



Cryptography and Network Security

Sixth Edition
by William Stallings



Chapter 1

Overview

“The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter. Consequently, it is not easy to find a fixed point of departure.”

— On War,

Carl Von Clausewitz

Cryptographic algorithms and protocols can be grouped into four main areas:

Symmetric encryption

- Used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords

Asymmetric encryption

- Used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures

Data integrity algorithms

- Used to protect blocks of data, such as messages, from alteration

Authentication protocols

- Schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities

The field of network and Internet security consists of:



measures to deter,
prevent, detect, and
correct security
violations that involve
the transmission of
information

Computer Security

- 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)

Computer Security Objectives

Confidentiality

- Data confidentiality
 - 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

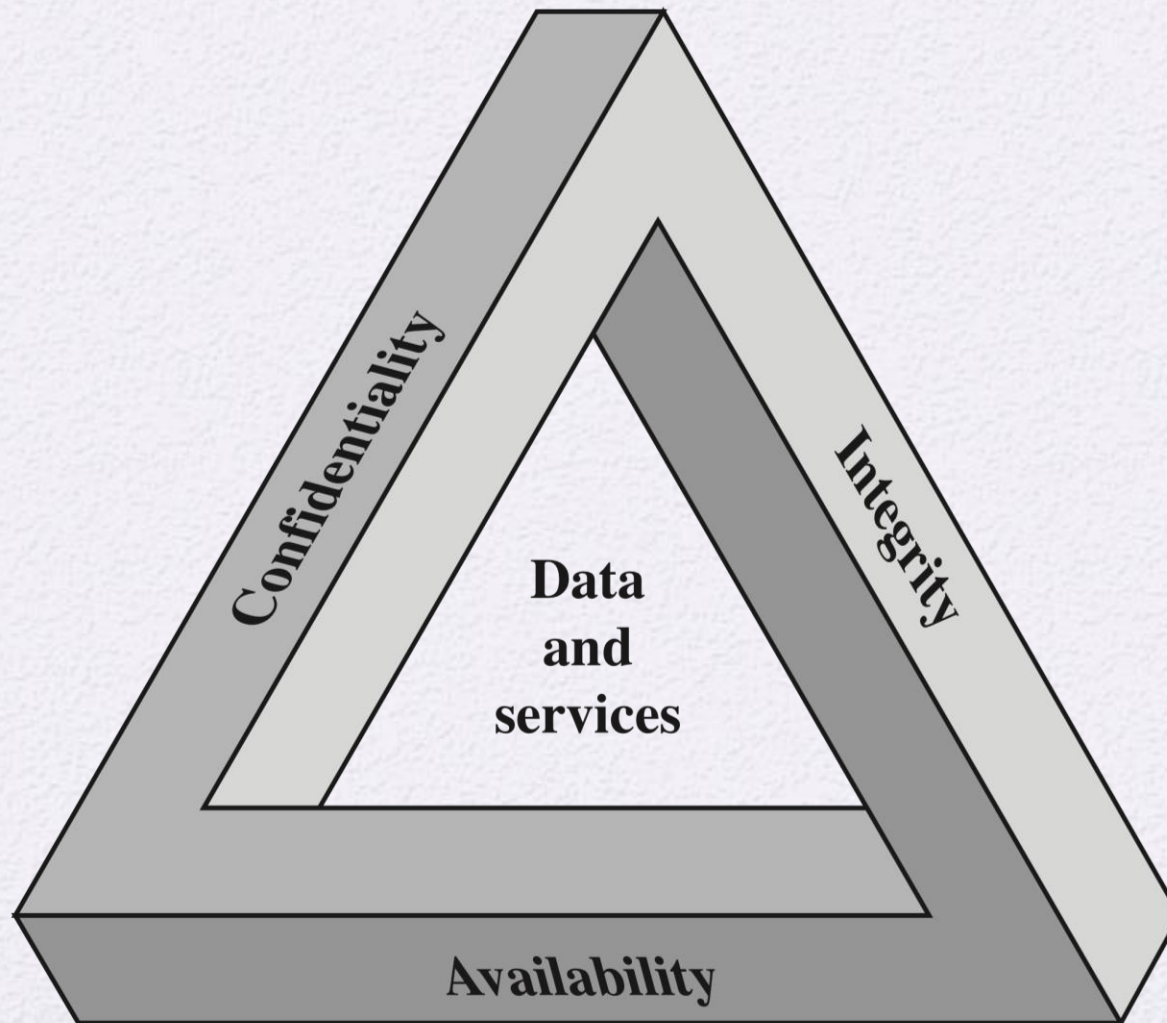
Integrity

- 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

CIA Triad



- • 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 nonrepudiation 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

