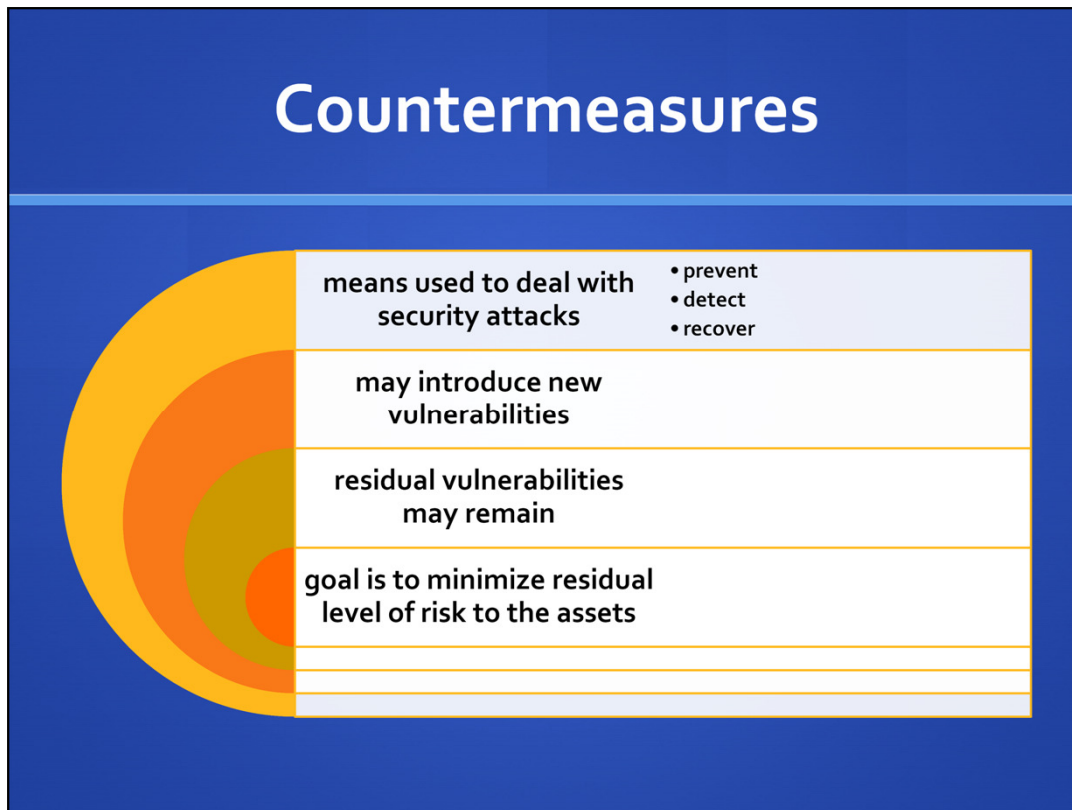
approved by those who granted the authorization.

- **Outside attack: Initiated from outside the perimeter, by an unauthorized or**

illegitimate user of the system (an “outsider”). On the Internet, potential

outside attackers range from amateur pranksters to organized criminals,  
international  
terrorists, and hostile governments.

# Countermeasures



Finally, a **countermeasure is any means taken to deal with a security attack.**

Ideally, a countermeasure can be devised to **prevent a particular type of attack from**

succeeding. When prevention is not possible, or fails in some instance, the goal is to

**detect the attack and then recover from the effects of the attack. A countermeasure**

may itself introduce new vulnerabilities. In any case, residual vulnerabilities may remain after the imposition of countermeasures. Such vulnerabilities may be

exploited by threat agents representing a residual level of **risk to the assets. Owners**

will seek to minimize that risk given other constraints.

Threat Consequence	Threat Action (attack)
<b>Unauthorized Disclosure</b> A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	<b>Exposure:</b> Sensitive data are directly released to an unauthorized entity. <b>Interception:</b> An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. <b>Inference:</b> A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. <b>Intrusion:</b> An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
<b>Deception</b> A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	<b>Masquerade:</b> An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. <b>Falsification:</b> False data deceive an authorized entity. <b>Repudiation:</b> An entity deceives another by falsely denying responsibility for an act.
<b>Disruption</b> A circumstance or event that interrupts or prevents the correct operation of system services and functions.	<b>Incapacitation:</b> Prevents or interrupts system operation by disabling a system component. <b>Corruption:</b> Undesirably alters system operation by adversely modifying system functions or data. <b>Obstruction:</b> A threat action that interrupts delivery of system services by hindering system operation.
<b>Usurpation</b> A circumstance or event that results in control of system services or functions by an unauthorized entity.	<b>Misappropriation:</b> An entity assumes unauthorized logical or physical control of a system resource. <b>Misuse:</b> Causes a system component to perform a function or service that is detrimental to system security.

Table 1.2

## Threat Consequences

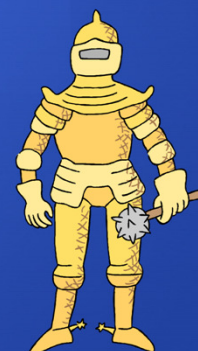


Table 1.2 , based on RFC 2828, describes four kinds of threat consequences and lists the kinds of attacks that result in each consequence.

**Unauthorized disclosure is a threat to confidentiality. The following types of attacks can result in this threat consequence:**

- **Exposure: This can be deliberate, as when an insider intentionally releases sensitive information, such as credit card numbers, to an outsider. It can also be the result of a human, hardware, or software error, which results in an entity gaining unauthorized knowledge of sensitive data. There have been numerous instances of this, such as universities accidentally posting student confidential information on the Web.**

- **Interception: Interception is a common attack in the context of communications.**

On a shared local area network (LAN), such as a wireless LAN or a broadcast Ethernet, any device attached to the LAN can receive a copy of packets intended for another device. On the Internet, a determined hacker can gain access to e-mail traffic and other data transfers. All of these situations

create the potential for unauthorized access to data.

- **Inference: An example of inference is known as traffic analysis, in which an**

adversary is able to gain information from observing the pattern of traffic on a network, such as the amount of traffic between particular pairs of hosts on

the network. Another example is the inference of detailed information from a database by a user who has only limited access; this is accomplished by repeated queries whose combined results enable inference.

- **Intrusion: An example of intrusion is an adversary gaining unauthorized**

access to sensitive data by overcoming the system's access control protections.

**Deception is a threat to either system integrity or data integrity. The following**

types of attacks can result in this threat consequence:

- **Masquerade: One example of masquerade is an attempt by an unauthorized**

user to gain access to a system by posing as an authorized user; this could happen if the unauthorized user has learned another user's logon ID and password. Another example is malicious logic, such as a Trojan horse, that appears to perform a useful or desirable function but actually gains unauthorized

access to system resources or tricks a user into executing other malicious

logic.

