RT 801 - Security in Computing

Module I

Module1

- Introduction: Security basics – Aspects of network security – Attacks – Different types– Security services and mechanisms – Hackers – Crackers – Common intrusion techniques –Trojan Horse, Virus, Worm.

Security Breaches in the News

•July 28, 2006 Sisters of St. Francis Health Services via Advanced Receivables Strategy (ARS), a Perot Systems Company

A contractor misplaced CD's containing the names and SSN's of 266,200 patients, employees, physicians, and board members of St. Francis hospitals in Indiana and Illinois. The disks were inadvertently left in a laptop case that was returned to a store. The purchaser returned the disks. The records were not encrypted even though St. Francis and ARS policies require encryption.

•Nov. 2, 2006 Intermountain Health Care
(Salt Lake City, UT)

A computer was purchased at a second-hand store, Deseret Industries, that contained the names, Social Security numbers, employment records, and other personal information about Intermountain Health Care employees employed there in 1999-2000.

•Records Lost: 6,244

•Dec 22, 2006 - Texas Woman's University
A document containing names, addresses and SSN's of 15,000 TWU students was transmitted over a non-secure connection.

•Jan 11th, 2007 - University of Idaho

3 desktop computers were stolen from the Advancement Services office containing personal information of alumni, donors, employees, and students. 331,000 individuals may have been exposed, with as many as 70,000 records containing SSN's, names and addresses.

Mobile security outrage: private details accessible on net

- The personal details of millions of Vodafone customers, including their names, home addresses, driver's licence numbers and credit card details, have been publicly available on the internet in what is being described as an "unbelievable" lapse in security by the mobile phone giant.
- Personal details, accessible from any computer because they are kept on an internet site rather than on Vodafone's internal system, include which numbers a person has dialled or texted, plus from where and when.

The Australian Privacy Commissioner is investigating

FBI probing theft of 8 million credit card numbers

Reuters, 02.19.03, 7:03 PM ET

Get quotes

get quotes

NEW YORK (Reuters) - The FBI is investigating a recent computer hacking incident in which as many as eight million credit card numbers may have been stolen from a company that processes transactions, industry representatives and investigators said Wednesday.

Omaha-based Data Processors International, which processes transactions involving Visa, MasterCard, American Express and Discover Financial Services for merchants, said in a statement that it had "recently experienced a system intrusion by an unauthorized outside party."

"We are aware of the matter and looking into it," said FBI spokesman Paul Bresson, who said he could not comment further on the pending investigation.

Omaha-based Data Processors International, which processes transactions involving Visa, MasterCard, American Express and Discover Financial Services for merchants, said in a statement that it had "recently experienced a system intrusion by an unauthorized outside party."

E-Mail Alerts

Get stories by e-mail on this topic.

Topics

Two Arrested, Charged With Stealing AOL Names For Spam

By AFX News
06/23/04 10:01 PM PT

AOL released a statement saying it was "absolutely committed" to the prosecution of Smathers. AOL kept its customer list in a database at its headquarters in Dulles, Virginia, according to the complaint. It said Smathers worked in that office, but was not authorized to access or copy the customer information when he stole it.

5 years and $250K

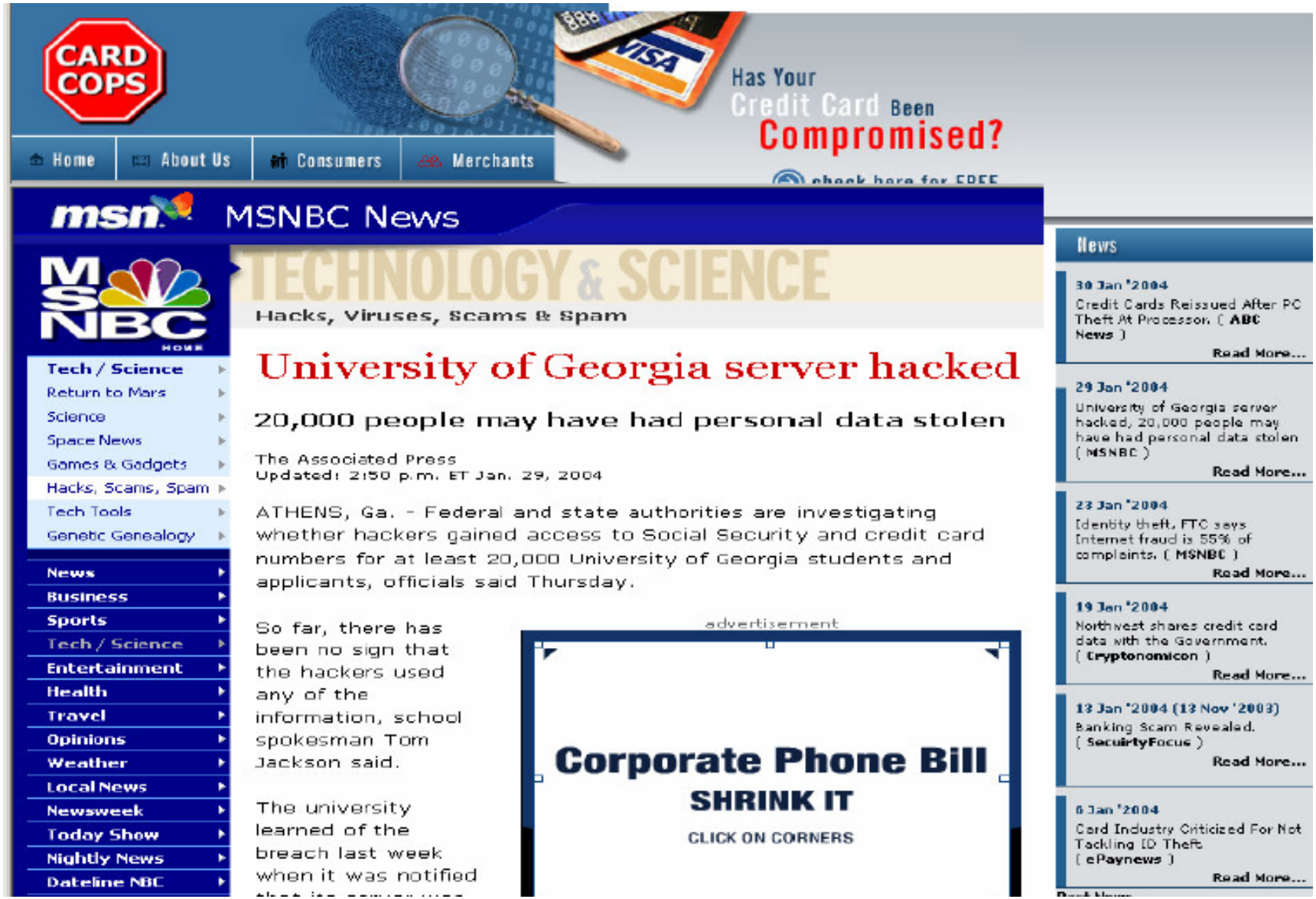
The complaint said Smathers and Dunaway each face a maximum sentence of five years in prison and a fine of $250,000, or twice the gross gain or gross loss from the offense. AOL's

Two men, one of them an employee of America Online, were arrested Wednesday on charges that they stole the entire list of AOL (NYSE: AOL) user names and sold it to e-mail marketers, according to prosecutors.

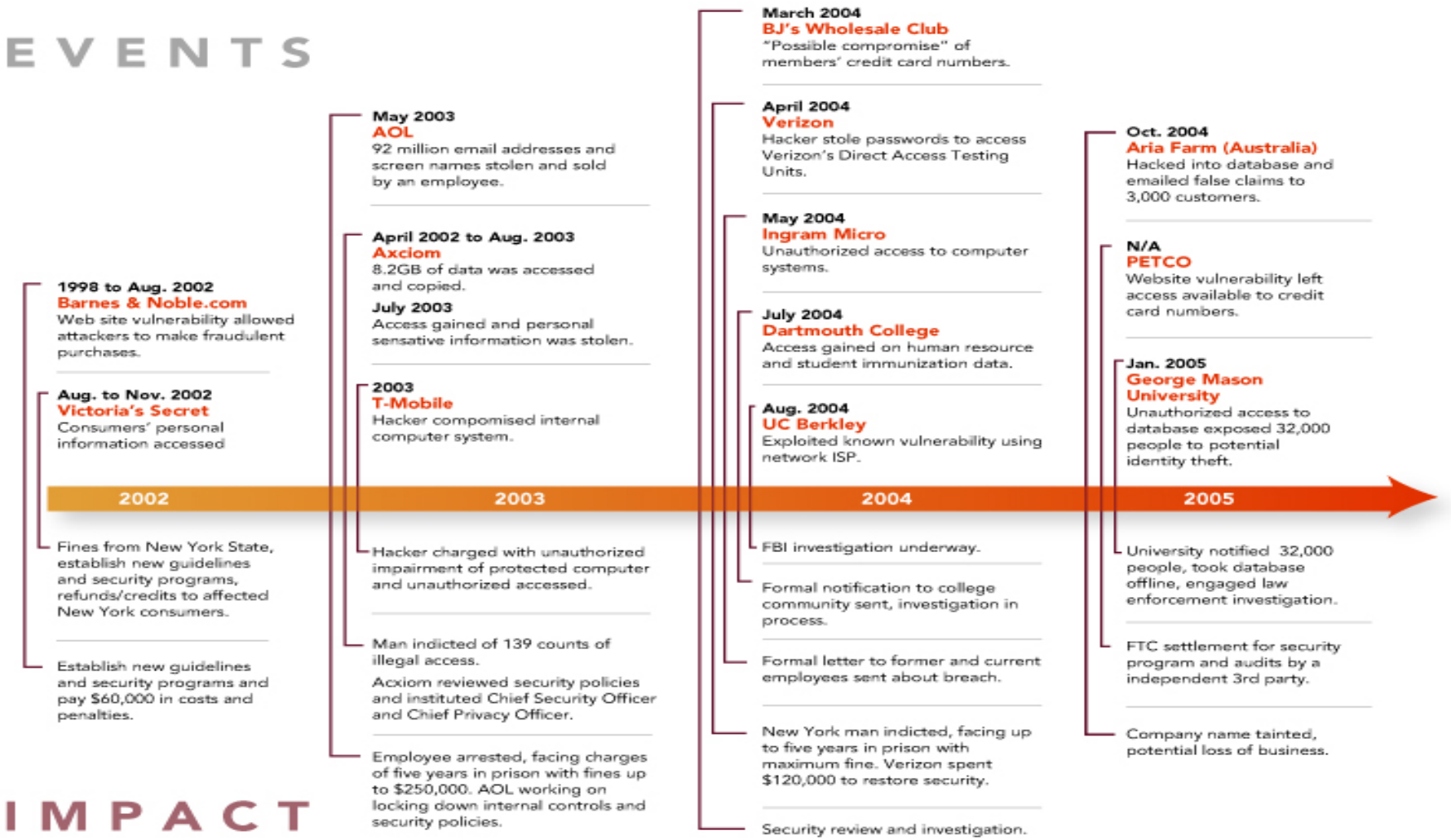
Jason Smathers, a 24-year-old AOL software engineer, and 21-year-old Sean Dunaway were arrested in their homes on conspiracy charges filed in New York federal court.