Possible additional concepts:

Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

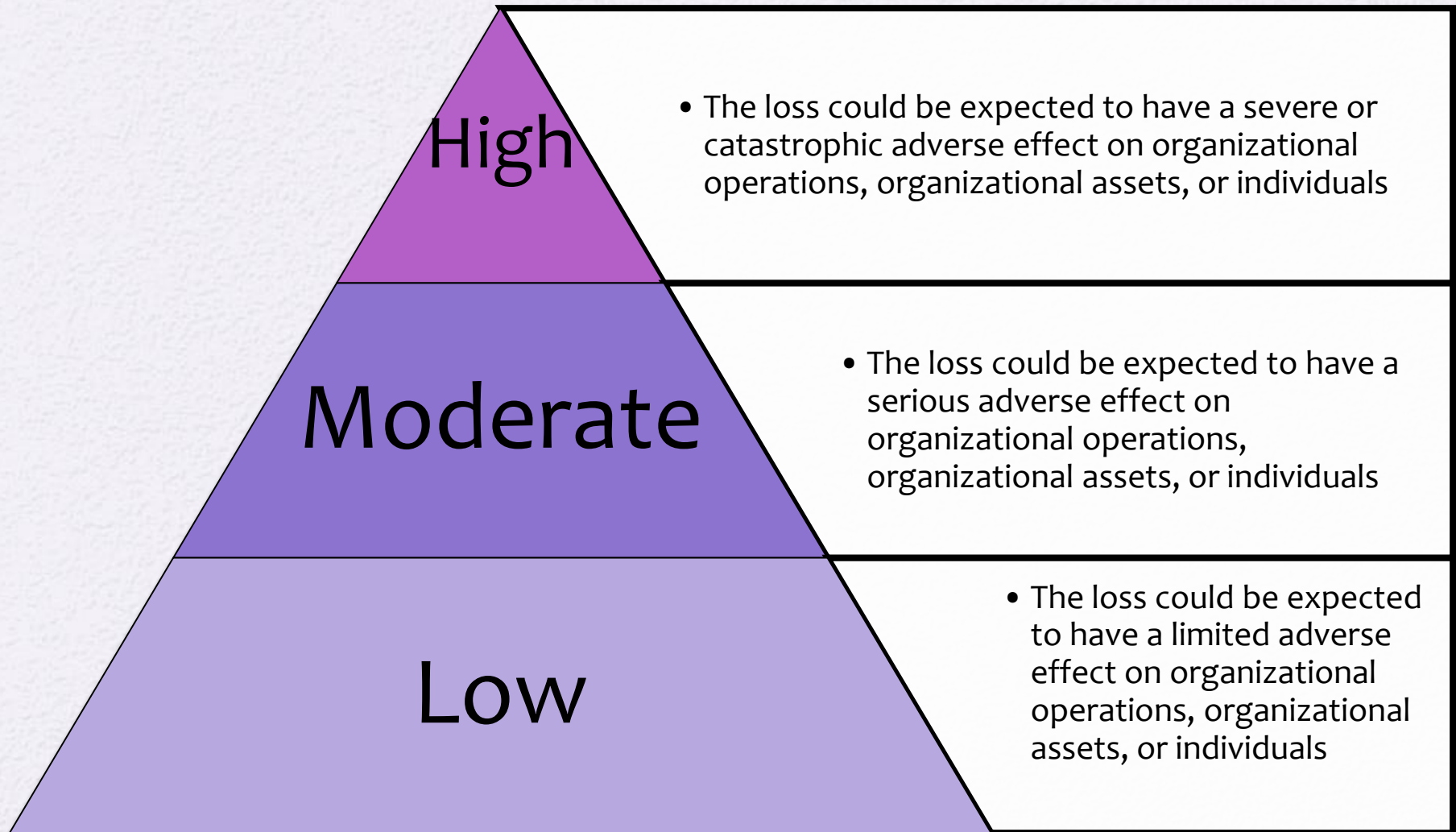
Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

- **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 afteraction recovery and legal action. Because truly secure systems are not 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.