- **Falsification: This refers to the altering or replacing of valid data or the introduction**

of false data into a file or database. For example, a student may alter his or her grades on a school database.

- **Repudiation: In this case, a user either denies sending data or a user denies**

receiving or possessing the data.

**Disruption is a threat to availability or system integrity. The following types of**

attacks can result in this threat consequence:

- **Incapacitation: This is an attack on system availability. This could occur as a**

result of physical destruction of or damage to system hardware. More typically,

malicious software, such as Trojan horses, viruses, or worms, could operate in

such a way as to disable a system or some of its services.

- **Corruption: This is an attack on system integrity. Malicious software in this**

context could operate in such a way that system resources or services function

in an unintended manner. Or a user could gain unauthorized access to a system

and modify some of its functions. An example of the latter is a user placing backdoor logic in the system to provide subsequent access to a system and its

resources by other than the usual procedure.

**Obstruction: One way to obstruct system operation is to interfere with communications**

by disabling communication links or altering communication control information. Another way is to overload the system by placing excess burden on communication traffic or processing resources.

**Usurpation is a threat to system integrity. The following types of attacks can**

result in this threat consequence:

**• Misappropriation: This can include theft of service. An example is a distributed**

denial of service attack, when malicious software is installed on a number of hosts

to be used as platforms to launch traffic at a target host. In this case, the malicious

software makes unauthorized use of processor and operating system resources.

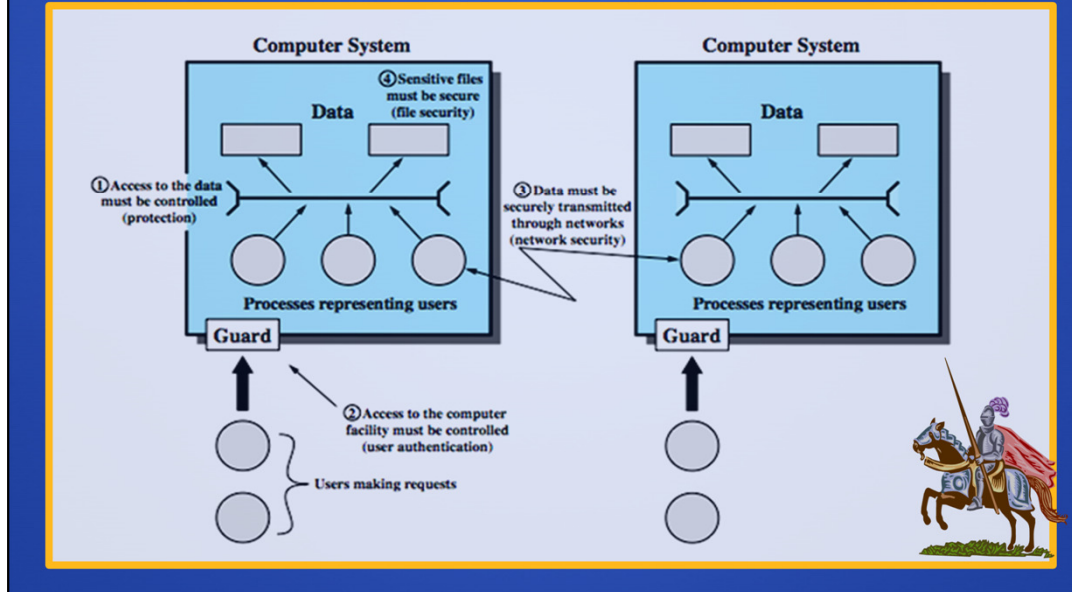
**• Misuse: Misuse can occur by means of either malicious logic or a hacker that**

has gained unauthorized access to a system. In either case, security functions

can be disabled or thwarted.



## Figure 1.3 Scope of Computer Security



The assets of a computer system can be categorized as hardware, software, data, and communication lines and networks. In this subsection, we briefly describe these four categories and relate these to the concepts of integrity, confidentiality, and availability introduced in Section 1.1 (see Figure 1.3 and Table 1.3 ).

## Table 1.3 Computer and Network Assets Examples of Threats



	Availability	Confidentiality	Integrity
<b>Hardware</b>	Equipment is stolen or disabled, thus denying service.		
<b>Software</b>	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
<b>Data</b>	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
<b>Communication Lines</b>	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Table 1.3 Computer and Network Assets, with Examples of Threats.

**HARDWARE** A major threat to computer system hardware is the threat to availability. Hardware is the most vulnerable to attack and the least susceptible to automated controls. Threats include accidental and deliberate damage to equipment as well as theft. The proliferation of personal computers and workstations and the widespread use of LANs increase the potential for losses in this area. Theft of CD-ROMs and DVDs can lead to loss of confidentiality. Physical and administrative security measures are needed to deal with these threats.

**SOFTWARE** Software includes the operating system, utilities, and application programs. A key threat to software is an attack on availability. Software, especially application software, is often easy to delete. Software can also be altered or damaged to render it useless. Careful software configuration management, which includes making backups of the most recent version of software, can maintain high availability. A more difficult problem to deal with is software modification that results in a program that still functions but that behaves differently than before, which is a threat to integrity/authenticity. Computer viruses and related attacks fall into this category. A final problem is protection against software piracy. Although certain countermeasures are available, by and large the problem of unauthorized copying of software has not been solved.

**DATA** Hardware and software security are typically concerns of computing center professionals or individual concerns of personal computer users. A much more widespread problem is data security, which involves files and other forms of data controlled by individuals, groups, and business organizations. Security concerns with respect to data are broad, encompassing availability, secrecy, and integrity. In the case of availability, the concern is with the destruction of data files, which can occur either accidentally or maliciously.

The obvious concern with secrecy is the unauthorized reading of data files or

databases, and this area has been the subject of perhaps more research and effort

than any other area of computer security. A less obvious threat to secrecy involves

the analysis of data and manifests itself in the use of so-called statistical databases,

which provide summary or aggregate information. Presumably, the existence of

aggregate information does not threaten the privacy of the individuals involved.

However, as the use of statistical databases grows, there is an increasing potential

for disclosure of personal information. In essence, characteristics of constituent

individuals may be identified through careful analysis. For example, if one table

records the aggregate of the incomes of respondents A, B, C, and D and another

records the aggregate of the incomes of A, B, C, D, and E, the difference between

the two aggregates would be the income of E. This problem is exacerbated by the


increasing desire to combine data sets. In many cases, matching several sets of data

for consistency at different levels of aggregation requires access to individual units.

