Network Security

Introduction

Kamalika Bhattacharjee
Assistant Professor
Dept of CSE, NIT Trichy

Cryptographic Algorithms and Protocols

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

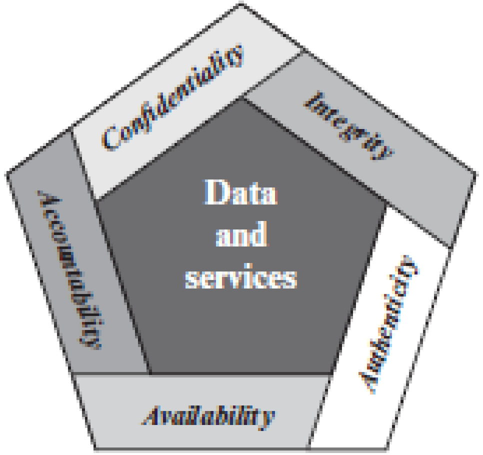
- **Asymmetric encryption:** Used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures.

- **Data integrity algorithms:** Used to protect blocks of data, such as messages, from alteration.

- **Authentication protocols:** These are schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities.

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)."* [Ref: NIST Computer Security Handbook]



CIA triad

- **Confidentiality**
- **Integrity**
- **Availability**

Computer Security

- **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 (both stored and in transmitted packets) 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.

Computer Security

- **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.*
  - 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.

Security Objectives

- **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.*

Breach of Security Levels

- **Low:** A limited adverse effect on organizational operations, organizational assets, or individuals
  - Ex: result in minor damage to organizational assets; result in minor financial loss; or result in minor harm to individuals, etc.
- **Moderate:** A serious adverse effect on organizational operations, organizational assets, or individuals :
  - Ex: significant damage to organizational assets; significant financial loss; or significant harm to individuals that does not involve loss of life or serious, life-threatening injuries, etc.
- **High:** A severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
  - Ex:: a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; major damage to organizational assets; major financial loss; or severe or catastrophic harm to individuals involving loss of life or serious, life-threatening injuries, etc.

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.

➢ The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

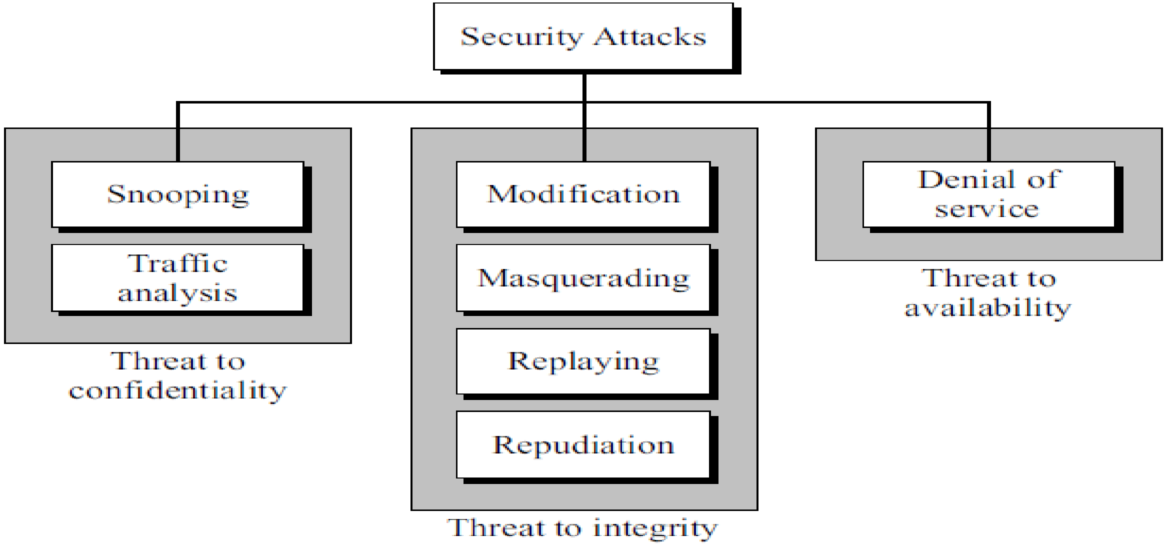
Threat and Attack

- **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.