Breach of Security Levels of Impact



Computer Security Challenges

- Security is not simple
- Potential attacks on the security features need to be considered
- Procedures used to provide particular services are often counter-intuitive
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Is too often an afterthought
- Security mechanisms typically involve more than a particular algorithm or protocol
- Security is essentially a battle of wits between a perpetrator and the designer
- Little benefit from security investment is perceived until a security failure occurs
- Strong security is often viewed as an impediment to efficient and user-friendly operation

The Challenges of Computer Security

- Computer and network security is both fascinating and complex. Some of the reasons follow:
- 1. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, nonrepudiation, or integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.

- 2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.
- 3. Because of point 2, the procedures used to provide particular services are often counterintuitive. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.

- 4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense (e.g., at what layer or layers of an architecture such as TCP/IP [Transmission Control Protocol/Internet Protocol] should mechanisms be placed).

- 5. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.

- 6. Computer and network 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. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

- 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, even constant, monitoring, and this is difficult in today's short-term, overloaded environment.
- 9. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.

- 10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.
- The difficulties just enumerated will be encountered in numerous ways as we examine the various security threats and mechanisms throughout this book.

The Open System Interconnect(OSI)

- To assess effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. This is difficult enough in a centralized data processing environment; with the use of local and wide area networks, the problems are compounded.

OSI Security Architecture

- Security attack
 - Any action that compromises the security of information owned by an organization
- Security mechanism
 - A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack
- Security service
 - A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization
 - Intended to counter security attacks, and they make use of one or more security mechanisms to provide the service

Table 1.1

Threats and Attacks (RFC 4949)



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. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

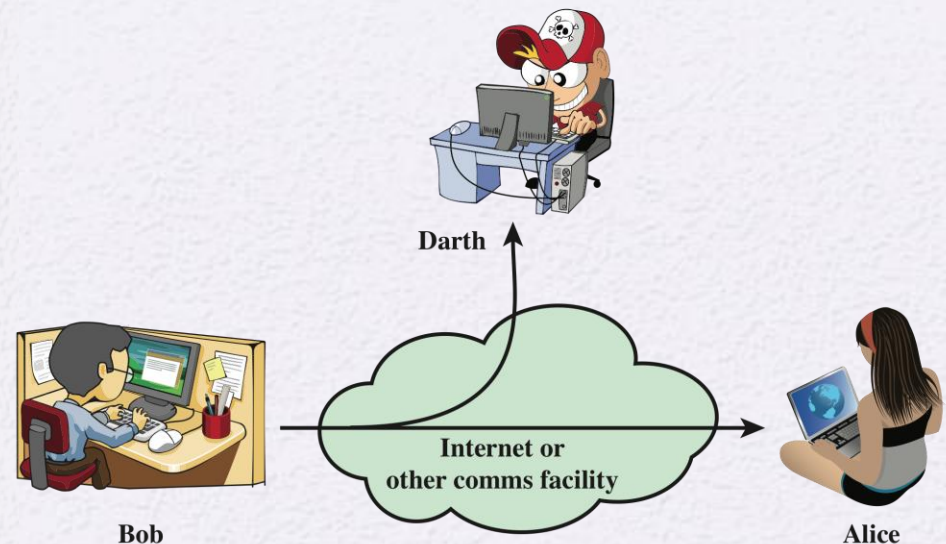
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Security Attacks