According to the complaint announced by U.S. Attorney David Kelley, Smathers in May 2003 misappropriated a list of 92 million AOL customer account screen names."

This case is one of the first to be prosecuted under a new U.S. law regulating unwanted e-mail.


CARD COPS
Has Your Credit Card Been Compromised?
Home
About Us
Consumers
Merchants
msn MSNBC News
MSNBC
Tech / Science
Return to Mars
Science
Space News
Games & Gadgets
Hacks, Scams, Spam
Tech Tools
Genetic Genealogy
News
Business
Sports
Tech / Science
Entertainment
Health
Travel
Opinions
Weather
Local News
Newsweek
Today Show
Nightly News
Dateline NBC
TECHNOLOGY & SCIENCE
Hacks, Viruses, Scams & Spam
University of Georgia server hacked
20,000 people may have had personal data stolen
The Associated Press
Updated: 2:50 p.m. ET Jan. 29, 2004
ATHENS, Ga. - Federal and state authorities are investigating whether hackers gained access to Social Security and credit card numbers for at least 20,000 University of Georgia students and applicants, officials said Thursday.
So far, there has been no sign that the hackers used any of the information, school spokesman Tom Jackson said.
The university learned of the breach last week when it was notified
advertisement
Corporate Phone Bill
SHRINK IT
CLICK ON CORNERS
News
30 Jan '2004
Credit Cards Reissued After PC Theft At Processor. (ABC News)
Read More...
29 Jan '2004
University of Georgia server hacked, 20,000 people may have had personal data stolen (MSNBC)
Read More...
23 Jan '2004
Identity theft, FTC says Internet fraud is 55% of complaints. (MSNBC)
Read More...
19 Jan '2004
Northwest shares credit card data with the Government. (Cryptonomicon)
Read More...
13 Jan '2004 (13 Nov '2003)
Banking Scam Revealed. (SecuirtyFocus)
Read More...
6 Jan '2004
Card Industry Criticized For Not Tackling ID Theft (ePaynews)
Read More...

New Target: Applications & Databases



What is “Security”

- Dictionary.com says:
  - 1. Freedom from risk or danger; safety.
  - 2. Freedom from doubt, anxiety, or fear; confidence.
  - 3. Something that gives or assures safety, as:
    - 1. A group or department of private guards: Call building security if a visitor acts suspicious.
    - 2. Measures adopted by a government to prevent espionage, sabotage, or attack.
    - 3. Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant.

  …etc.

Security

- **Security** is the condition of being protected against danger or loss.
- Facilities and the information systems they support have become increasingly accessible as a result of the explosion of the open, public Internet since about 1993.
- **Insecurity** - Lack of security
- Security is important throughout the information life-cycle, i.e. during the collection, storage, processing, use and disclosure phases, as well as transmission.
- Security is used in at least two senses:
  - **a condition** in which harm does not arise, despite the occurrence of threatening events; and
  - **a set of safeguards** designed to achieve that condition.

Why do we need security?

- Protect vital information while still allowing access to those who need it
  - Trade secrets, medical records, etc.
- Provide authentication and access control for resources
- Guarantee availability of resources

Who is vulnerable?

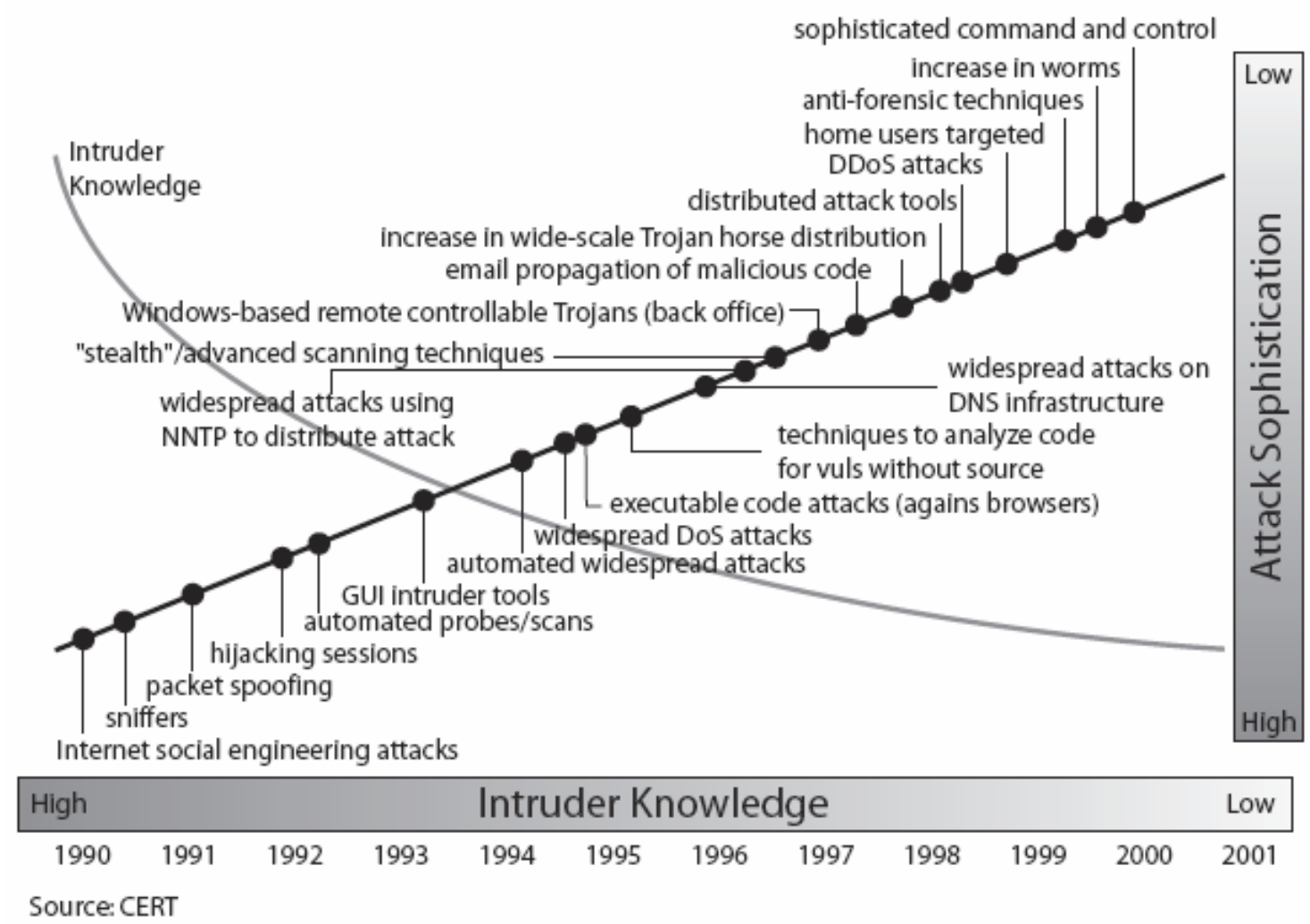
- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations
- **ANYONE ON THE NETWORK**

Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

- **Internet Security**
  - which consists of measures to prevent, detect, and correct security violations that involve the transmission & storage of information

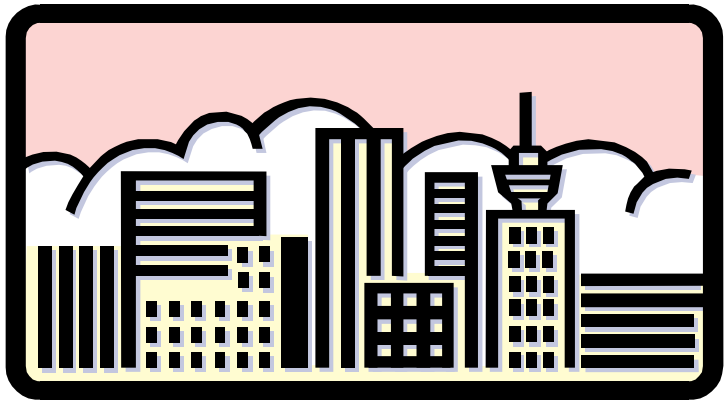
Security Trends



Source: CERT

OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements
- OSI Security architecture provides focuses on security attacks, mechanisms and services



Aspects of Security

- 3 aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**

Attacks, Services and Mechanisms

- **Security Attack:** Any action that compromises the security of information owned by an organization.
- **Security Mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security Service:** A service that enhances the security of data processing systems and information transfers.
  - A security service makes use of one or more security mechanisms.