Threat and Attack

Taxonomy of attacks with relation to security goals

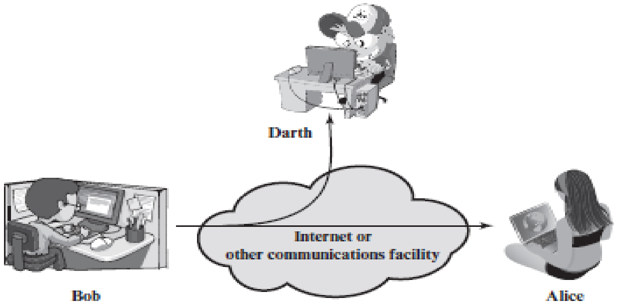


Passive Attacks

- Nature of eavesdropping on, or monitoring of, transmissions.
- The goal of the opponent is to obtain information that is being transmitted

- **Release of message contents**. We would like to prevent an opponent from learning the contents of these transmissions.
- **Traffic analysis:** An opponent might still be able to observe the pattern of encrypted messages.
  - Can determine location and identity of communicating hosts and observe the frequency and length of messages being exchanged.
  - useful in guessing the nature of the communication taking place

- Passive attacks are very difficult to detect
- It is feasible to prevent the success of these attacks, usually by means of encryption.
- Emphasis is on prevention rather than detection.

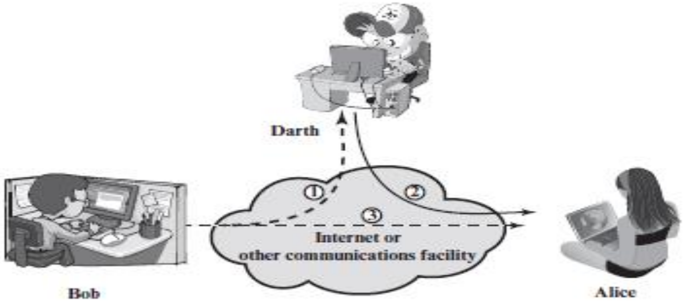


(a) Passive attacks

Active Attacks

- A **masquerade** takes place when one entity pretends to be a different entity. It usually includes one of the other forms of active attack. (Path 2 active)
- **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect. (Paths 1, 2, 3 active)
- **Modification of messages:** some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized. (Paths 1, 2 active)
- **Denial of service** prevents or inhibits the normal use or management of communications facilities (path 3 active).

  ➢ Goal is to detect active attacks and to recover from any disruption or delays caused by them

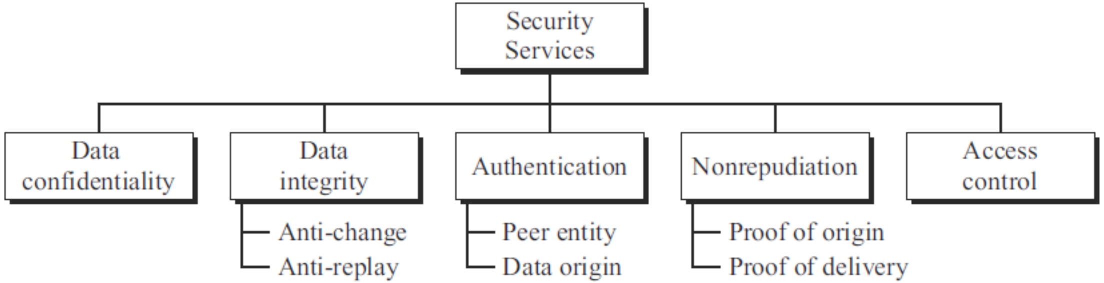


(b) Active attacks

Security Services

- [X.800] 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.
    - *five categories and fourteen specific services*

- [RFC 4949] 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.