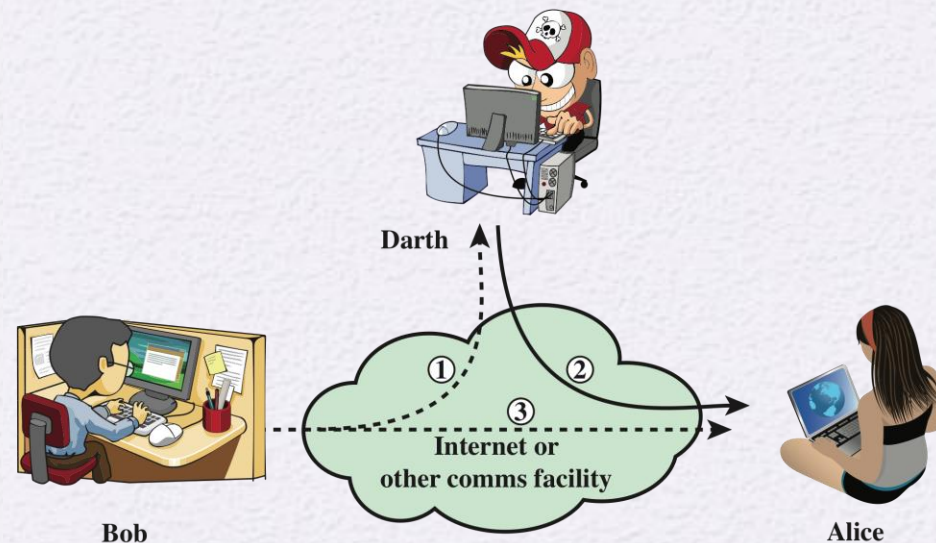
- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*

- 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



(a) Passive attacks



(b) Active attacks

Figure 1.1 Security Attacks

Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions
- Goal of the opponent is to obtain information that is being transmitted



- Two types of passive attacks are:
 - The release of message contents
 - 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.

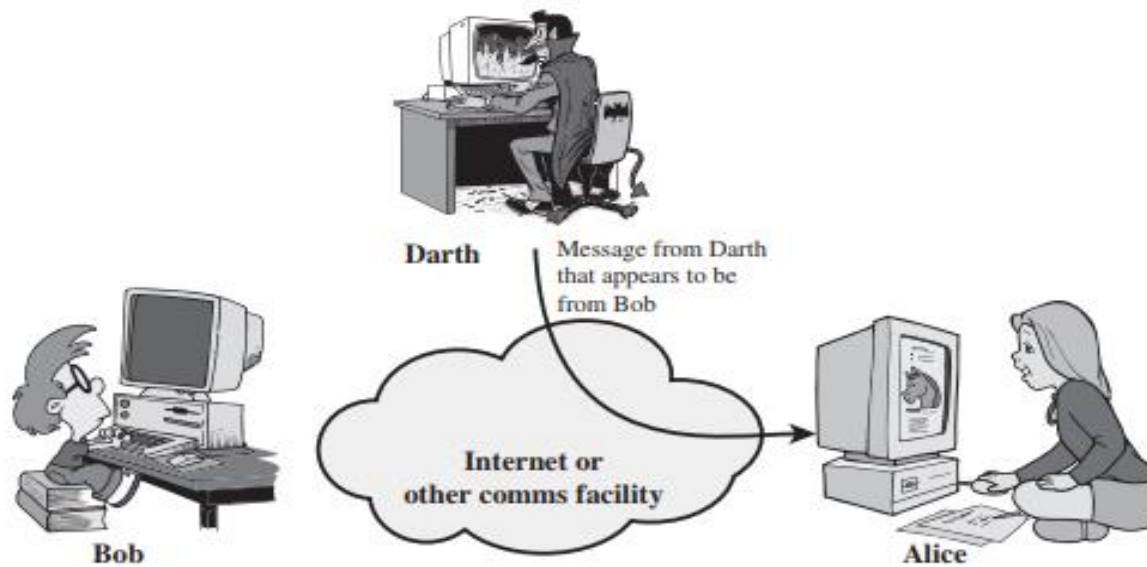
- A second type of passive attack, traffic analysis, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message.

- 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.