Thus, the individual units, which are the subject of privacy concerns, are available at


various stages in the processing of data sets.

Finally, data integrity is a major concern in most installations. Modifications to data files can have consequences ranging from minor to disastrous.



# Passive and Active Attacks

- **Passive attacks** attempt to learn or make use of information from the system but does not affect system resources
  - eavesdropping/monitoring transmissions
  - difficult to detect
  - emphasis is on prevention rather than detection
  - two types:
    - release of message contents
    - traffic analysis
- **Active attacks** involve modification of the data stream
  - goal is to detect them and then recover
  - four categories:
    - masquerade
    - replay
    - modification of messages
    - denial of service



## **COMMUNICATION LINES AND NETWORKS**

### ***Network security attacks can be classified***

*as passive attacks and active attacks . A passive attack attempts to learn or make*

use of information from the system but does not affect system resources.

An active

attack attempts to alter system resources or affect their operation.

**Passive attacks are in the nature of eavesdropping on, or monitoring of,**

transmissions. The goal of the attacker is to obtain information that is being transmitted.

Two types of passive attacks are release of message contents and traffic analysis.

**The release of message contents is easily understood. A telephone conversation,**

an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

A second type of passive attack, **traffic analysis**, is subtler. **Suppose that we**

had a way of masking the contents of messages or other information traffic so that

opponents, even if they captured the message, could not extract the information

from the message. The common technique for masking contents is encryption. If we

had encryption protection in place, an opponent might still be able to observe the

pattern of these messages. The opponent could determine the location and identity

of communicating hosts and could observe the frequency and length of messages

being exchanged. This information might be useful in guessing the nature of the

communication that was taking place.

Passive attacks are very difficult to detect because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an

apparently normal fashion and neither the sender nor receiver is aware that a

third party has read the messages or observed the traffic pattern. However, it is

feasible to prevent the success of these attacks, usually by means of encryption.

Thus, the emphasis in dealing with passive attacks is on prevention rather than

detection.

**Active attacks involve some modification of the data stream or the**

## **creation**

of a false stream and can be subdivided into four categories: replay, masquerade, modification of messages, and denial of service.

## **Replay involves the passive capture of a data unit and its subsequent retransmission**

to produce an unauthorized effect.

## **A masquerade takes place when one entity pretends to be a different entity. A**

masquerade attack usually includes one of the other forms of active attack. For example,

authentication sequences can be captured and replayed after a valid authentication

sequence has taken place, thus enabling an authorized entity with few privileges

to obtain extra privileges by impersonating an entity that has those privileges.

## **Modification of messages simply means that some portion of a legitimate**

message is altered, or that messages are delayed or reordered, to produce an

unauthorized effect. For example, a message stating, "Allow John Smith to read

confidential file accounts" is modified to say, "Allow Fred Brown to read confidential

file accounts."

## **The denial of service prevents or inhibits the normal use or management of**

communications facilities. This attack may have a specific target; for example, an


entity may suppress all messages directed to a particular destination (e.g., the security

audit service). Another form of service denial is the disruption of an entire

network,  
either by disabling the network or by overloading it with messages so as to  
degrade  
performance.

Active attacks present the opposite characteristics of passive attacks.  
Whereas  
passive attacks are difficult to detect, measures are available to prevent  
their  
success. On the other hand, it is quite difficult to prevent active attacks  
absolutely,  
because to do so would require physical protection of all communications  
facilities  
and paths at all times. Instead, the goal is to detect them and to recover  
from any  
disruption or delays caused by them. Because the detection has a deterrent  
effect, it  
may also contribute to prevention.



<p style="text-align: center;"><b>Table 1.4</b> <b>(FIPS PUB 200)</b></p> <p style="text-align: center;"><b>R e m e m b e r s</b></p> 	
<p><b>Access control:</b> Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.</p> <p><b>Awareness and training:</b> (i) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulation, and policies related to the security of organizational information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.</p> <p><b>Audit and accountability:</b> (i) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.</p> <p><b>Certification, accreditation, and security assessments:</b> (i) Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.</p> <p><b>Configuration management:</b> (i) Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.</p> <p><b>Contingency planning:</b> Establish, maintain, and implement plans for emergency response, backup operations, and postdisaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.</p> <p><b>Identification and authentication:</b> Identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.</p> <p><b>Incident response:</b> (i) Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.</p> <p><b>Maintenance:</b> (i) Perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.</p>	<p><b>Media protection:</b> (i) Protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.</p> <p><b>Physical and environmental protection:</b> (i) Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.</p> <p><b>Planning:</b> Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.</p> <p><b>Personnel security:</b> (i) Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.</p> <p><b>Risk assessment:</b> Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.</p> <p><b>Systems and services acquisition:</b> (i) Allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.</p> <p><b>System and communications protection:</b> (i) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.</p> <p><b>System and information integrity:</b> (i) Identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.</p>

There are a number of ways of classifying and characterizing the countermeasures that may be used to reduce vulnerabilities and deal with threats to system assets. It will be useful for the presentation in the remainder of the book to look at several approaches, which we do in this and the next two sections. In this section, we view countermeasures in terms of functional requirements, and we follow the classification defined in FIPS PUB 200 (*Minimum Security Requirements for Federal Information and Information Systems*). This standard enumerates 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of information systems and the information processed, stored, and transmitted by those systems. The areas are defined in Table 1.4 .

The requirements listed in FIP PUB 200 encompass a wide range of countermeasures to security vulnerabilities and threats. Roughly, we can divide these



countermeasures into two categories: those that require computer security technical measures (covered in this book in Parts One and Two), either hardware or software, or both; and those that are fundamentally management issues (covered in Part Three).

# Security Functional Requirements

functional areas that primarily require computer security technical measures include:

- access control; identification & authentication; system & communication protection; and system & information integrity

functional areas that primarily require management controls and procedures include:

- awareness & training; audit & accountability; certification, accreditation, & security assessments; contingency planning; maintenance; physical & environmental protection; planning; personnel security; risk assessment; and systems & services acquisition

functional areas that overlap computer security technical measures and management controls include:

- configuration management; incident response; and media protection

Each of the functional areas may involve both computer security technical measures and management measures. Functional areas that primarily require

computer security technical measures include access control, identification and

authentication, system and communication protection, and system and information

integrity. Functional areas that primarily involve management controls and procedures

include awareness and training; audit and accountability; certification, accreditation,

and security assessments; contingency planning; maintenance; physical and

environmental protection; planning; personnel security; risk assessment; and systems


and services acquisition. Functional areas that overlap computer security technical

measures and management controls include configuration management, incident

response, and media protection.

