



Advance Security 1

Lecture 1

Introduction

Assessment Methods

- Written examination – 60%
- Continuous assessment – 40%
 - Theory test 1 (week 6)- 10%
 - Theory test 2 (week 12)- 10% (All Lectures included)
 - Assignment 1 Cryptographic Tools (week 5)- 10%
 - Assignment 2 Algorithms Implementations (week 13)- 10%

Module Contents

- Introduction to Advanced Security
- Number theory, Discrete logarithms and Elliptic Curves
- Steganography
- **Symmetric Encryption:** Block Ciphers and Advanced Encryption Standard, Confidentiality Using Conventional Encryption.
- **Asymmetric Encryption:** Public-Key Cryptography and RSA,
- **Mutual Trust:** Key management and Authentication Protocols
- **Cryptographic Hash Functions:** Message Authentication and Hash Functions, Hash and Mac Algorithms, Digital Signatures.

Text Book

Cryptography and Network Security : Principles
and Practices, 6th Ed, Williams Stallings (2014)
Pearson.

Book Chapters

- Chapter 1: Overview
- Chapter 2: Classical Encryption Techniques
- Chapter 3: Block ciphers and the data encryption standard
- Chapter 4: Basic Concepts in Number Theory and Finite Fields
- Chapter 5 Advanced Encryption Standard
- Chapter 6 Block Cipher Operation
- Chapter 7 Pseudorandom Number Generation and Stream Ciphers
- Chapter 8 More Number Theory
- Chapter 9 Public-Key Cryptography and RSA
- Chapter 11 Cryptographic Hash Functions
- Chapter 14 Key Management and Distribution

References

- Network Security Essentials: Applications and Standards, 4th Ed, William Stallings (2010), Prentice Hall.
- Introduction to Cryptography with Java Applets, David Bishop (2003), Jones and Batlett Computer Science.
- Cryptography Engineering, Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno (2010), John Wiley and Sons
- Any Book on Cryptography
- Web

Assessment guidelines

- This is not a distant education module, therefore attendance to lectures and labs is necessary and make sure you sign the attendance sheet.
- Anyone who is not attending the assumption is that you know what we are doing.
- If you miss an assessment submission date marks will be deducted as follows:
 - Each day 20%
 - No submission will be accepted after I finish marking and give feedback in class.

Assessment guidelines

- The success of the module is a team effort:
- Depends on honest participation, increase knowledge, share and dare
- Submission guidelines
 - naming files (Full-Name_Student-Number_Assignment-Name), use Brightspace, no email submission
- Report guidelines
 - Cover page, introduction, body, discussion, conclusion and references
- Lab demonstration guidelines – must be done in the lab

Postgraduate Studies

- MSc in Computing (Security & Forensics)
 - Full time - DT228A Part time - DT228B
 - Digital forensics, also known as computer and network forensics is the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. Every organisation and user needs to have the capability to perform digital forensics. Without such a capability, organisations and users will have difficulty determining what events have occurred within their systems, networks and mobile devices, such as the exposure of protected, sensitive data.

Security and Forensics Course at other Universities in Ireland

- Institute of Technology Blanchardstown
 - Master of Science in Computing (Information Security & Digital Forensics)
- Cork Institute of Technology
 - Master of Science in Networking & Security
- Dublin City University
 - M.Sc. in Security and Forensic Computing
- Letterkeny IT
 - Master of Science in Computing in Systems & Software Security

Security and Forensics Course at other Universities in Ireland

- University College Dublin
 - MSc Digital Investigation and Forensic Computing
 - Forensic Computing and Cybercrime Investigation (FCCI). Qualifications include Graduate Certificate, Graduate Diploma, Master of Science and Continuous Professional Development programme (CPD).
- University of Limerick
 - MEng Information and Network Security

Final Year Projects in Security

- Use of Cryptography in applications running in mobile devices.
- How Cryptography can be used to provide secure transmission of information in Cloud and the Internet of things
- Efficient deployment of Cryptography in systems
- Security protocols or algorithms
- Security Games development

Final Year Projects in Security

- Intelligent rules creation in Firewall, IDS and IPS.
- E-learning project to demonstrate vulnerabilities of applications, protocols or Operating Systems.
- Extend or modify the functionalities of Security Tools such as Kali Linux, Snort, Wireshark, nmap, netcat etc
- Test the performance of security tools