Authentication

- The assurance that the communicating entity is the one that it claims to be.
- **Peer Entity Authentication:** Provides for the corroboration of the identity of a peer entity in an association.
    - Two entities are considered peers if they implement to same protocol in different systems; used in association with a logical connection to provide confidence in the identity of the entities connected.
- **Data-Origin Authentication:** Provides for the corroboration of the source of a data unit. In a connectionless transfer, provides assurance that the source of received data is as claimed.
    - Supports applications like electronic mail, where there are no prior interactions between the communicating entities.

Access Control

- It 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.

Data Confidentiality

- Confidentiality is the protection of transmitted data from passive attacks.
- **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:** 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.

Availability Service

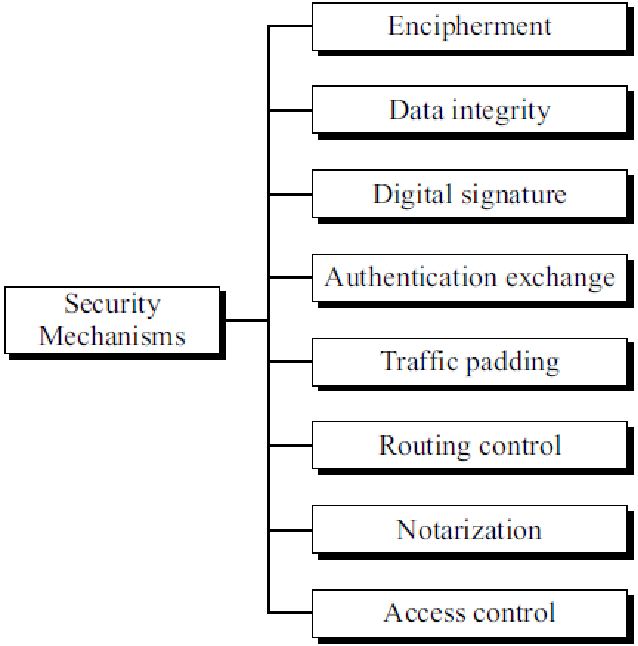
- Both X.800 and RFC 4949 define availability to be the property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.
- Some of the attacks on loss of or reduction in availability are amenable to automated countermeasures, such as authentication and encryption, whereas others require some sort of physical action to prevent or recover from loss of availability of elements of a distributed system.
- [X.800] Availability is 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

- Incorporated into the appropriate protocol layer to provide OSI security services.
- Recommended by ITU-T (X.800)

- Encipherment: hiding or covering data, can provide confidentiality. Techniques: cryptography and steganography
- *Cryptography: concealing the contents of a message by enciphering*
- *Steganography: concealing the message itself by covering it with something else*
- Data integrity mechanism: appends to the data a short *checkvalue* that has been created by a specific process from the data itself. Integrity of data has been preserved is newly calculated *checkvalue* by receiver is same as received

Specific Security Mechanisms



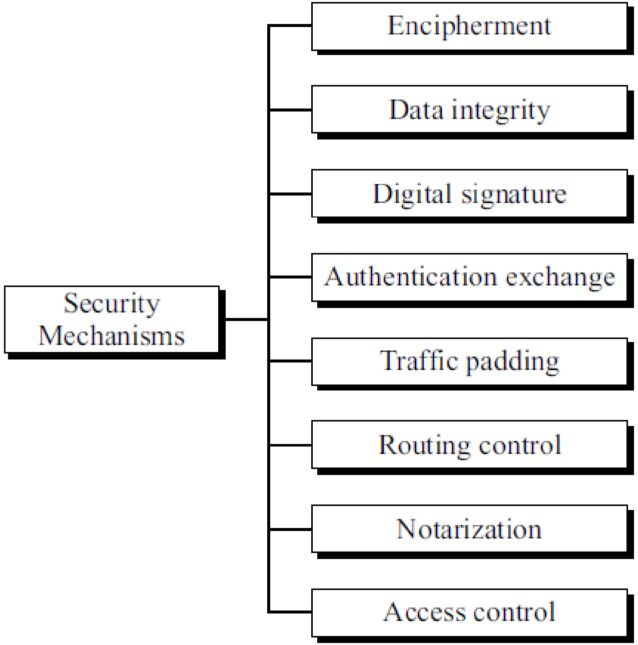
Security Mechanisms

- A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.
- Sender uses private key, receiver uses sender’s public key to prove that the message is indeed signed by the sender who claims to have sent the message.