Note that the majority of the functional requirements areas in FIP PUB 200 are either primarily issues of management or at least have a significant management component, as opposed to purely software or hardware solutions. This may be new to some readers and is not reflected in many of the books on computer and information security. But as one computer security expert observed, “If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology” [SCHN00]. This book reflects the need to combine technical and managerial approaches to achieve effective computer security.

FIPS PUB 200 provides a useful summary of the principal areas of concern, both technical and managerial, with respect to computer security. This book attempts to cover all of these areas.



## Security Architecture For Open Systems

- ITU-T Recommendation X.800, *Security Architecture for OSI*
  - systematic way of defining the requirements for security and characterizing the approaches to satisfying them
  - was developed as an international standard
  - focuses on:
    - security attacks – action that compromises the security of information owned by an organization
    - security mechanism – designed to detect, prevent, or recover from a security attack
    - security service – intended to counter security attacks

ITU-T Recommendation X.800, *Security Architecture for OSI*, defines a systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. The OSI security architecture is useful to managers as a way of organizing the task of providing security. The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as:

- **Security attack:** Any action that compromises the security of information owned by an organization. cf. network security attacks slide earlier
- **Security mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack. cf. functional requirements from previous slide or Table 1.6 in text.
- **Security service:** A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service. cf CIA security concepts earlier, or Table 1.5 in text.

# Security Services


## X.800

- defines a security service as a service that is provided by a protocol layer of communicating open systems and ensures adequate security of the systems or of data transfers

## RFC 2828

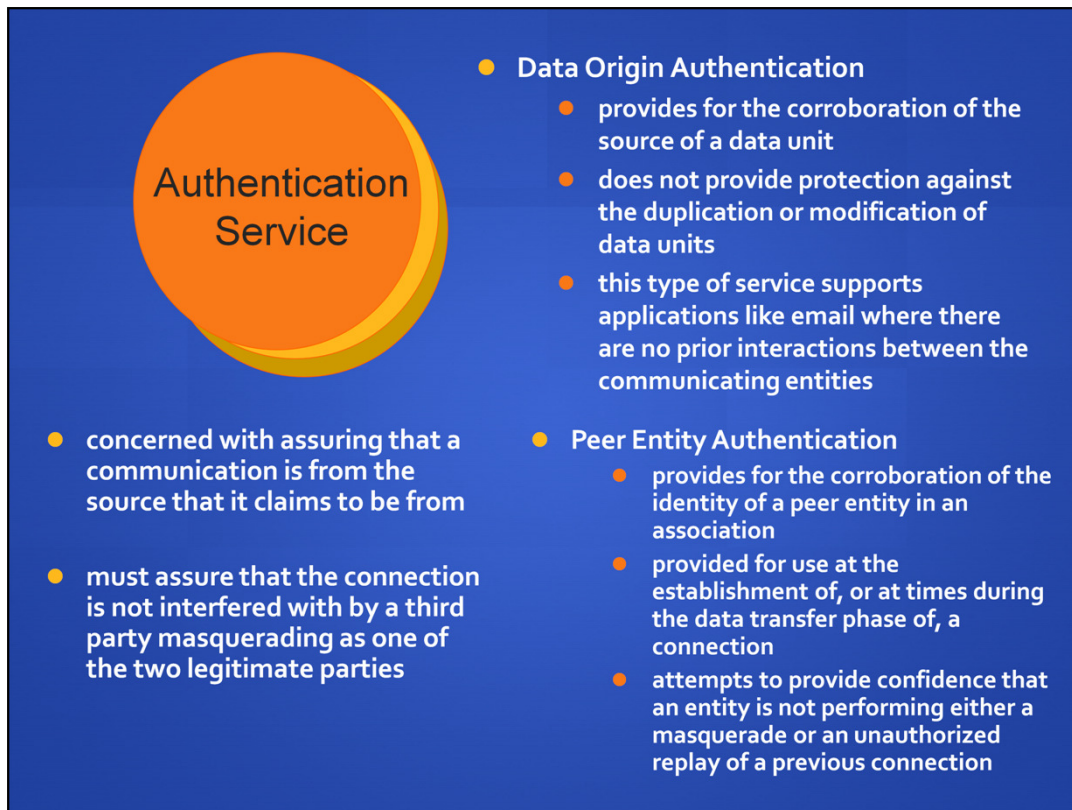
- defines a security service as a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms

X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers. Perhaps a clearer definition is found in RFC 2828, which provides the following definition: a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.

<p><b>Table 1.5</b></p> <p><b>Security Services</b></p> 	<p><b>AUTHENTICATION</b></p> <p>The assurance that the communicating entity is the one that it claims to be.</p> <p><b>Peer Entity Authentication</b> Used in association with a logical connection to provide confidence in the identity of the entities connected.</p> <p><b>Data-Origin Authentication</b> In a connectionless transfer, provides assurance that the source of received data is as claimed.</p> <p><b>ACCESS CONTROL</b></p> <p>The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).</p> <p><b>DATA CONFIDENTIALITY</b></p> <p>The protection of data from unauthorized disclosure.</p> <p><b>Connection Confidentiality</b> The protection of all user data on a connection.</p> <p><b>Connectionless Confidentiality</b> The protection of all user data in a single data block.</p> <p><b>Selective-Field Confidentiality</b> The confidentiality of selected fields within the user data on a connection or in a single data block.</p> <p><b>Traffic-Flow Confidentiality</b> The protection of the information that might be derived from observation of traffic flows.</p> <p><b>AVAILABILITY</b></p> <p>Ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network. Disaster recovery solutions are included in this category.</p>	<p><b>DATA INTEGRITY</b></p> <p>The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).</p> <p><b>Connection Integrity with Recovery</b> Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.</p> <p><b>Connection Integrity without Recovery</b> As above, but provides only detection without recovery.</p> <p><b>Selective-Field Connection Integrity</b> Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.</p> <p><b>Connectionless Integrity</b> Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.</p> <p><b>Selective-Field Connectionless Integrity</b> Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.</p> <p><b>NONREPUDIATION</b></p> <p>Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.</p> <p><b>Nonrepudiation, Origin</b> Proof that the message was sent by the specified party.</p> <p><b>Nonrepudiation, Destination</b> Proof that the message was received by the specified party.</p>
	<p><i>Source: From X.800, Security Architecture for OSI</i></p>	

X.800 divides these services into 6 categories and 14 specific services ( Table 1.5 ). We look at each category in turn. 5 Keep in mind that to a considerable extent, X.800 is focused on distributed and networked systems and so emphasizes network security over single-system computer security. Nevertheless, Table 1.5 is a useful checklist of security services.