Security Attack

- Any action that compromises the security of information owned by an organization
- Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- Often *threat* & *attack* used to mean same thing
- have a wide range of attacks
- generic types of attacks
  - passive
  - active

Threats and Vulnerabilities

- **Vulnerability:** A weakness which can be exploited to cause loss or harm.
- **Threat:** A set of circumstances that has the potential to cause loss or harm.

Here is a picture of a threat.

Can you see the vulnerability?

A threat is blocked by control of a vulnerability.

Attacks

- An attack is **an attempt by a human to exploit a vulnerability**.
- An attacker needs to have "**MOM**":
  - **Method**: The necessary skills to pull off the attack.
  - **Opportunity**: The time and access to perform the attack.
  - **Motive**: A reason to perform the attack.
- Reasons can be very diverse!
  - Revenge
  - Entertainment
  - Prestige
  - "Because it was there"
  - Economic gain
  - Political/religious

- Perceived security compared to real security
  - fear of flying is much more common than a fear of driving; however, driving is generally a much more dangerous form of transport.
  - The tool may be mistaken for the effect
    - for example when multiple computer security programs interfere with each other, the user assumes the computer is secure when actual security has vanished.

Multiple computer security programs

- Scanning your computer for viruses and spyware uses some of the available memory on your computer.
- If you have multiple programs trying to scan at the same time, you may limit the amount of resources left to perform your tasks. Essentially, you have created a denial of service against yourself.
- It is also possible that in the process of scanning for viruses and spyware, anti-virus or anti-spyware software may misinterpret the virus definitions of other programs.
- Instead of recognizing them as definitions, the software may interpret the definitions as actual malicious code.
- The anti-virus or anti-spyware software may actually quarantine or delete the other software.

- Sometimes if it is perceived that there is security then there will be an increase in actual security, even if the perception of security is mistaken.
  - Sometimes a sign may warn that video surveillance is covering an area, and even if there is no actual visual surveillance then some malicious agents will be deterred by the belief that there may be.

- Also, often when there is actual security present in an area, such as video surveillance, an alarm system in a home, or an anti-theft system in a car - advertising this security will increase its effectiveness, protecting the value of the secured vehicle or area itself.
  - The car itself and the objects inside aren't stolen, but with perceived security even the windows of the car have a lower chance of being damaged

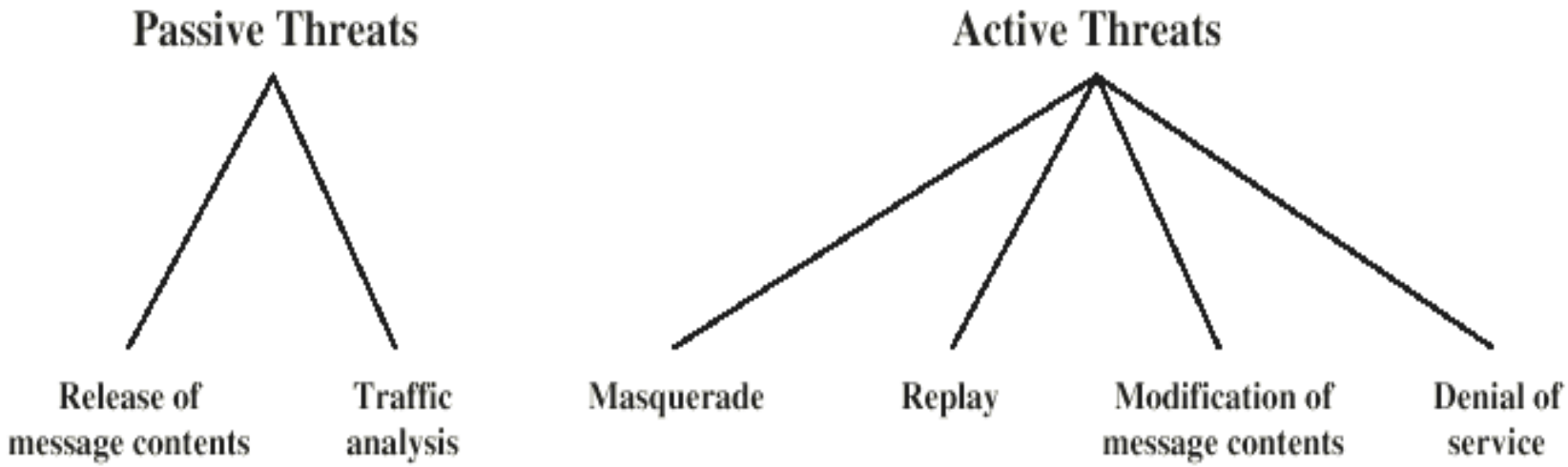
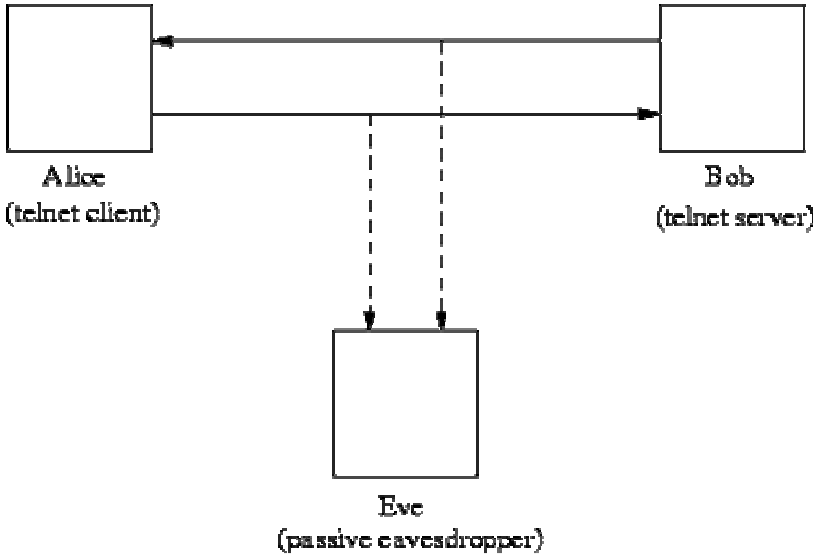


Figure 1.2 Active and Passive Security Threats

Passive Attacks

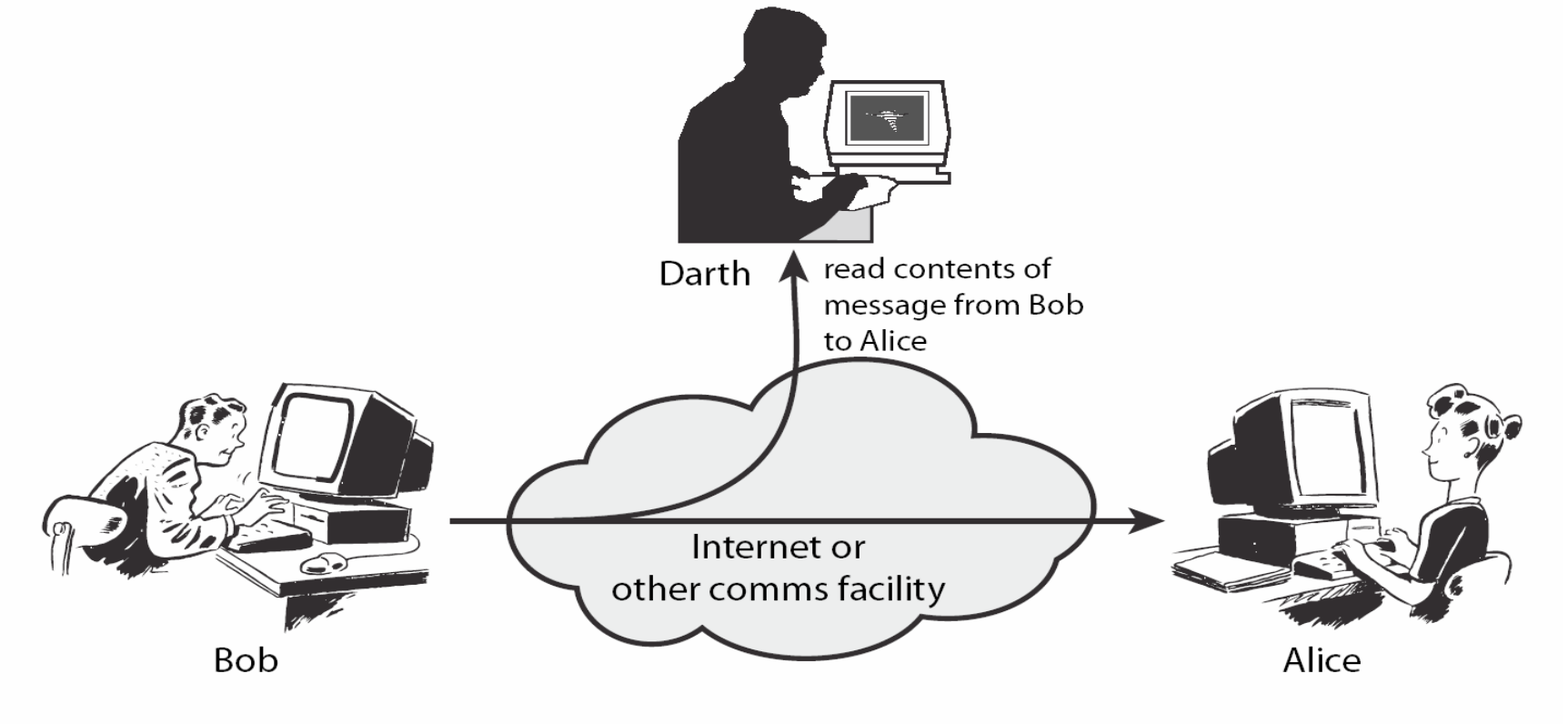
- A passive attack is an attack where an unauthorized attacker monitors or listens in on the communication between two parties.