- Authentication exchange: two entities exchange some messages to prove their identity to each other.

- Traffic padding: inserting bogus data into the data traffic to thwart adversary’s attempt to use traffic analysis

Specific Security Mechanisms



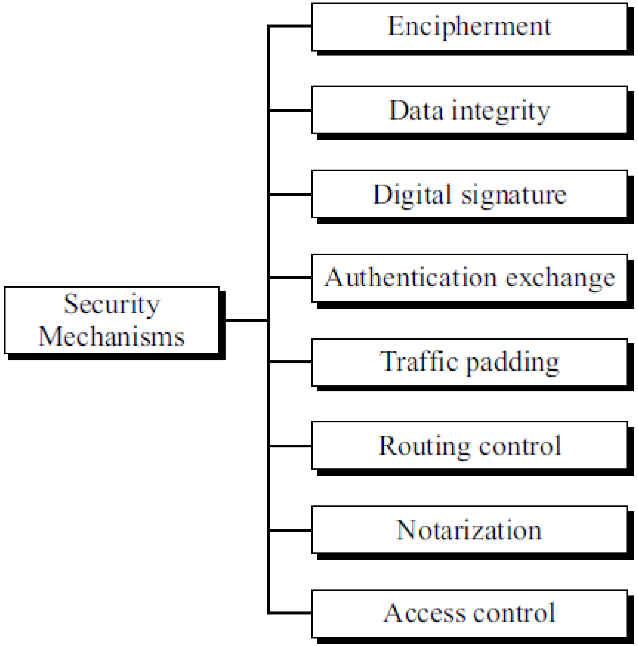
Security Mechanisms

- Routing control: selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.

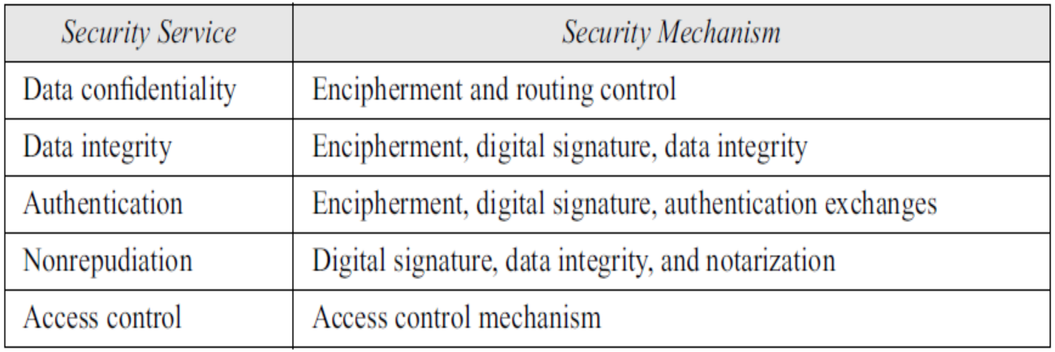
- Notarization: selecting a third trusted party to control the communication between two entities. Can be done, for example, to prevent repudiation.

- Access control uses methods to prove that a user has access right to the data or resources owned by a system.
  Examples of proofs: passwords and PINs.