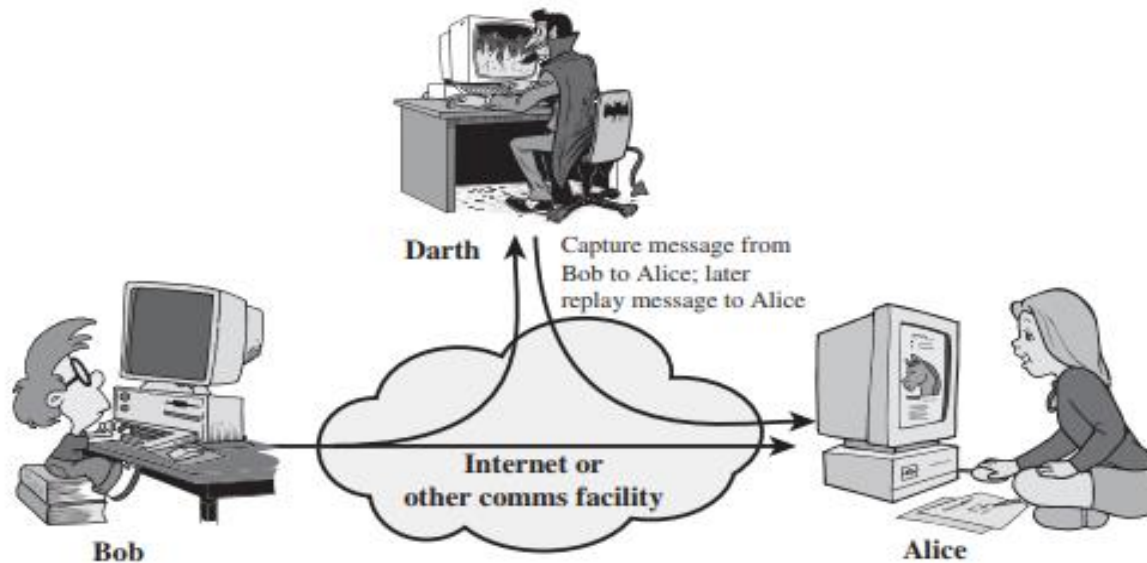
- Passive attacks are very difficult to detect, because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. 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

- Active attacks (Figure 1.1b) involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