Passive Attacks

•Release of Message Contents

A telephone conversation, an E-mail messages, and file transfer can be easily accessed without effecting the message



Passive Attacks -Traffic Analysis

- Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication.
- It can be performed even when the messages are encrypted and cannot be decrypted.
- The greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic.
- Traffic analysis can be performed in the context of military intelligence or counter-intelligence.

In military intelligence

- Representative patterns include:
  - Frequent communications — can denote planning
  - Rapid, short, communications — can denote negotiations
  - A lack of communication — can indicate a lack of activity, or completion of a finalized plan
  - Frequent communication to specific stations from a central station — can highlight the chain of command
  - Who talks to whom — can indicate which stations are 'in charge' or the 'control station' of a particular network. This further implies something about the personnel associated with each station
  - Who changes from station to station, or medium to medium — can indicate movement, fear of interception

- 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 -Traffic Analysis

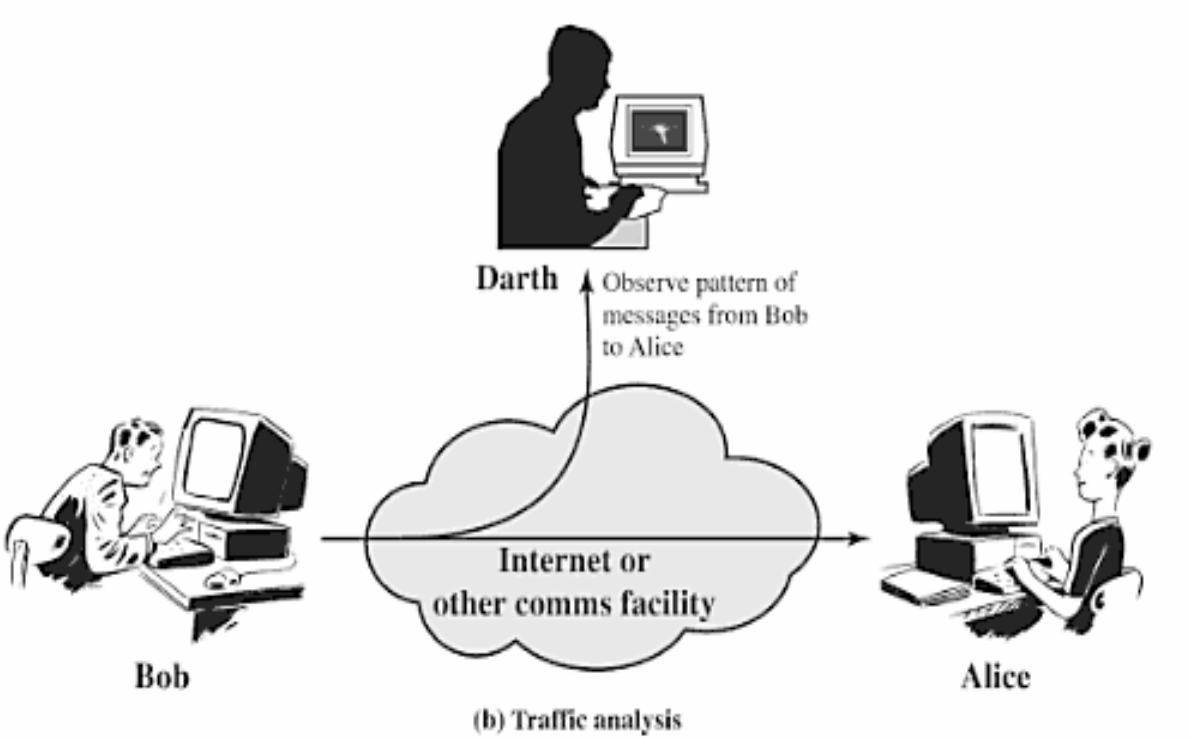
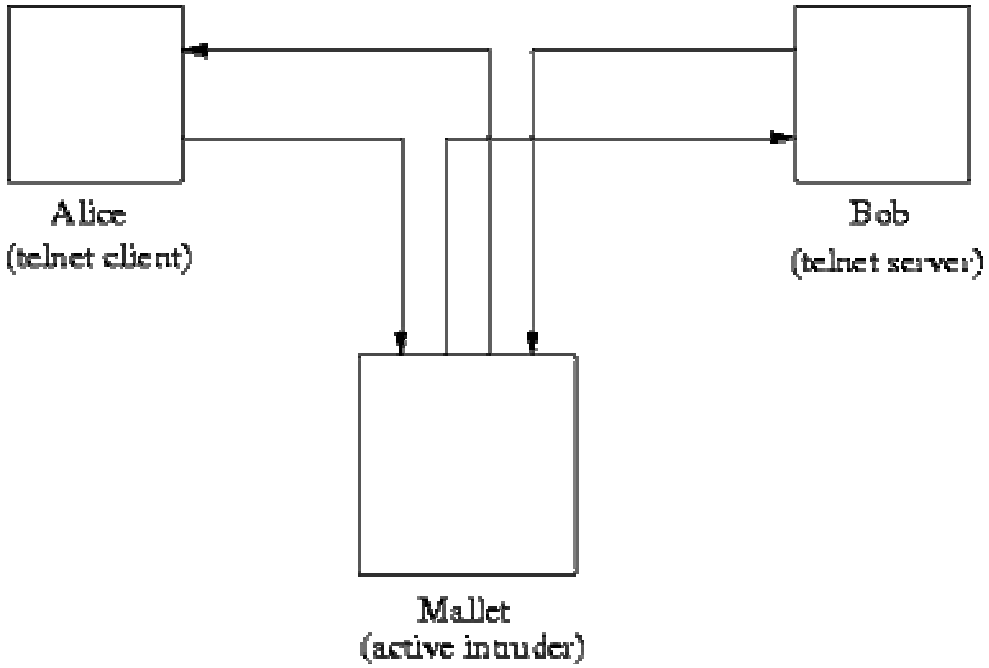


Figure 1.3 Passive Attacks

Active Attacks

- Active attacks involve some modification of the data stream or the creation of a false stream.
- This type of attack requires the attacker to be able to transmit data to one or both of the parties, or block the data stream in one or both directions.
- The attacker is located between the communicating parties.

Active Attacks

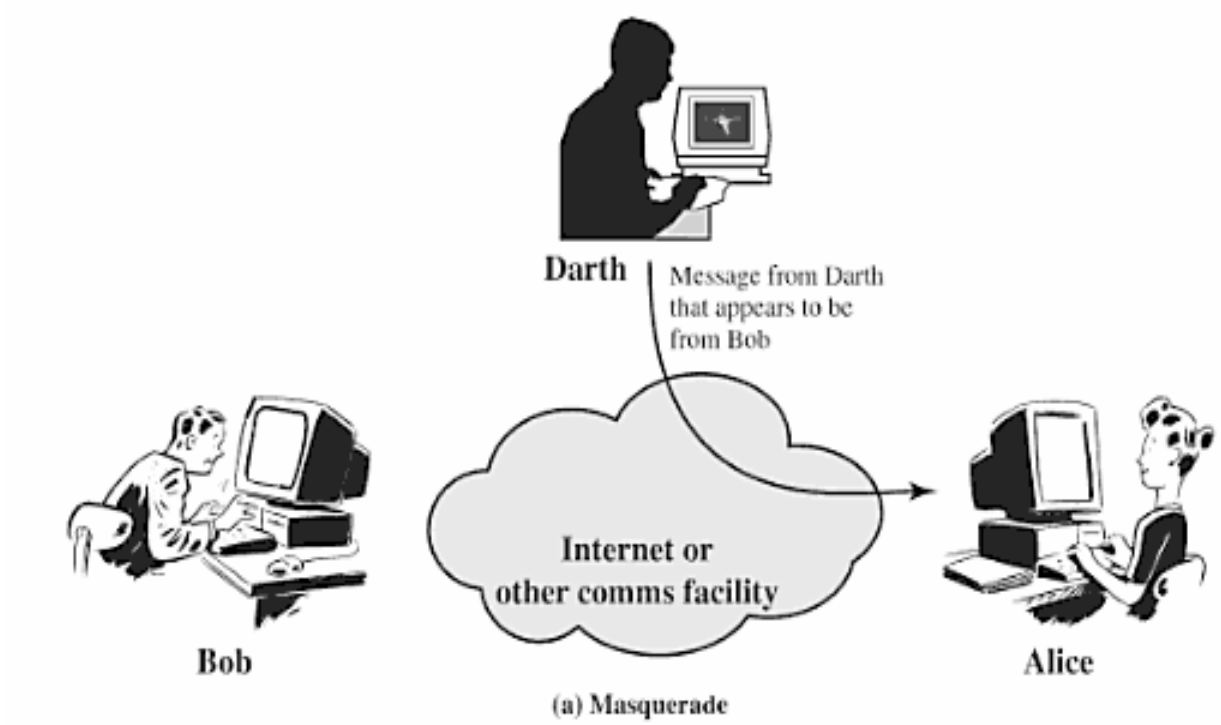


Active Attacks

- Subdivided into four categories:
  - Masquerade
  - Replay
  - Modification of messages
  - Denial of service

Active Attacks

The attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for.