## ***AUTHENTICATION***

***The authentication service is concerned with assuring that a*** communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be. Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

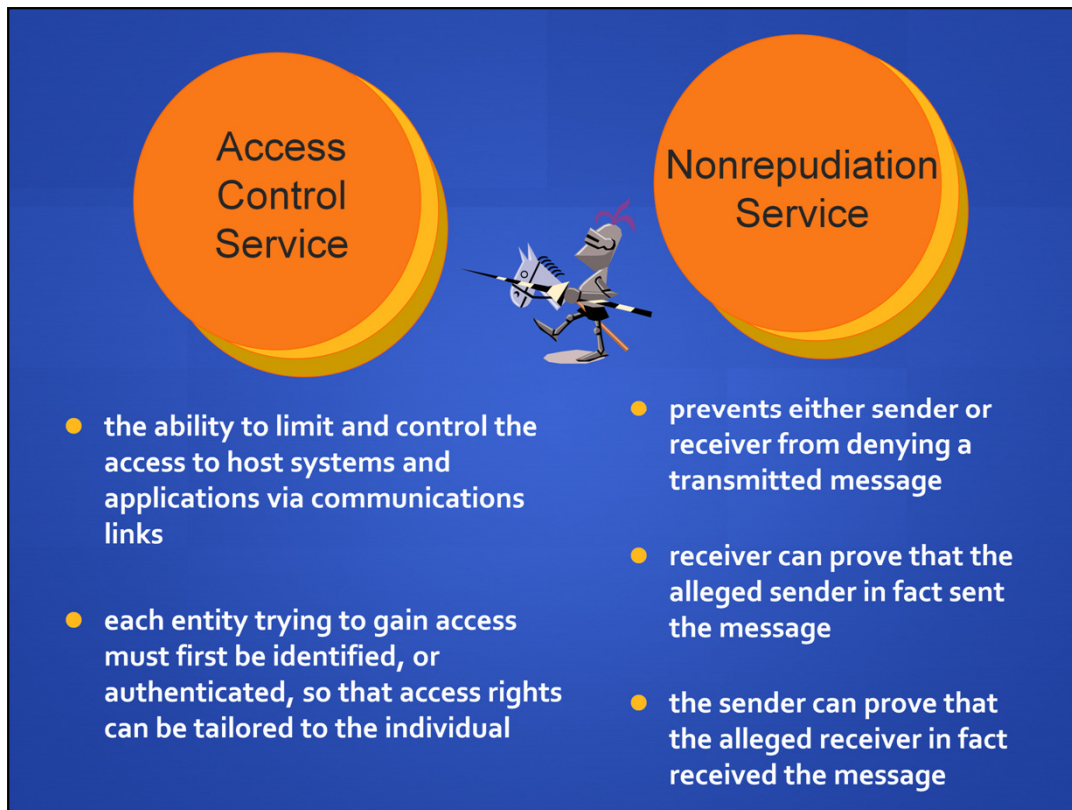
Two specific authentication services are defined in the standard:

- **Peer entity authentication: Provides for the corroboration of the identity** of a peer entity in an association. Two entities are considered peer if they implement the same protocol in different systems (e.g., two TCP users in two communicating systems). Peer entity authentication is provided for use at the establishment of, or at times during the data transfer phase of, a connection. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.

- **Data origin authentication: Provides for the corroboration of the source**

of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail where there are no prior interactions between the communicating entities.





***ACCESS CONTROL*** In the context of network security, access control is the ability

to limit and control the access to host systems and applications via communications

links. To achieve this, each entity trying to gain access must first be identified, or

authenticated, so that access rights can be tailored to the individual.

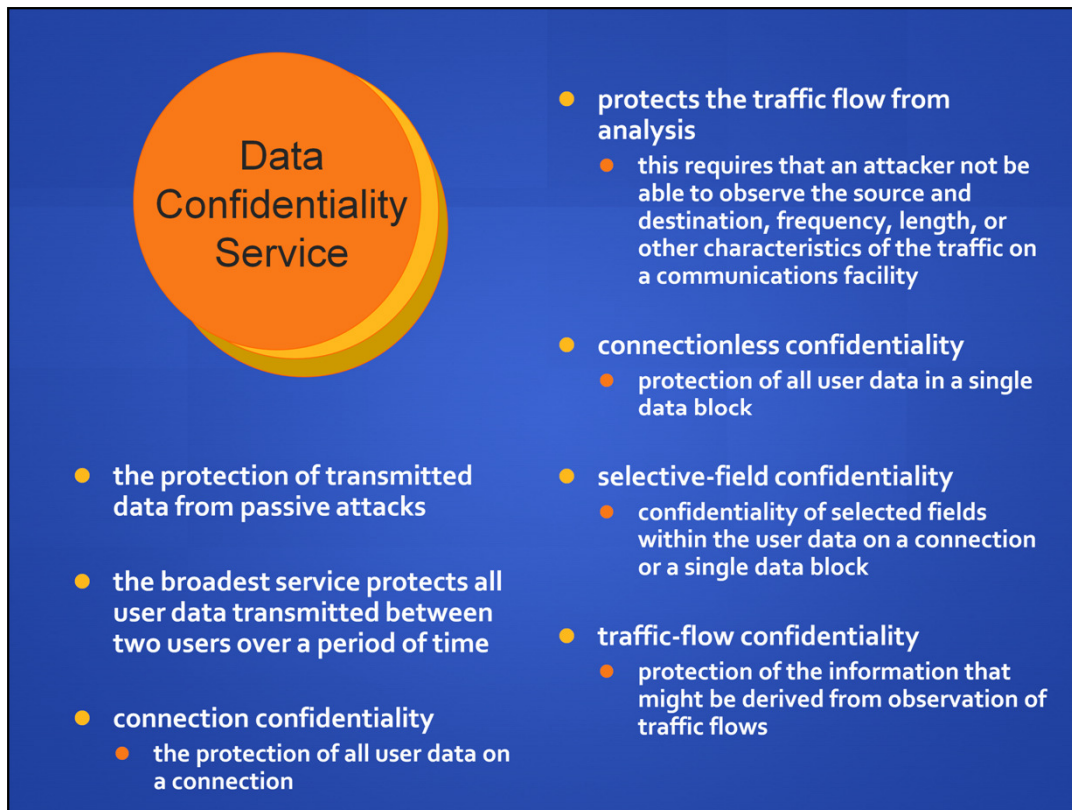
***NONREPUDIATION*** prevents either sender or receiver from

denying a transmitted message. Thus, when a message is sent, the receiver can

prove that the alleged sender in fact sent the message. Similarly, when a message

is received, the sender can prove that the alleged receiver in fact received the

message.