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

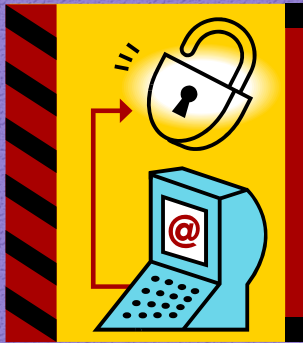
Data integrity algorithms

- 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

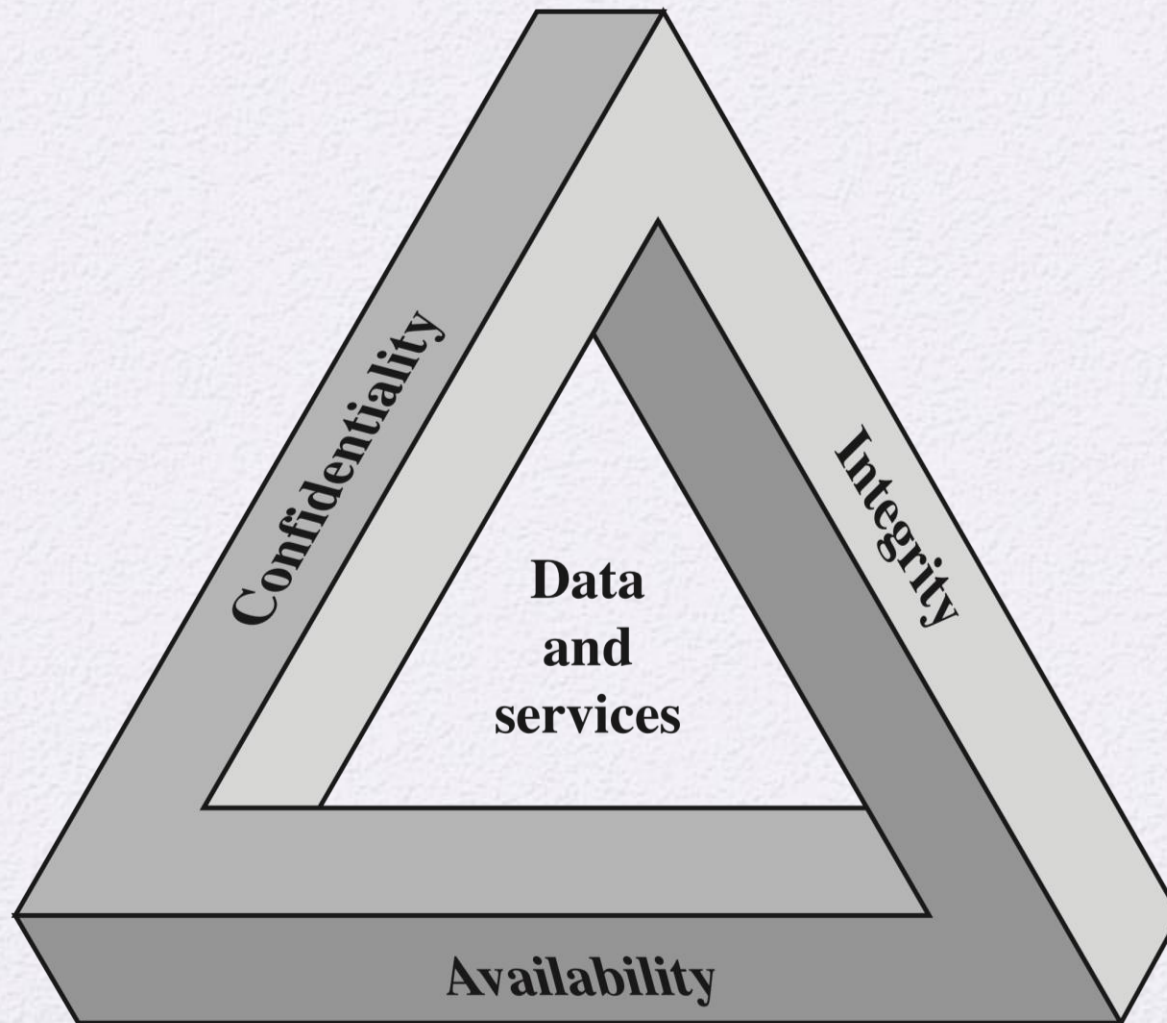
Integrity

- 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



Possible additional concepts:

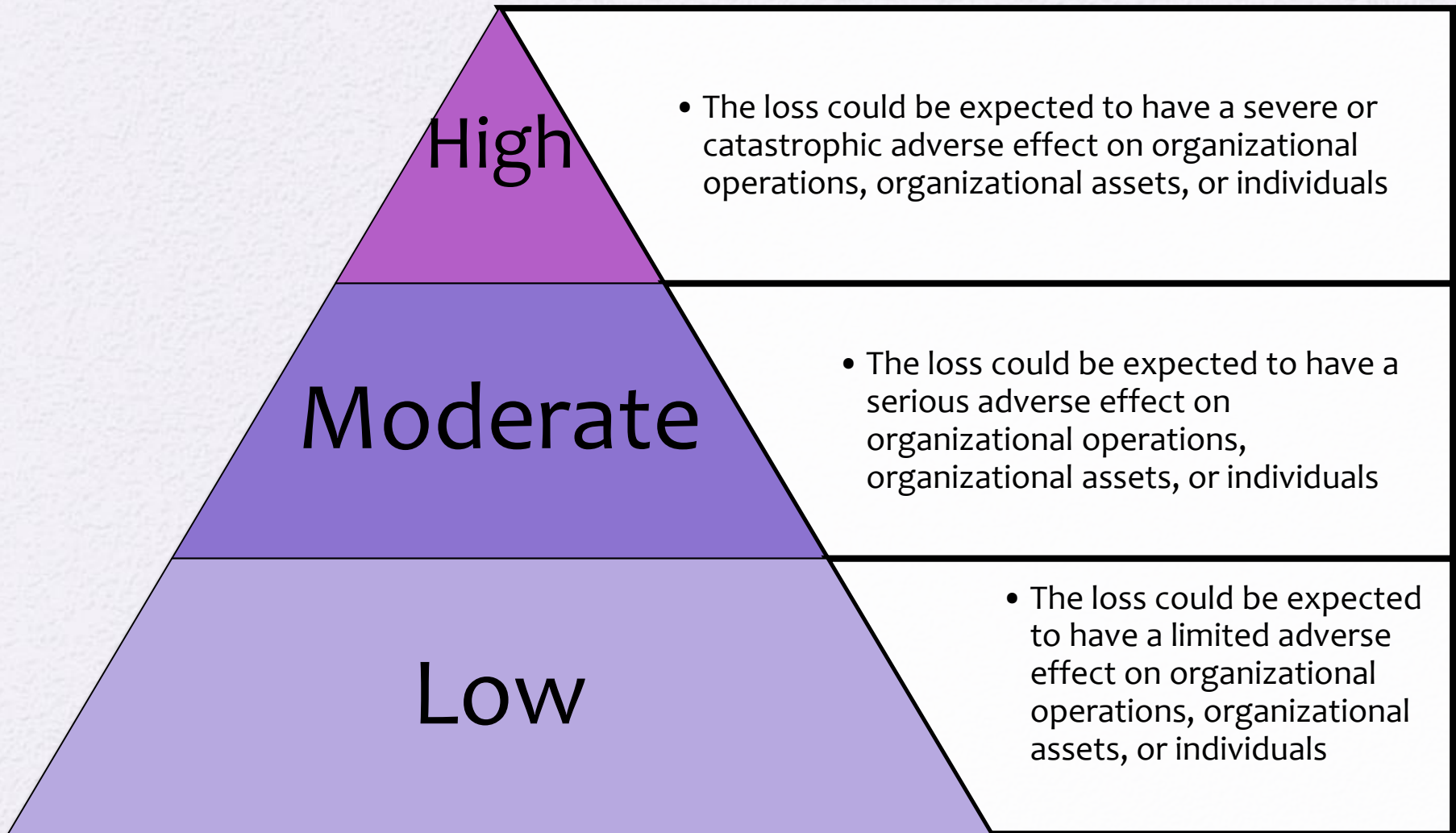
Authenticity

- 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

Breach of Security Levels of Impact



Computer Security Challenges

- Security is not simple
- Potential attacks on the security features need to be considered
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- 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

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

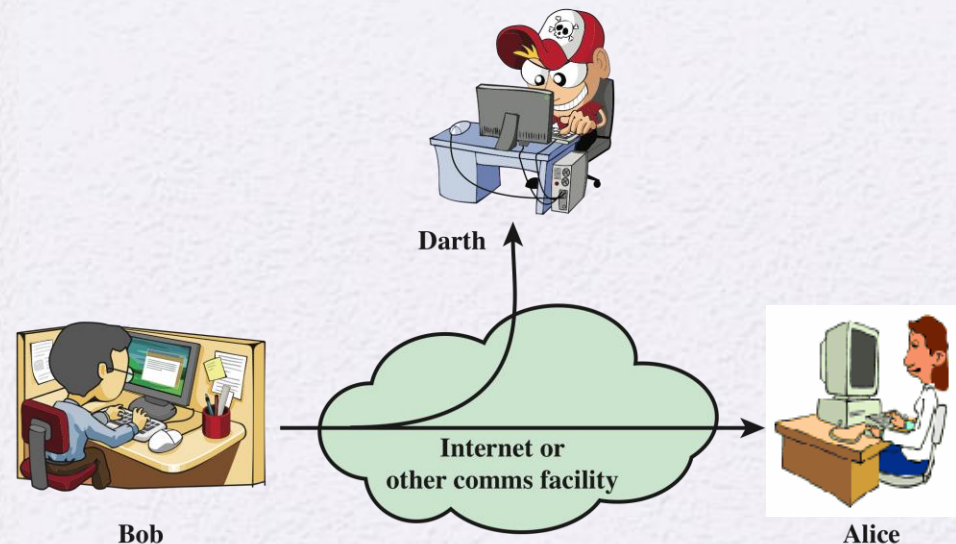
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Security Attacks