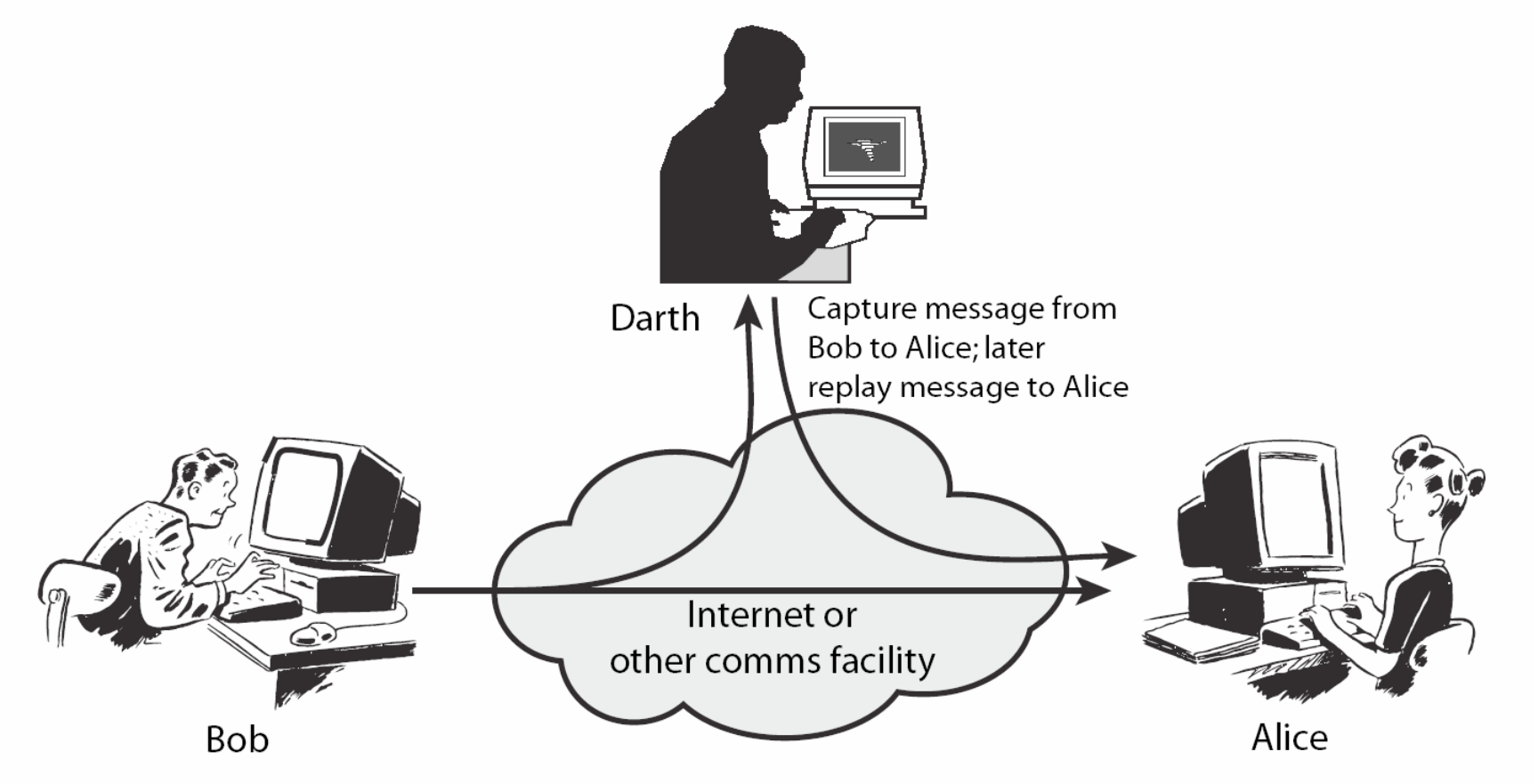
Masquerade

- A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism.
- The attempt may come from within an organization, for example, from an employee; or from an outside user through some connection to the public network.

- **Weak authentication** provides one of the easiest points of entry for a masquerade, since it makes it much easier for an attacker to gain access.
- Once the attacker has been authorized for entry, they may have full access to the organization's critical data, and may be able to modify and delete software and data, and make changes to network configuration and routing information.

Active Attacks

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

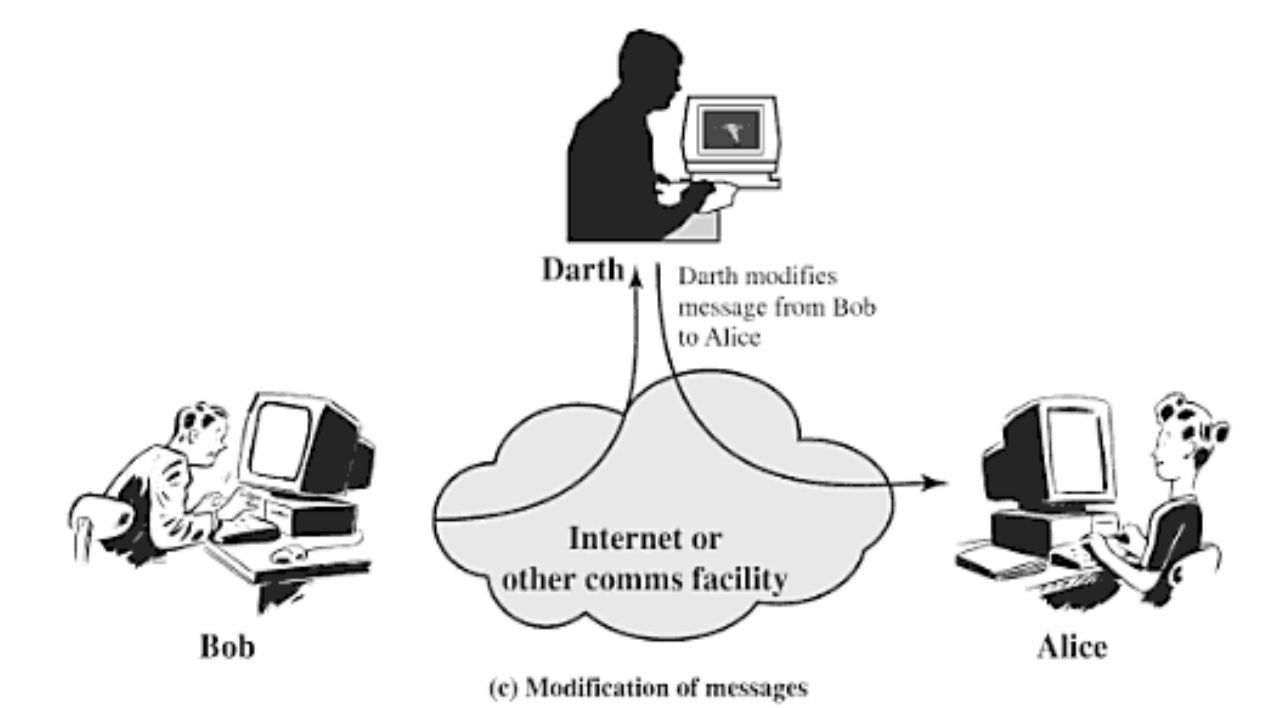


Replay Attack

- Suppose Alice wants to prove her identity to Bob.
- Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Mallory is eavesdropping the conversation and keeps the password.
- After the interchange is over, Darth connects to Bob posing as Alice; when asked for a proof of identity, Mallory sends Alice's password read from the last session, which Bob accepts.

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 meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."

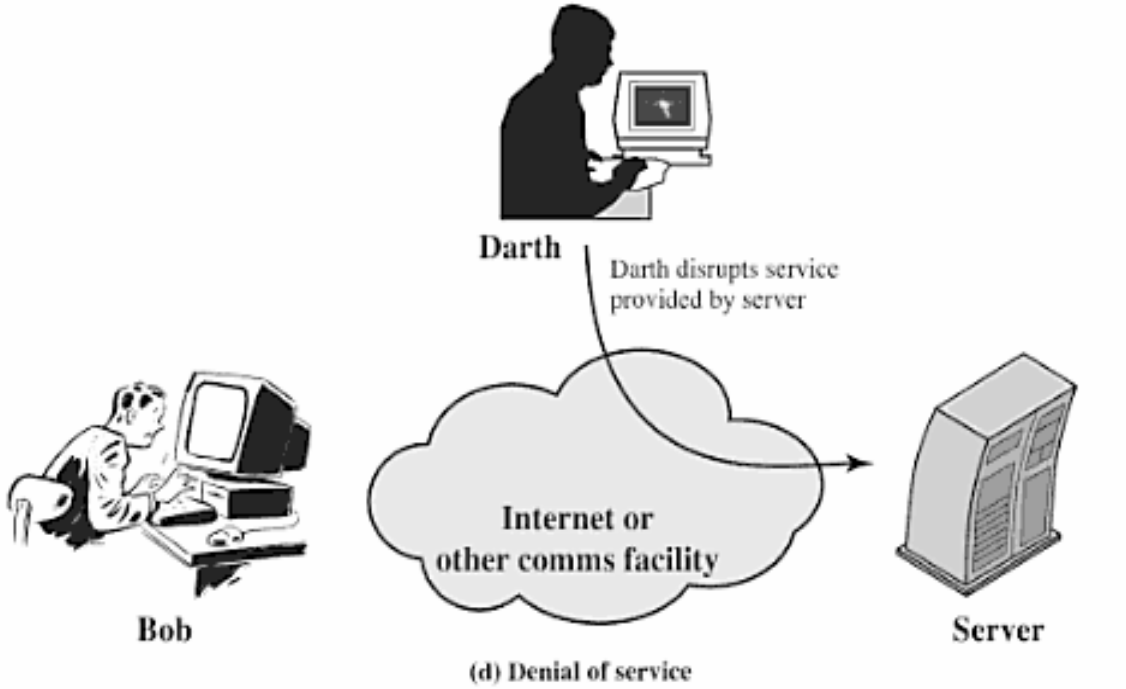


(c) Modification of messages

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.