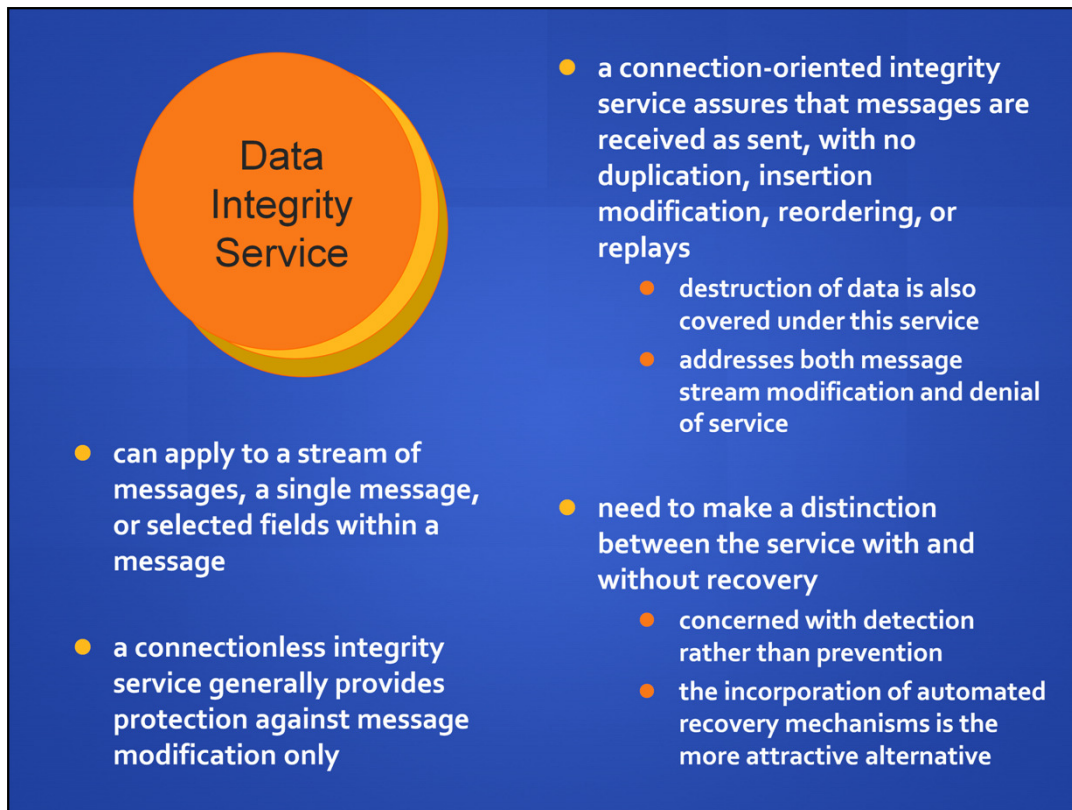


## ***DATA CONFIDENTIALITY***

### ***In the context of network security, confidentiality***

is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. For example, when a TCP connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection. Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message. These refinements are less useful than the broad approach and may even be more complex and expensive to implement.

The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.



## **DATA INTEGRITY**

### ***In the context of network security, as with data confidentiality,***

data integrity can apply to a stream of messages, a single message, or selected fields within a message. Again, the most useful and straightforward approach is total stream protection.

A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service. Thus, the connection-oriented integrity service addresses both message stream modification and denial of service. On the other hand, a connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only.

We need to make a distinction between the service with and without recovery. Because the integrity service relates to active attacks, we are concerned with detection rather than prevention. If a violation of integrity is detected, then the service may simply report this violation, and some other portion of software or human intervention is required to recover from the violation. Alternatively, there are mechanisms available to recover from the loss of integrity of data, as we will review subsequently. The incorporation of automated recovery mechanisms is, in general, the more attractive alternative.




## **AVAILABILITY**

### ***Both X.800 and RFC 2828 define availability to be the property***

of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them). A variety of attacks can result in the loss of or reduction in availability. Some of these attacks are amenable to automated countermeasures, such as authentication and encryption, whereas others require a physical action to prevent or recover from loss of availability.

X.800 treats availability as a property to be associated with various security services. X.805, *Security Architecture for Systems Providing End-to-End Communications*, refers specifically to an availability service. An availability service is one that protects a system to ensure its availability. This service addresses the security concerns raised by denial-of-service attacks. It depends on proper management and control of system resources and thus depends on access control service and other security services.



SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
<p>May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.</p> <p><b>Encipherment</b> The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.</p> <p><b>Digital Signature</b> Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).</p> <p><b>Access Control</b> A variety of mechanisms that enforce access rights to resources.</p> <p><b>Data Integrity</b> A variety of mechanisms used to assure the integrity of a data unit or stream of data units.</p> <p><b>Authentication Exchange</b> A mechanism intended to ensure the identity of an entity by means of information exchange.</p> <p><b>Traffic Padding</b> The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.</p> <p><b>Routing Control</b> Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.</p> <p><b>Notarization</b> The use of a trusted third party to assure certain properties of a data exchange.</p>	<p>Mechanisms that are not specific to any particular OSI security service or protocol layer.</p> <p><b>Trusted Functionality</b> That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).</p> <p><b>Security Label</b> The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.</p> <p><b>Event Detection</b> Detection of security-relevant events.</p> <p><b>Security Audit Trail</b> Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.</p> <p><b>Security Recovery</b> Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.</p> 

**Table 1.6**  
**X.800**  
**Security**  
**Mechanisms**

## Security Mechanisms

Table 1.6 lists the security mechanisms defined in X.800. The mechanisms are

divided into those that are implemented in a specific protocol layer, such as TCP

or an application-layer protocol, and those that are not specific to any particular

protocol layer or security service. These mechanisms will be covered in the appropriate