Specific Security Mechanisms

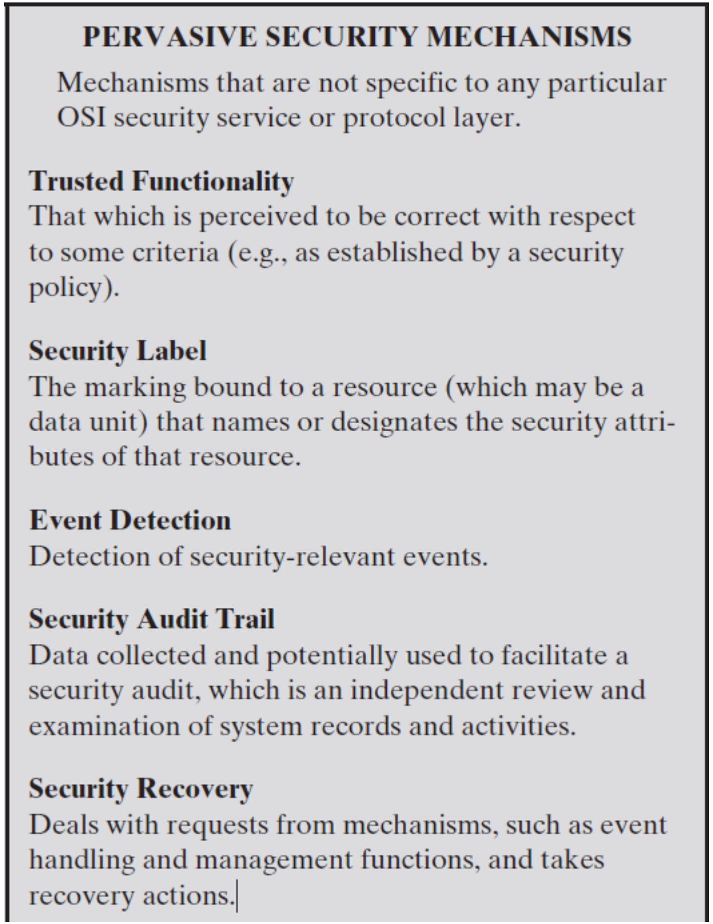


Security Service vs Mechanisms



Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

[Ref: X.800]



PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

Trusted Functionality
That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

Security Label
The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection
Detection of security-relevant events.

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.

Security Recovery
Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Fundamental Security Design Principles

- Economy of mechanism *as simple and small as possible → easier to test and verify thoroughly*
- Fail-safe defaults *access decisions should be based on permission rather than exclusion*
- Complete mediation *every access must be checked against access control mechanism*
- Open design *security mechanism should be open to public scrutiny rather than secret*
- Separation of privilege *Multiple privilege attributes are required to achieve access to a restricted resource*
- Least privilege *every process/user of the system should operate using the least set of privileges necessary to perform the task → role based access control*
- Least common mechanism *minimize the functions shared by different users → mutual security*
- Psychological acceptability *security mechanisms should be transparent to users or at most introduce minimal obstruction.*

Fundamental Security Design Principles

- Isolation
  - public access systems should be isolated from critical resources (data, processes, etc.) to prevent disclosure or tampering → Physical and logical isolation
  - Processes & files of individual users should be isolated from one another except explicitly desired
  - security mechanisms should be isolated in the sense of preventing access to those mechanisms
- Encapsulation
  - isolation based on object oriented functionality
- Modularity
  - development of security functions as separate, protected modules → Cryptographic module
  - modular architecture for mechanism design and implementation → scalable & upgradable
- Layering: *defense in depth* multiple, overlapping protection approaches
- Least astonishment a program or user interface should always respond in the way that is least likely to astonish the user