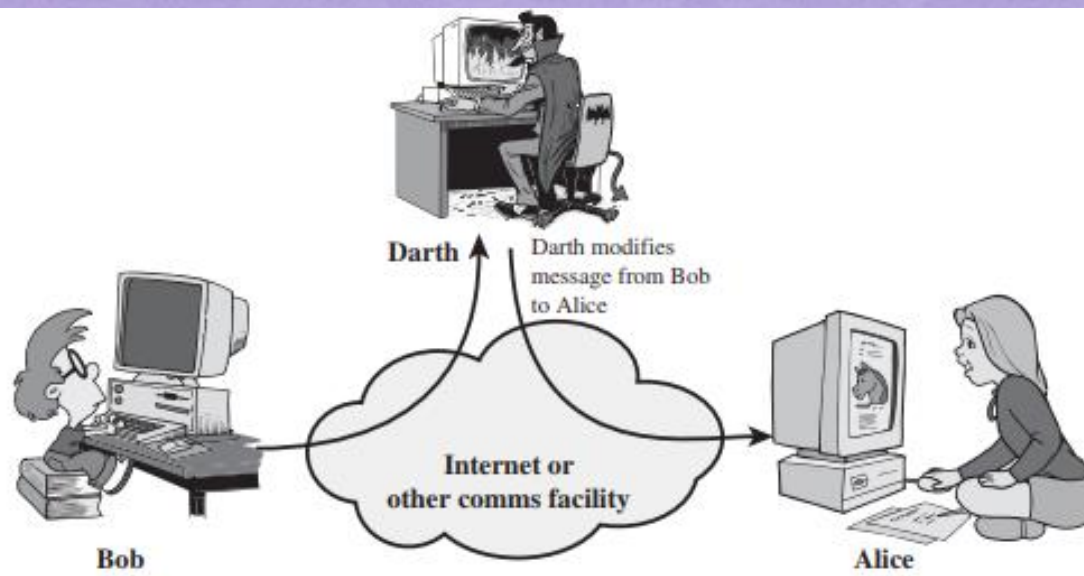


(a) Masquerade

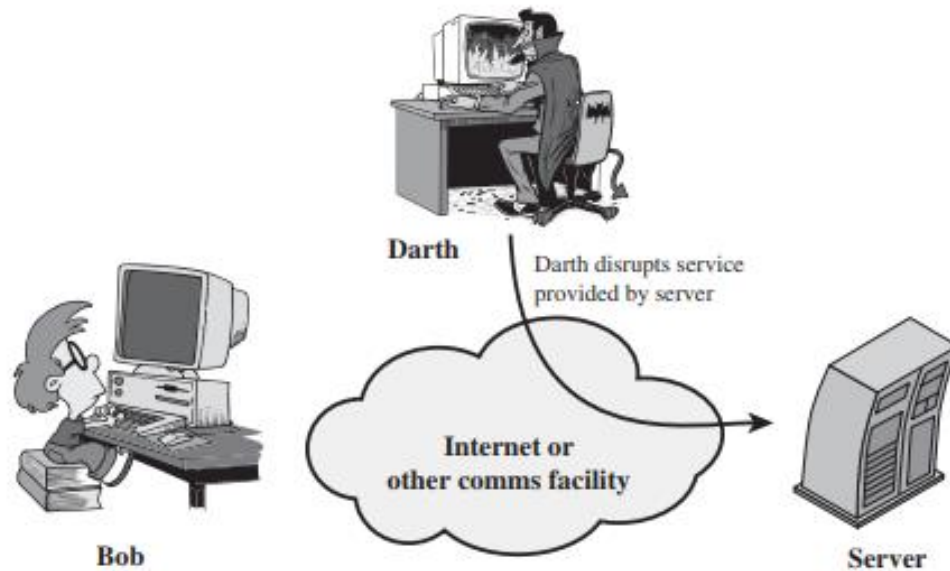


(b) Replay

Figure 1.3 Active attacks (Continued)



(c) Modification of messages



(d) Denial of service

Figure 1.3 Active attacks

- A masquerade takes place when one entity pretends to be a different entity (path 2 of Figure 1.1b is active). 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.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (paths 1, 2, and 3 active).

- 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 (paths 1 and 2 active). For example, a message meaning “Allow John Smith to read confidential file accounts” is modified to mean “Allow Fred Brown to read confidential file accounts.”

- The denial of service prevents or inhibits the normal use or management of communications facilities (path 3 active). 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 of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention.

Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them



Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of service

- Prevents or inhibits the normal use or management of communications facilities

Security Services

- Defined by X.800 as:
 - A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers
- Defined by RFC 4949 as:
 - A processing or communication service provided by a system to give a specific kind of protection to system resources

X.800 Service Categories

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Nonrepudiation



Authentication

- Concerned with assuring that a communication is authentic
 - In the case of a single message, assures the recipient that the message is from the source that it claims to be from
 - In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

Two specific authentication services are defined in X.800:

- Peer entity authentication
- Data origin authentication

Access Control


- 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 indentified, or authenticated, so that access rights can be tailored to the individual



Data Confidentiality

- The protection of transmitted data from passive attacks
 - Broadest service protects all user data transmitted between two users over a period of time
 - Narrower forms of service includes the protection of a single message or even specific fields within a message
- 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



Can apply to a stream of messages, a single message, or selected fields within a message

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

A connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only

Nonrepudiation

- Prevents either sender or receiver from denying a transmitted message
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message
- When a message is received, the sender can prove that the alleged receiver in fact received the message

Table 1.2

Security Services (X.800)

(This table is found on page 18 in textbook)

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication

Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication

In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

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).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality

The protection of all user data on a connection.

Connectionless Confidentiality

The protection of all user data in a single data block

Selective-Field Confidentiality

The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality

The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery

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.

Connection Integrity without Recovery

As above, but provides only detection without recovery.

Selective-Field Connection Integrity

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.

Connectionless Integrity

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.

Selective-Field Connectionless Integrity

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.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin

Proof that the message was sent by the specified party.