places in the book and so we do not elaborate now, except to comment on the

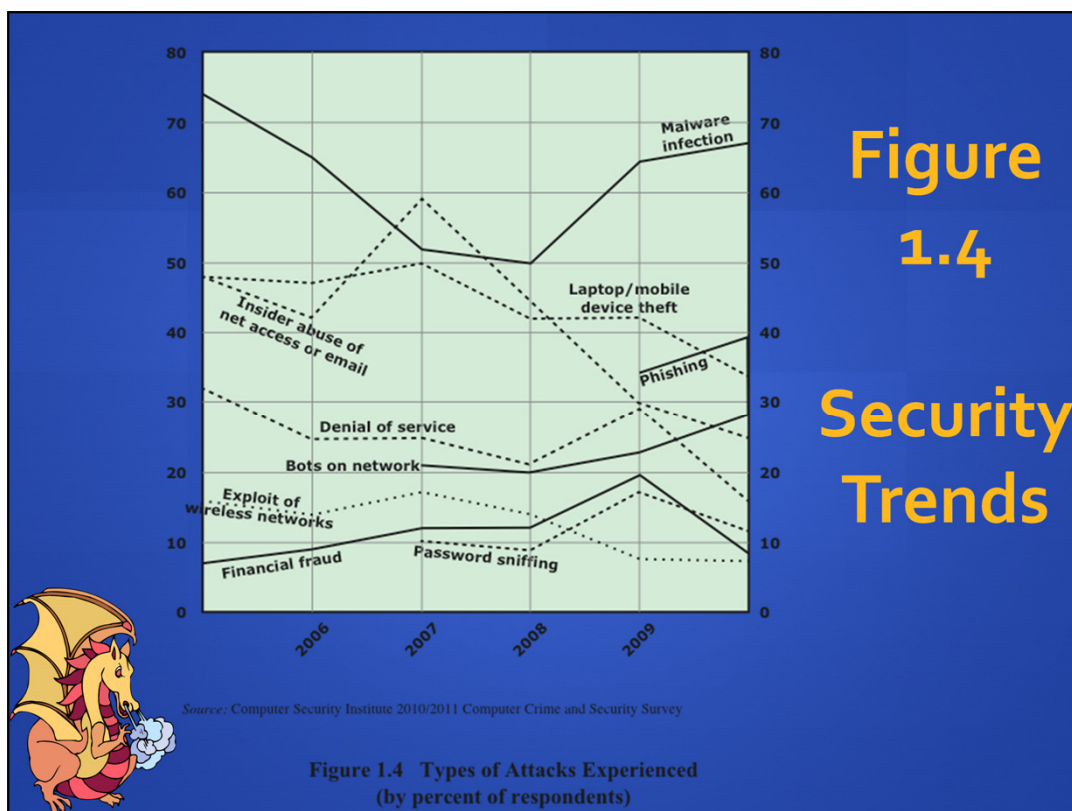
definition of encipherment. X.800 distinguishes between reversible encipherment

mechanisms and irreversible encipherment mechanisms. A reversible encipherment

mechanism is an encryption algorithm that allows data to be encrypted and subsequently

decrypted. Irreversible encipherment mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message

authentication applications.



In order to assess the relative severity of various threats and the relative importance of various approaches to computer security, it is useful to look at the experience of organizations. A useful view is provided by the CSI Computer Crime and Security Survey for 2010/2011, conducted by the Computer Security Institute. The respondents consisted of over 350 U.S.-based companies, nonprofit organizations, and public sector organizations.

Figure 1.4 shows the types of attacks experienced by respondents in nine major categories. Most noteworthy is the large and growing prevalence of malicious software (malware) attacks. It is also worth noting that most categories of attack exhibit a somewhat downward trend. The CSI report speculates that this is due in large part to improved security techniques by organizations.