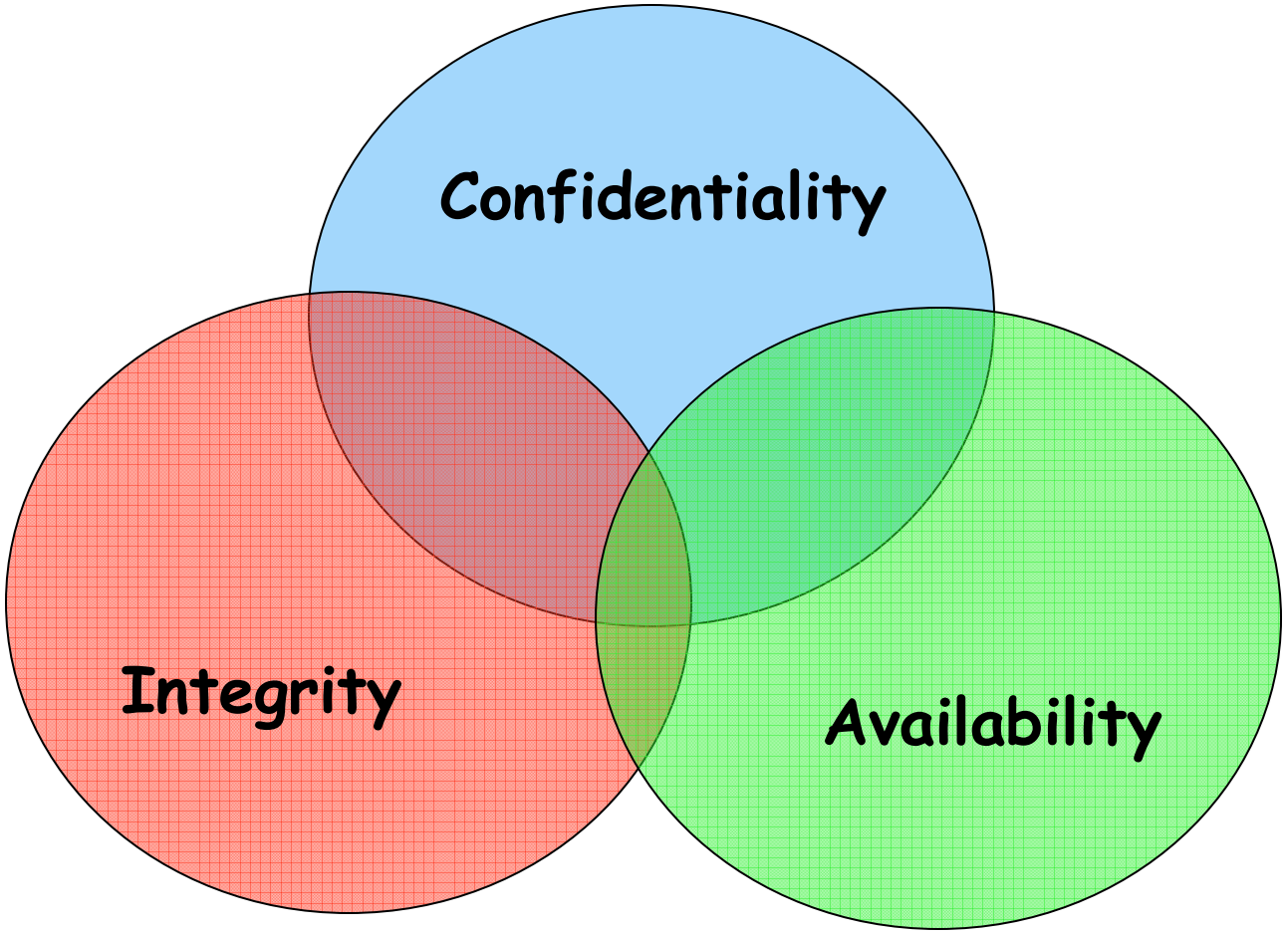
(d) Denial of service

- **Denial of service** generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.
- Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways etc..

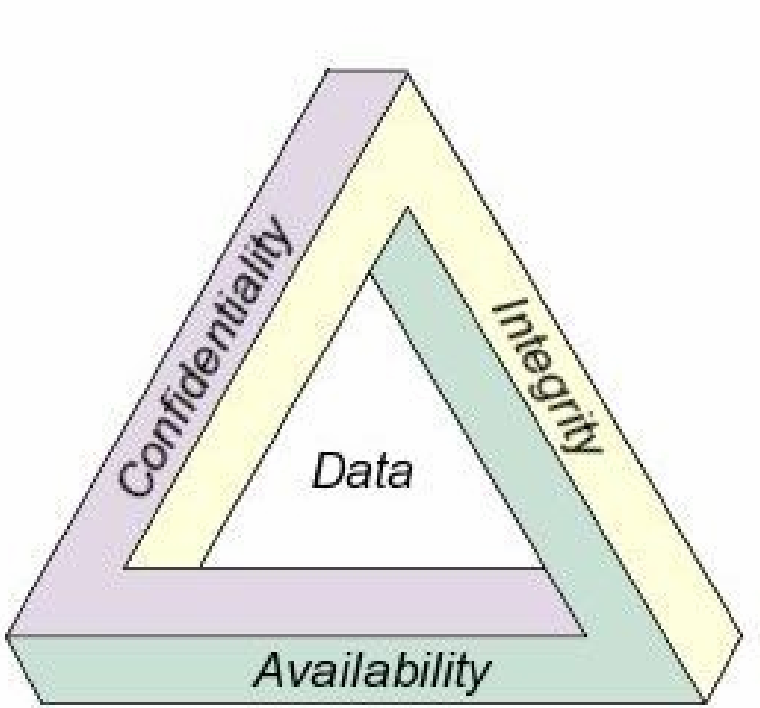
- A DoS attack can be perpetrated in a number of ways.
  - Consumption of computational resources, such as bandwidth, disk space, or processor time.
  - Disruption of configuration information, such as routing information.
  - Disruption of state information, such as unsolicited resetting of TCP sessions (falsely terminating an established TCP connection) .
  - Disruption of physical network components.
  - Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

- 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.
- 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.

Security Goals



CIA Triad



What are the Basic Facets of Database Security?

- Unauthorized entry or access to a server signifies a loss of confidentiality
- Unauthorized alteration to the available data signifies loss of integrity
- and lack of access to services signifies loss of availability

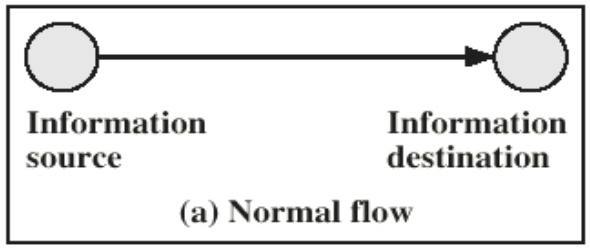
Illustration

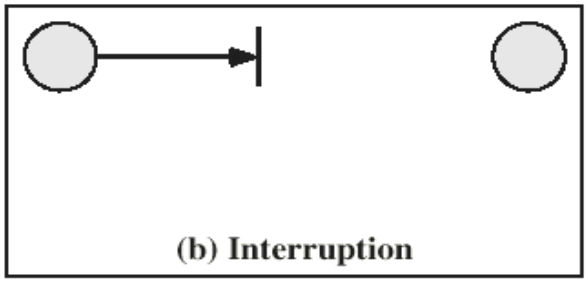
- Imagine that the website of a company contains information like who they are, what they do, and what prospective customers have to do to contact them for their queries.
  - In this case, the availability of the database services is more important when compared with other factors like the confidentiality or integrity of the database security.
- For a company that sells products or goods online, however, confidentiality and integrity are more important as customers use their credit cards to buy goods online only when the site is available.

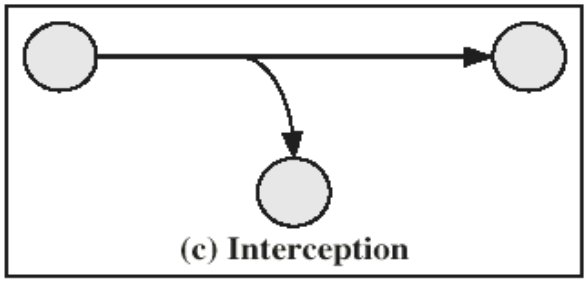
Integrity

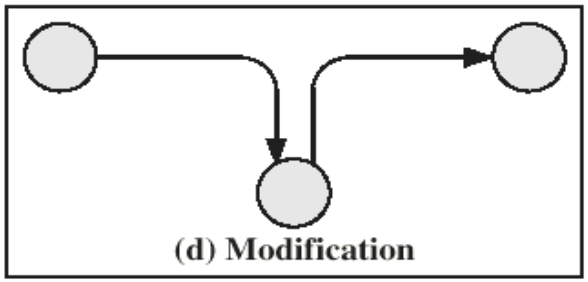
- Integrity can be enforced by setting User Access Controls (UAC) that define which users have to be given what permissions in the database.
- For example, data related to employee information is stored in a database.
  - An employee may have permission for viewing the records and altering only part of information like his contact details, whereas a person in the human resources department will have more privileges.
  - Students may be allowed to see their grades, yet not allowed to modify it.