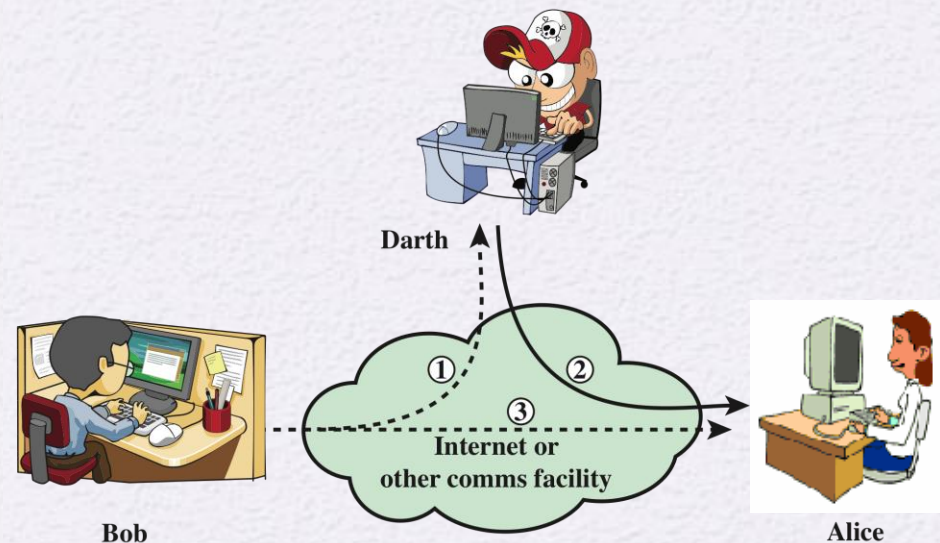
- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*

- 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

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 identified, 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	PERVASIVE 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