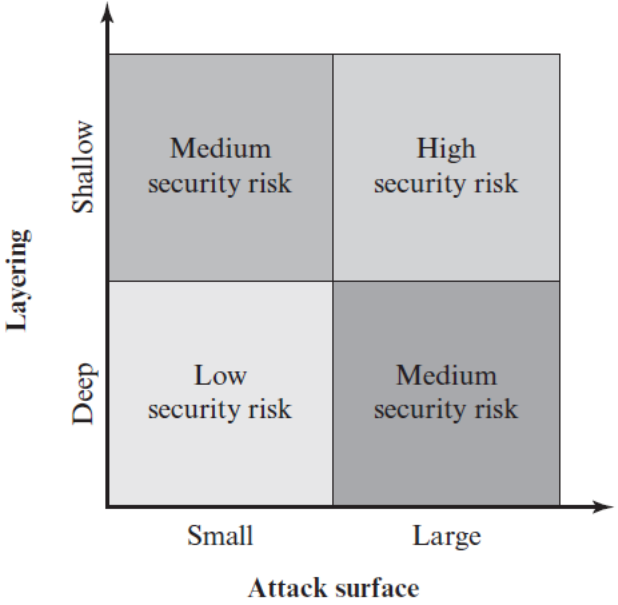
Attack Surfaces

Reachable and exploitable vulnerabilities in a system

- **Network attack surface**
  - Vulnerabilities over an enterprise network, wide-area network, or the Internet.
  - Ex: network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks.
- **Software attack surface**
  - vulnerabilities in application, utility, or operating system code. Ex: Web server software
- **Human attack surface**
  - vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

Attack Surfaces Analysis

- Useful technique for assessing the scale and severity of threats to a system
- A systematic analysis of points of vulnerability makes developers and security analysts aware of where security mechanisms are required.
- Once an attack surface is defined, designers may be able to find ways to make the surface smaller, thus making the task of the adversary more difficult.
- Provides guidance on setting priorities for testing, strengthening security measures, and modifying the service or application.



Layering	Small	Large
Shallow	Medium security risk	High security risk
Deep	Low security risk	Medium security risk

- Use of layering, or defense in depth, and attack surface reduction complement each other in mitigating security risk

Attack Tree

- A branching, hierarchical data structure representing a set of potential techniques for exploiting security vulnerabilities.

- Goal of the attack is represented as the root node
- The ways that an attacker could reach that goal are iteratively and incrementally represented as branches and subnodes of the tree
- Each subnode defines a subgoal, and each subgoal may have its own set of further subgoals, and so on
- Leaf nodes, represent different ways to initiate an attack

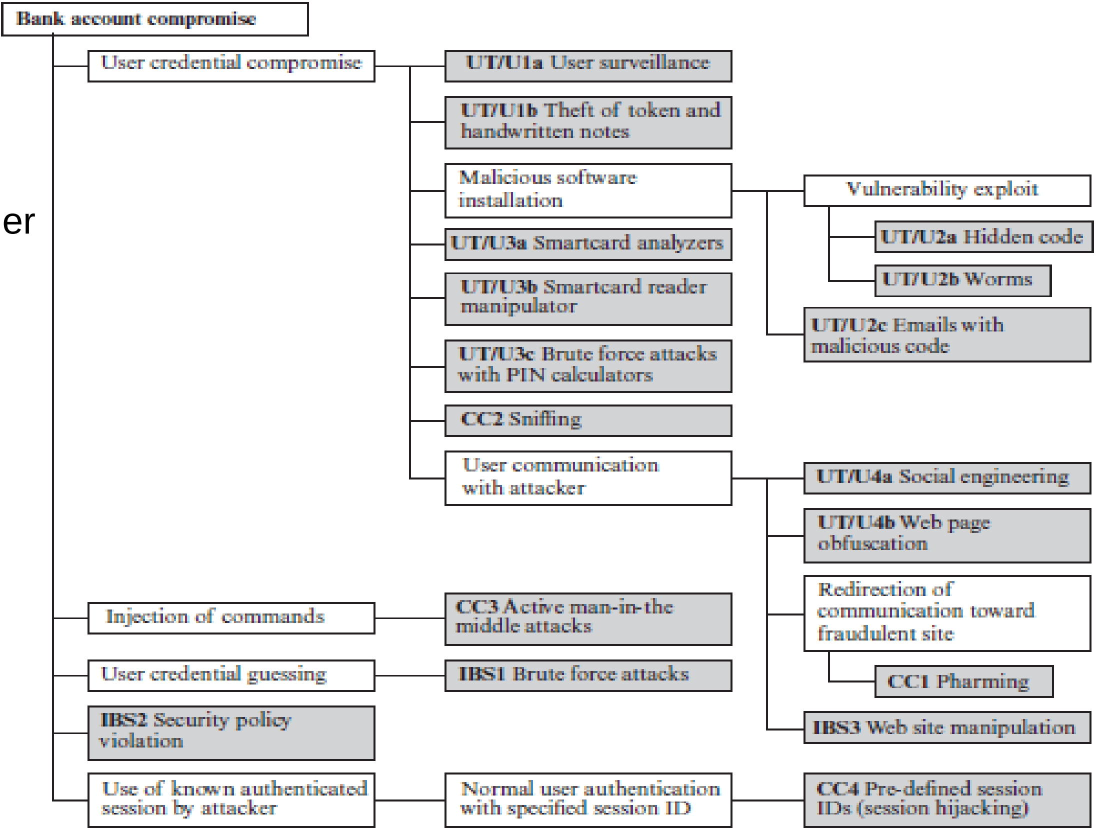
- The motivation for the use of attack trees is to effectively exploit the information available on attack patterns