Security Attacks









Security Attacks

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity

Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, or destruction; be notarized or witnessed

Security Services

Definition

- X.800

  "a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers"

- RFC 2828

  "a processing or communication service provided by a system to give a specific kind of protection to system resources"

Security Services (X.800)

OSI Security Architecture has been defined in the ITU-T recommendation X.800

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication
- **Availability Service**

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.

Authentication

- 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.

Authentication

- Two specific authentication services are defined in X.800
  - **Peer Entity Authentication**
  - **Data Origin Authentication**

- **Peer Entity Authentication-** A security service that verifies an identity claimed by or for a system entity in an association.
  - With peer entity authentication, the security service verifies that the identity of a peer in an association such as a session between a sender and receiver is the identity claimed.
  - It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.
  - Logging in with a password
  - Gaining access via biological identity verification
    - DNA identification, retinal scan, finger/hand print identification
  - Access via audio voice identification

- **Data Origin Authentication -** In a connectionless transfer, provides assurance that the source of received data is as claimed.
- Data origin authentication verifies that the original source of a received message is as claimed, but, unlike peer entity authentication, no association between the sender and receiver is required.
- With data origin authentication, a target receiver can verify the identity of a message as belonging to the original message creator even if the message passes from its initial source through multiple participants before arriving at the target receiver.

- Use data origin authentication, which enables the recipient to verify that messages have not been tampered with in transit (data integrity) and that they originate from the expected sender (authenticity).

Access Control

- Access control is the ability to limit and control the access to host systems and applications via communications links.
- Each entity trying to gain access must first be authenticated.
  - Who can access
  - Under what conditions
  - What they are allowed to do

Data Confidentiality

- the protection of data from unauthorized disclosure.
- It has four specific services:
  - *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 protection of selected fields within 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.

- Traffic Flow Confidentiality (TFC) mechanisms are techniques devised to hide/masquerade the traffic pattern to prevent statistical traffic analysis attacks.
- TFC adds extra padding to the packets being sent and sends dummy packets with different lengths at random intervals to conceal the actual length of the packets.
- TFC is used for extra security against attackers who might guess the type of data being sent from the length of the packet.

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 detection and recovery from any integrity violation (modification, insertion, deletion, relay) against any user data within an entire data sequence in connection-oriented communication.
  - **Connection Integrity without Recovery**
    - Detect any modification and report it
      - 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 determines whether the selected fields have been modified, inserted, deleted, or replayed..
  - **Connectionless Integrity**
    - provides for the integrity of a single data block, and detects data modification.
  - **Selective-Field Connectionless Integrity**
    - provides for the integrity of selected fields within a single data block, and determines whether the selected field is 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**
  - provides proof that the message was sent by the specified party.
- **Nonrepudiation, Destination**
  - provides proof that the message was received by the received party.

- 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.

Availability Service

- 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.

- X.800 treats availability as a property to be associated with various security services.
- 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.

Security Mechanisms

- A mechanism that is designed to detect, prevent, or recover from a security attack.
- No single mechanism that will support all services required
  - One particular element underlies many of the security mechanisms in use:
    - **cryptographic techniques**

Security Mechanisms (X.800)

- Security mechanisms are used to implement the security services.
- **Specific security mechanisms:**
  - Specific security mechanisms may be incorporated into an appropriate layer to provide some of the security services
  - OSI security architecture enumerates eight specific security mechanisms.
    - Encipherment
    - Digital signature mechanisms
    - Access control mechanisms
    - Data integrity mechanisms
    - Authentication exchange mechanisms
    - Traffic padding mechanisms
    - Routing control mechanisms
    - Notarization mechanisms

- Pervasive security mechanisms
- Security mechanisms that are not specific to any particular service area are referred to as *pervasive security mechanisms*.
    - Trusted functionality
    - Security labels
    - Event detection
    - Security audit trail
    - Security recovery

Specific security mechanisms

- *Encipherment* is used either to protect the confidentiality of data units and traffic flow information or to support or complement other security mechanisms.
- *Digital signature mechanisms* are used to provide an electronic analog of handwritten signatures for electronic documents.
  - Like handwritten signatures, digital signatures must not be forgeable; a recipient must be able to verify it, and the signer must not be able to repudiate it later.
  - But unlike handwritten signatures, digital signatures incorporate the data (or the hash of the data) that are signed.
  - Different data therefore result in different signatures even if the signatory is unchanged.

Specific security mechanisms

- *Access control mechanisms* use the authenticated identities of principals, information about these principals, or capabilities to determine and enforce access rights.
  - If a principal attempts to use an unauthorized resource, or an authorized resource with an improper type of access, the access control function rejects the attempt and may additionally report the incident for the purposes of generating an alarm and recording it as part of a security audit trail.
- *Data integrity mechanisms* are used to protect the integrity of either single data units and fields within these data units or sequences of data units and fields within these sequences of data units.

Specific security mechanisms

- *Authentication exchange mechanisms* are used to verify the claimed identities of principals.
- *strong* to refer to an authentication exchange mechanism that uses cryptographic techniques to protect the messages that are exchanged, and
- *weak* to refer to an authentication exchange mechanism that does not do so.
  - Weak authentication exchange mechanisms are vulnerable to passive and replay attacks.

Specific security mechanisms

- *Traffic padding mechanisms* are used to protect against traffic analysis attacks.
  - Traffic padding refers to the generation of spurious instances of communication, spurious data units, and spurious data within data units.
  - The aim is not to reveal if data that are being transmitted actually represent and encode information.

Specific security mechanisms

- *Routing control mechanisms* can be used to choose specific routes for data transmission.
  - Communicating systems may, on detection of persistent passive or active attacks, wish to instruct the network service provider to establish a connection via a different route.
- *Notarization mechanisms* can be used to assure certain properties of the data communicated between two or more entities, such as its integrity, origin, time, or destination.
  - The assurance is provided by a trusted third party (TTP) in a testifiable manner.

- Pervasive security mechanisms are not specific to any particular security service and are in general directly related to the level of security required.
- The OSI security architecture enumerates five pervasive security mechanisms.
- Pervasive security mechanisms
  - Trusted functionality
  - Security labels
  - Event detection
  - Security audit trail
  - Security recovery

Pervasive security mechanisms

- *Trusted functionality*
  - Any functionality that directly provides security mechanisms should be trustworthy.
- System resources may have *security labels* associated with them.
  - It is often necessary to convey the appropriate security label with data in transit.
  - A security label may be additional data associated with the data transferred (*e.g., the use of a specific key to encipher data*).

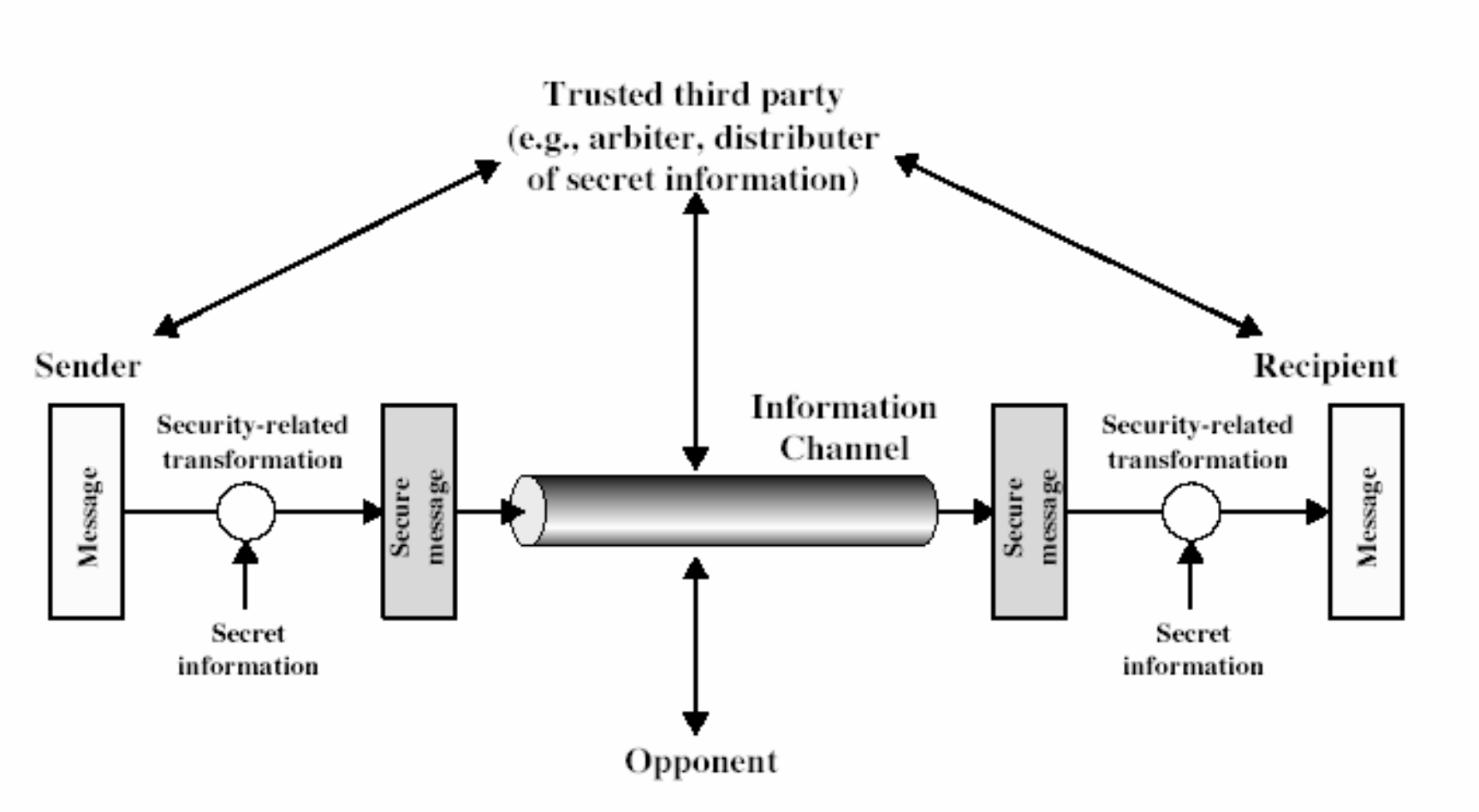
Pervasive security mechanisms

- Security-relevant *event detection* can be used to detect apparent violations of security.
- A *security audit* refers to an independent review and examination of system records and activities to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy, and procedures.
  - A *security audit trail* refers to data collected and potentially used to facilitate a security audit.
- *Security recovery* deals with requests from mechanisms such as event handling and management functions, and takes recovery actions as the result of applying a set of rules.