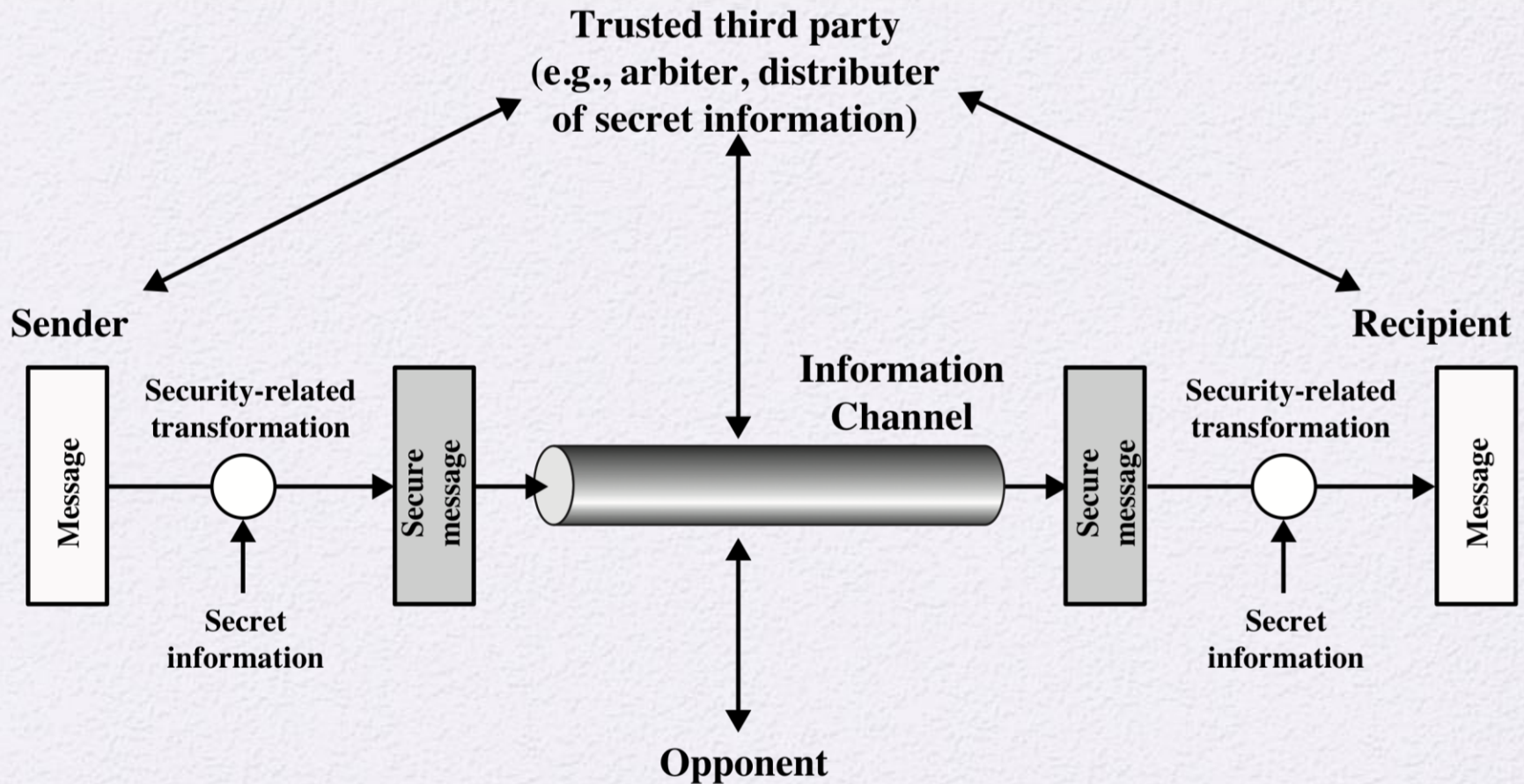


Figure 1.2 Model for Network Security

Network Access Security Model

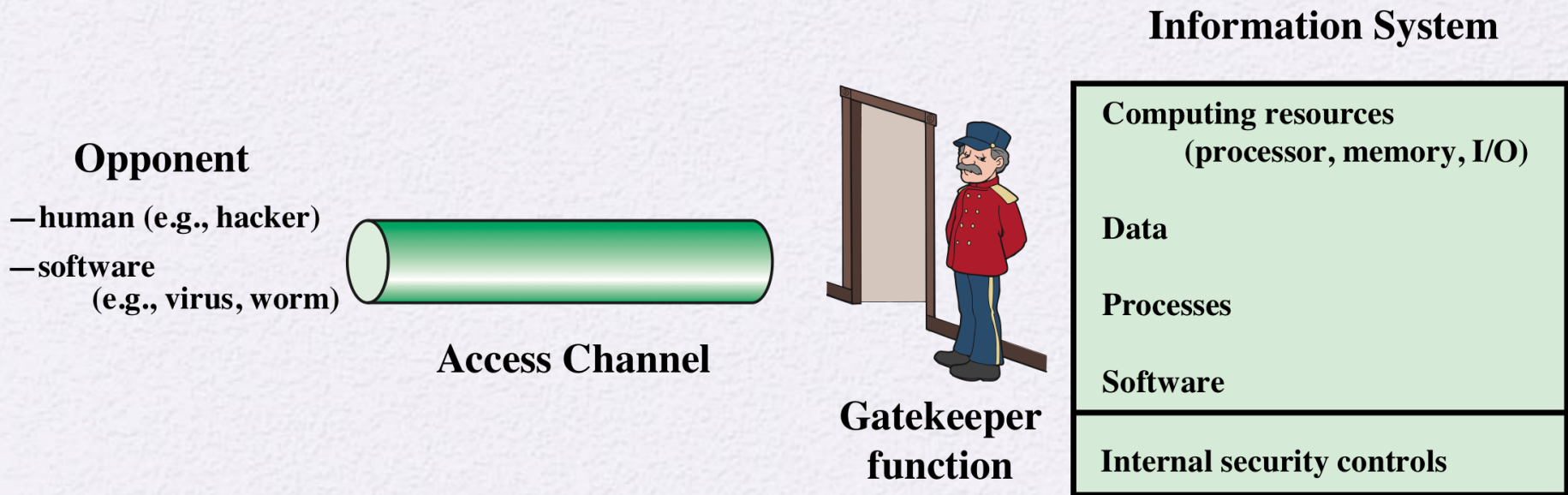


Figure 1.3 Network Access Security Model

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