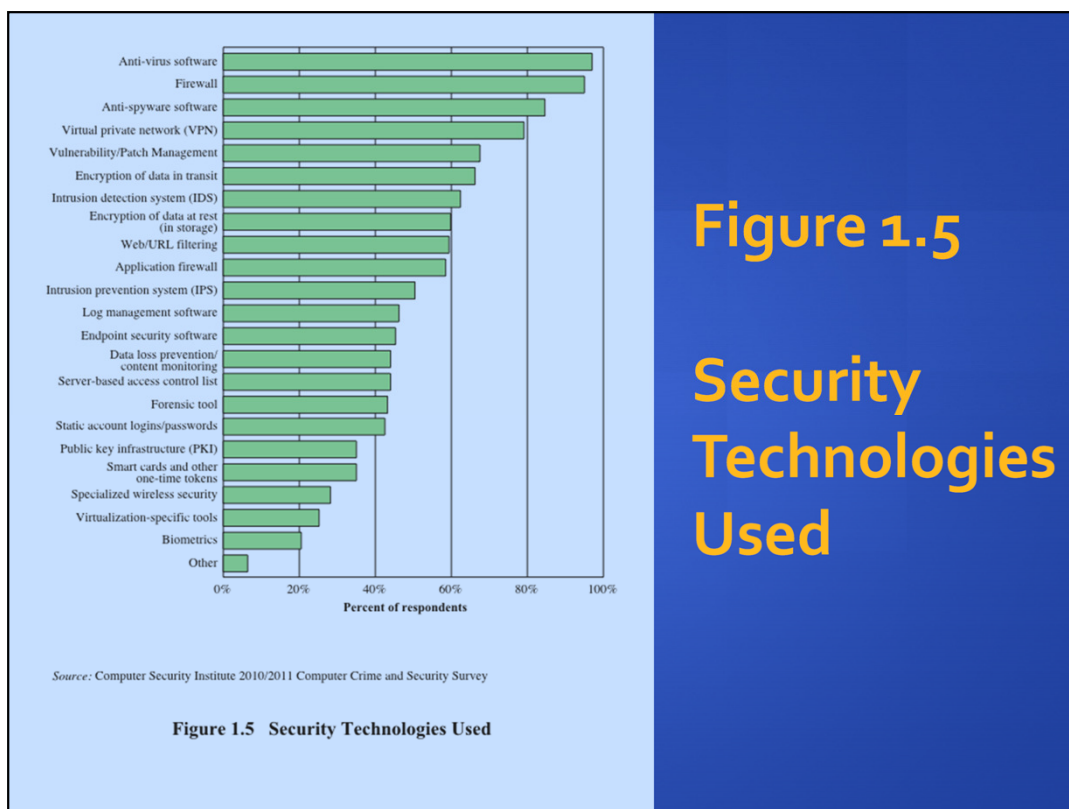


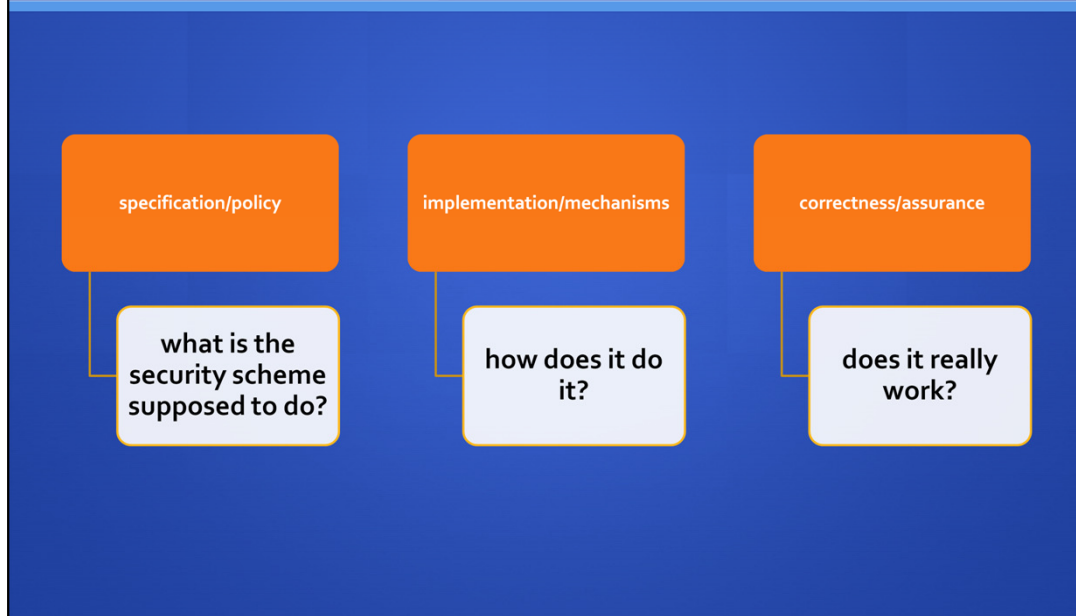
Figure 1.5 indicates the types of security technology used by organizations to counter threats. Both firewalls and antivirus software are used almost universally.

This popularity reflects a number of factors:

- The maturity of these technologies means that security administrators are very familiar with the products and are confident of their effectiveness.
- Because these technologies are mature and there are a number of vendors, costs tend to be quite reasonable and user-friendly interfaces are available.
- The threats countered by these technologies are among the most significant facing security administrators.



# Computer Security Strategy



We conclude this chapter with a brief look at the overall strategy for providing computer security. [LAMP04] suggests that a comprehensive security strategy involves three aspects:

- **Specification/policy: What is the security scheme supposed to do?**
- **Implementation/mechanisms: How does it do it?**
- **Correctness/assurance: Does it really work?**



# Security Policy

- formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources
- factors to consider:
  - value of the assets being protected
  - vulnerabilities of the system
  - potential threats and the likelihood of attacks
- trade-offs to consider:
  - ease of use versus security
  - cost of security versus cost of failure and recovery



The first step in devising security services and mechanisms is to develop a security policy. Those involved with computer security use the term *security policy* in various ways. At the least, a security policy is an informal description of desired system behavior [NRC91]. Such informal policies may reference requirements for security, integrity, and availability. More usefully, a security policy is a formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources (RFC 2828). Such a formal security policy lends itself to being enforced by the system's technical controls as well as its management and operational controls. In developing a security policy, a security manager needs to consider the following factors:

- The value of the assets being protected
- The vulnerabilities of the system
- Potential threats and the likelihood of attacks

Further, the manager must consider the following trade-offs:

- **Ease of use versus security: Virtually all security measures involve some penalty** in the area of ease of use. The following are some examples. Access control mechanisms require users to remember passwords and perhaps perform other access control actions. Firewalls and other network security measures may reduce available transmission capacity or slow response time. Virus-checking software reduces available processing power and introduces the possibility of system crashes or malfunctions due to improper interaction between the security software and the operating system.
- **Cost of security versus cost of failure and recovery: In addition to ease of use** and performance costs, there are direct monetary costs in implementing and maintaining security measures. All of these costs must be balanced against the cost of security failure and recovery if certain security measures are lacking. The cost of security failure and recovery must take into account not only the value of the assets being protected and the damages resulting from a security violation, but also the risk, which is the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Security policy is thus a business decision, possibly influenced by legal requirements.



Security implementation involves four complementary courses of action:

• **Prevention: An ideal security scheme is one in which no attack is successful.**

Although this is not practical in all cases, there is a wide range of threats in which prevention is a reasonable goal. For example, consider the transmission of encrypted data. If a secure encryption algorithm is used, and if measures are in place to prevent unauthorized access to encryption keys, then attacks on confidentiality of the transmitted data will be prevented.

• **Detection: In a number of cases, absolute protection is not feasible, but it is**

practical to detect security attacks. For example, there are intrusion detection systems designed to detect the presence of unauthorized individuals logged onto a system. Another example is detection of a denial of service attack, in which communications or processing resources are consumed so that they are unavailable to legitimate users.

• **Response: If security mechanisms detect an ongoing attack, such as a denial of**

service attack, the system may be able to respond in such a way as to halt the attack and prevent further damage.

• **Recovery:** An example of recovery is the use of backup systems, so that if data

integrity is compromised, a prior, correct copy of the data can be reloaded.

# Assurance and Evaluation

- **assurance**
  - the *degree* of confidence one has that the security measures work as intended to protect the system and the information it processes
  - encompasses both system design and system implementation
- **evaluation**
  - process of examining a computer product or system with respect to certain criteria
  - involves testing and formal analytic or mathematical techniques

Those who are “consumers” of computer security services and mechanisms (e.g., system managers, vendors, customers, and end users) desire a belief that the security measures in place work as intended. That is, security consumers want to feel that the security infrastructure of their systems meet security requirements and enforce security policies. These considerations bring us to the concepts of assurance and evaluation.

The NIST Computer Security Handbook [NIST95] defines **assurance as the** degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes. This encompasses both system design and system implementation. Thus, assurance deals with the questions, “Does the security system design meet its requirements?” and “Does the security system implementation meet its specifications?”

Note that assurance is expressed as a degree of confidence, not in terms of a formal proof that a design or implementation is correct. With the present state of the art, it is very difficult if not impossible to move beyond a degree of confidence to absolute proof. Much work has been done in developing formal models that define requirements and characterize designs and implementations, together with logical and mathematical techniques for addressing these issues. But assurance is still a matter of degree.

**Evaluation is the process of examining a computer product or system with respect to certain criteria.** Evaluation involves testing and may also involve formal analytic or mathematical techniques. The central thrust of work in this area is

the development of evaluation criteria that can be applied to any security system (encompassing security services and mechanisms) and that are broadly supported for making product comparisons.



# Summary

- security concepts
  - CIA triad
    - confidentiality – preserving the disclosure of information
    - integrity – guarding against modification or destruction of information
    - availability – ensuring timely and reliable access to information
  - terminology – table 1.1
    - threats – exploits vulnerabilities
    - attack – a threat carried out
    - countermeasure – means to deal with a security attack
    - assets – hardware, software, data, communication lines, networks
- security architecture
  - security services – enhances the security of systems and information transfers, table 1.5
  - security mechanisms – mechanisms designed to detect, prevent, or recover from a security attack, table 1.6
  - security attack – any action that compromises the security of information owned by an organization
- security trends
  - figure 1.4
- security strategy
  - policy, implementation, assurance and evaluation
- functional requirements
  - table 1.4



Chapter 1 summary.