Relationship between Security Services and Mechanisms

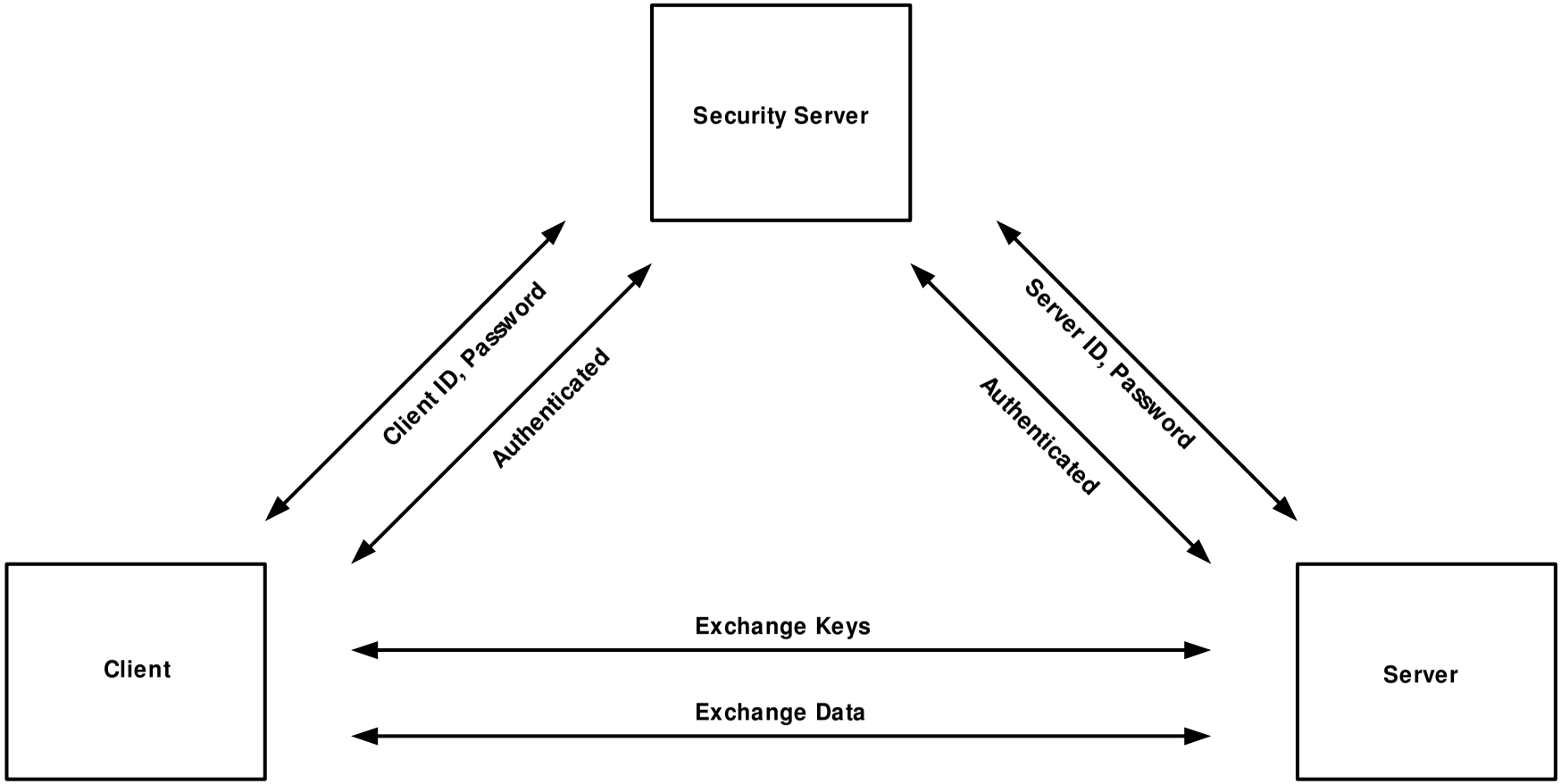
Security Service	Supporting Security Mechanisms
Peer entity authentication	encipherment, digital signature, authentication exchange
Data origin authentication	encipherment, digital signature
Access control	access control
Confidentiality	encipherment, routing control
Traffic flow confidentiality	encipherment, traffic padding, routing control
Data integrity	encipherment, digital signature, data integrity
Nonrepudiation	digital signature, data integrity, notarization
Availability	access control, authentication exchange

Model for Network Security



Trusted Third Party

- A third party may be responsible for distributing the secret information to the principals while keeping it from any opponent.
- A third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

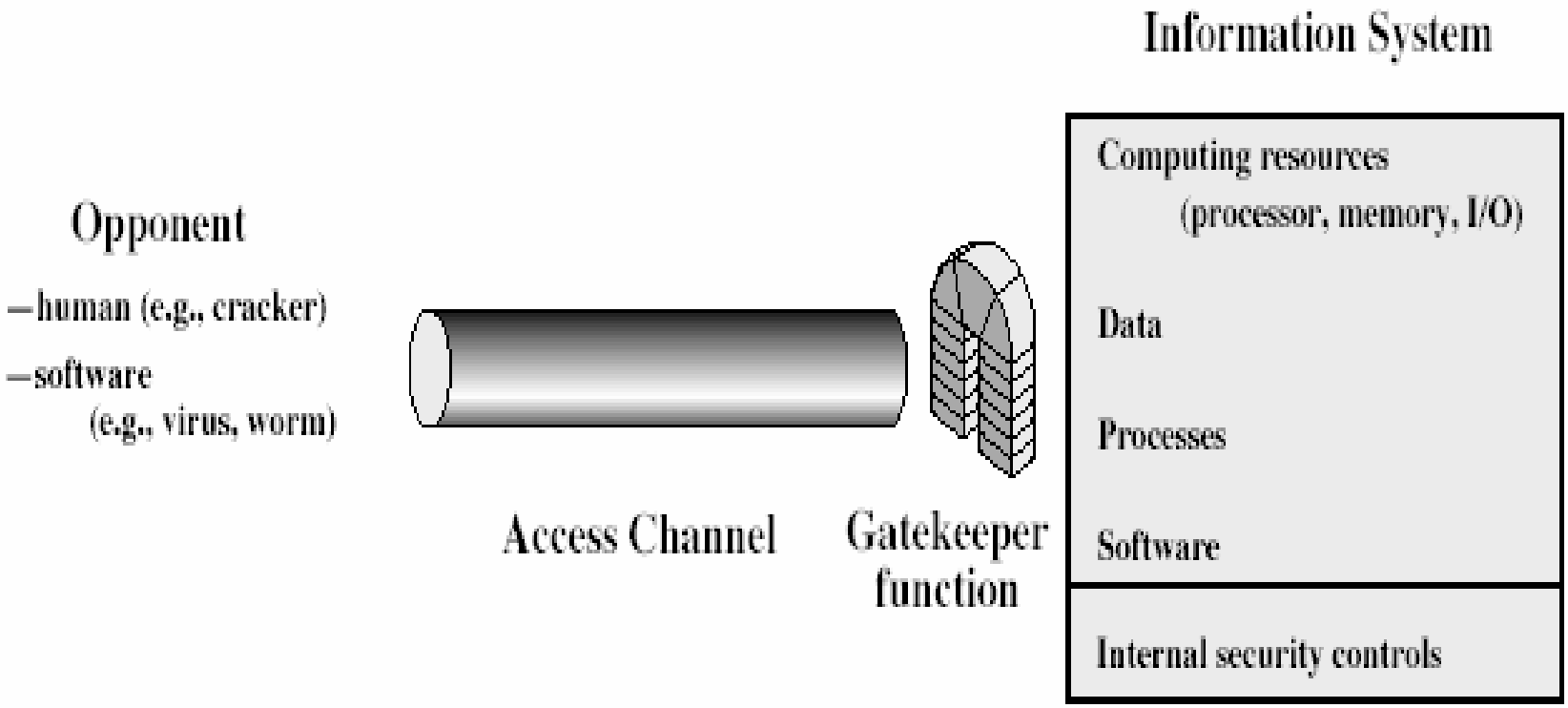


Third-Party Authentications

Model for Network Security

- using this model requires us to:
  1. Design a suitable algorithm for the security transformation
  2. Generate the secret information used by the algorithm
  3. Develop methods to distribute and share the secret information
  4. Specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Model for Network Access Security

- The security mechanisms needed to cope with unwanted access fall into two broad categories:
  - Gatekeeper function
    - Includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses and other similar attacks.
  - Internal Controls
    - Monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

Review Questions

1.1. What is the OSI security architecture?

1.2. What is the difference between passive and active security threats?

1.3. List and briefly define categories of passive and active security attacks.

1.4. List and briefly define categories of security services.

1.5. List and briefly define categories of security mechanisms.