Nonrepudiation, Destination

Proof that the message was received by the specified party.

Security Mechanisms (X.800)

Specific Security Mechanisms

- Encipherment
- Digital signatures
- Access controls
- Data integrity
- Authentication exchange
- Traffic padding
- Routing control
- Notarization

Pervasive Security Mechanisms

- Trusted functionality
- Security labels
- Event detection
- Security audit trails
- Security recovery

SPECIFIC SECURITY MECHANISMS	PERVERSIVE SECURITY MECHANISMS
<p>May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.</p> <p>Encipherment 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>Digital Signature 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>Access Control A variety of mechanisms that enforce access rights to resources.</p> <p>Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.</p> <p>Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.</p> <p>Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.</p> <p>Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.</p> <p>Notarization 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>Trusted Functionality That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).</p> <p>Security Label The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.</p> <p>Event Detection Detection of security-relevant events.</p> <p>Security Audit Trail Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.</p> <p>Security Recovery Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.</p>

Table 1.3

Security Mechanisms (X.800)

(This table is found on pages 20-21 in textbook)

Model for Network Security

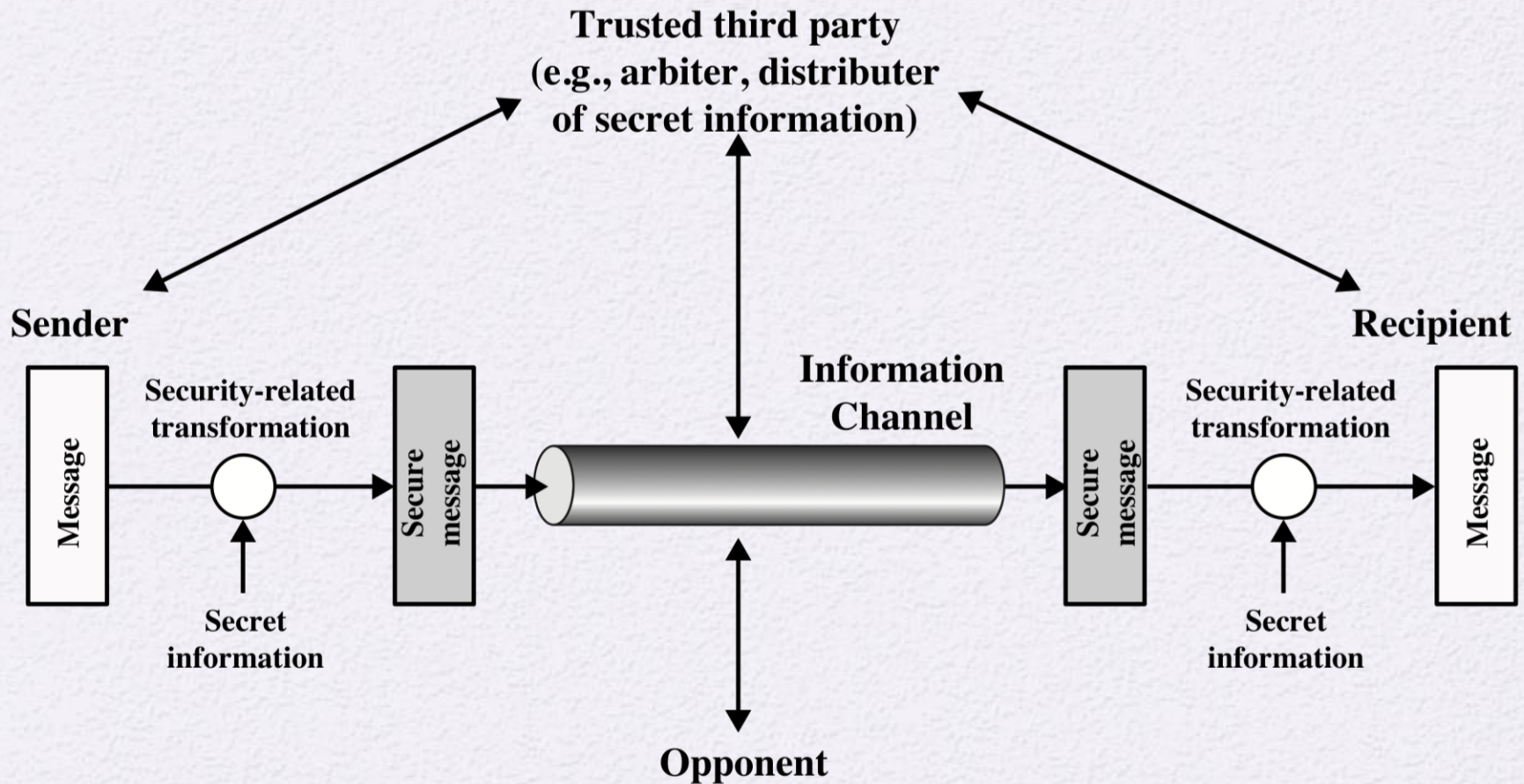


Figure 1.2 Model for Network Security

Network Access Security Model

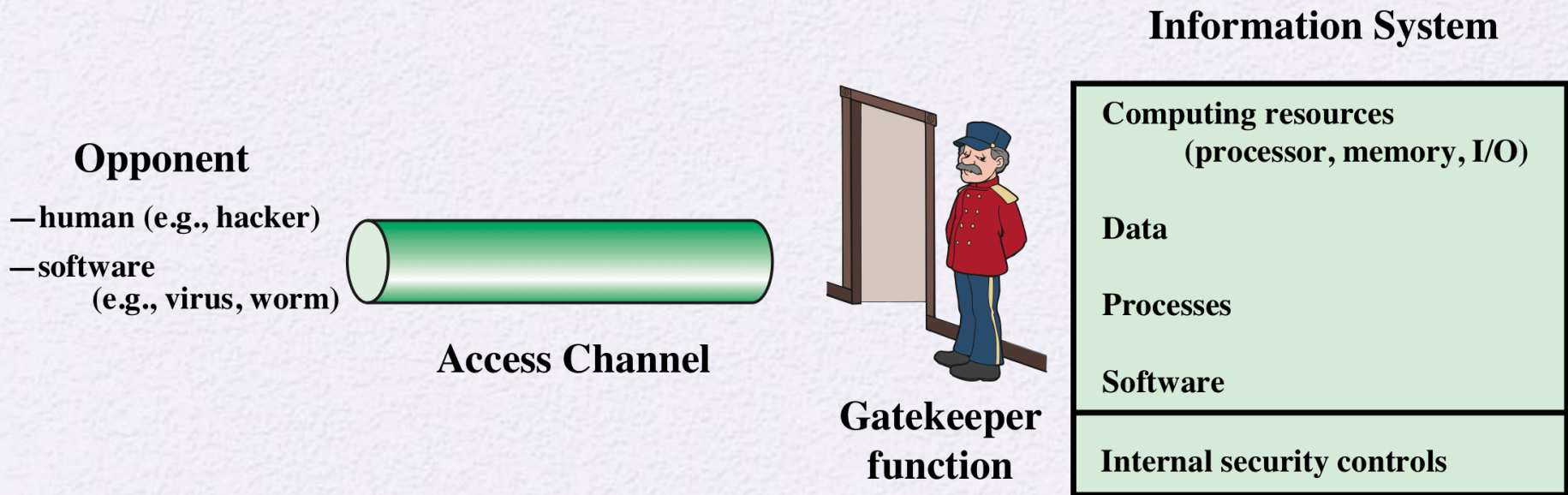


Figure 1.3 Network Access Security Model

Unwanted Access

- Placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs such as editors and compilers
- Programs can present two kinds of threats:
 - Information access threats
 - Intercept or modify data on behalf of users who should not have access to that data
 - Service threats
 - Exploit service flaws in computers to inhibit use by legitimate users



Summary

- Computer security concepts
 - Definition
 - Examples
 - Challenges
- The OSI security architecture
- Security attacks
 - Passive attacks
 - Active attacks



- Security services
 - Authentication
 - Access control
 - Data confidentiality
 - Data integrity
 - Nonrepudiation
 - Availability service
- Security mechanisms