Attack Tree Example

- **User terminal and user (UT/U):** attacks target the user equipment, including the tokens that may be involved, such as smartcards or other password generators, as well as actions of user

- **Communications channel (CC):** attack focuses on communication links

- **Internet banking server (IBS):** offline attacks against the servers that host the Internet banking application



Bank account compromise

User credential compromise

UT/U1a User surveillance

UT/U1b Theft of token and handwritten notes

Malicious software installation

Vulnerability exploit

UT/U2a Hidden code

UT/U2b Worms

UT/U2c Emails with malicious code

UT/U3a Smartcard analyzers

UT/U3b Smartcard reader manipulator

UT/U3c Brute force attacks with PIN calculators

CC2 Sniffing

User communication with attacker

UT/U4a Social engineering

UT/U4b Web page obfuscation

Redirection of communication toward fraudulent site

CC1 Pharming

IBS3 Web site manipulation

Injection of commands

CC3 Active man-in-the middle attacks

User credential guessing

IBS1 Brute force attacks

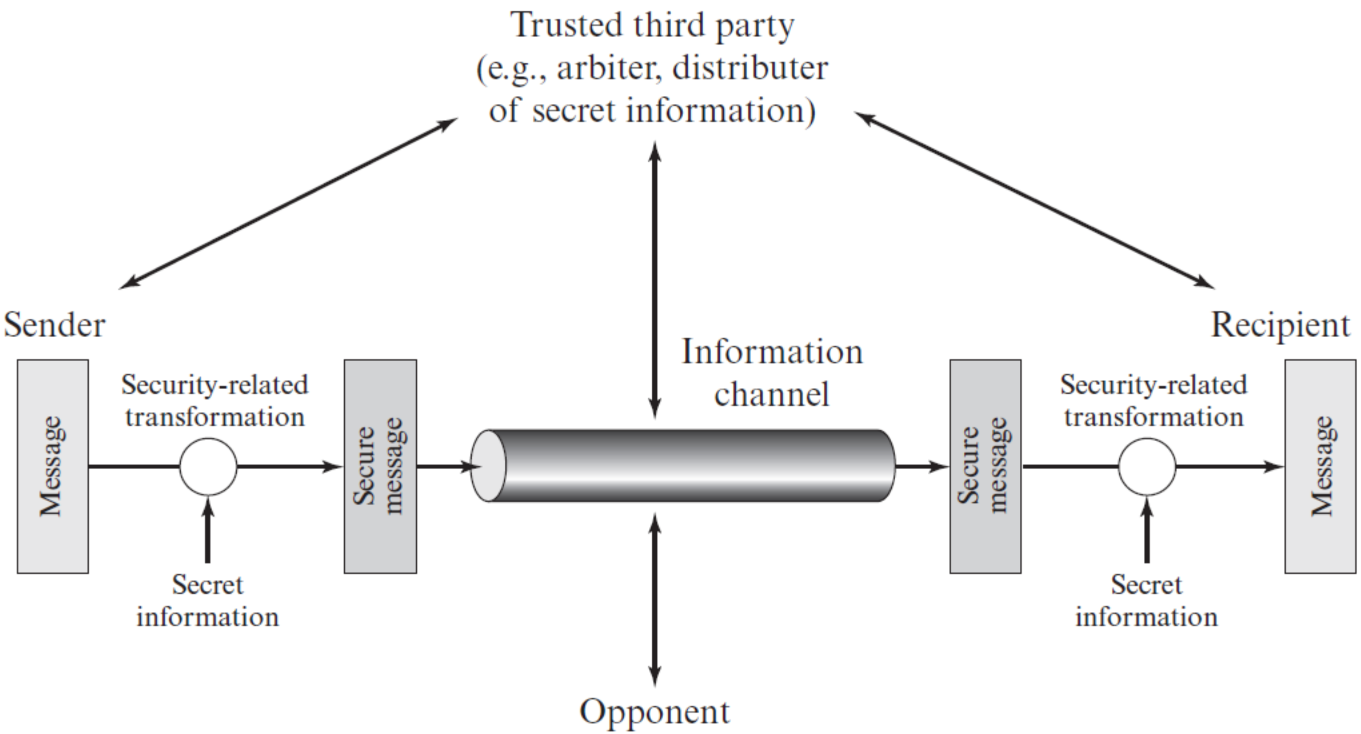
IBS2 Security policy violation

Use of known authenticated session by attacker

Normal user authentication with specified session ID

CC4 Pre-defined session IDs (session hijacking)

Model for Network Security



Model for Network Security

Basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.

2. Generate the secret information to be used with the algorithm.

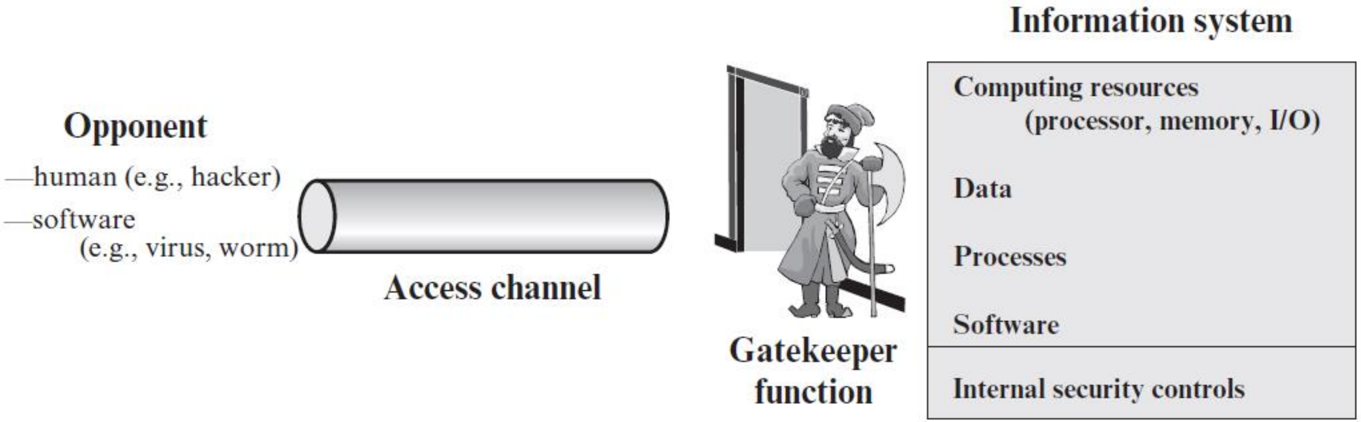
3. Develop methods for the distribution and sharing of the secret information.

4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

Network Access Security Model

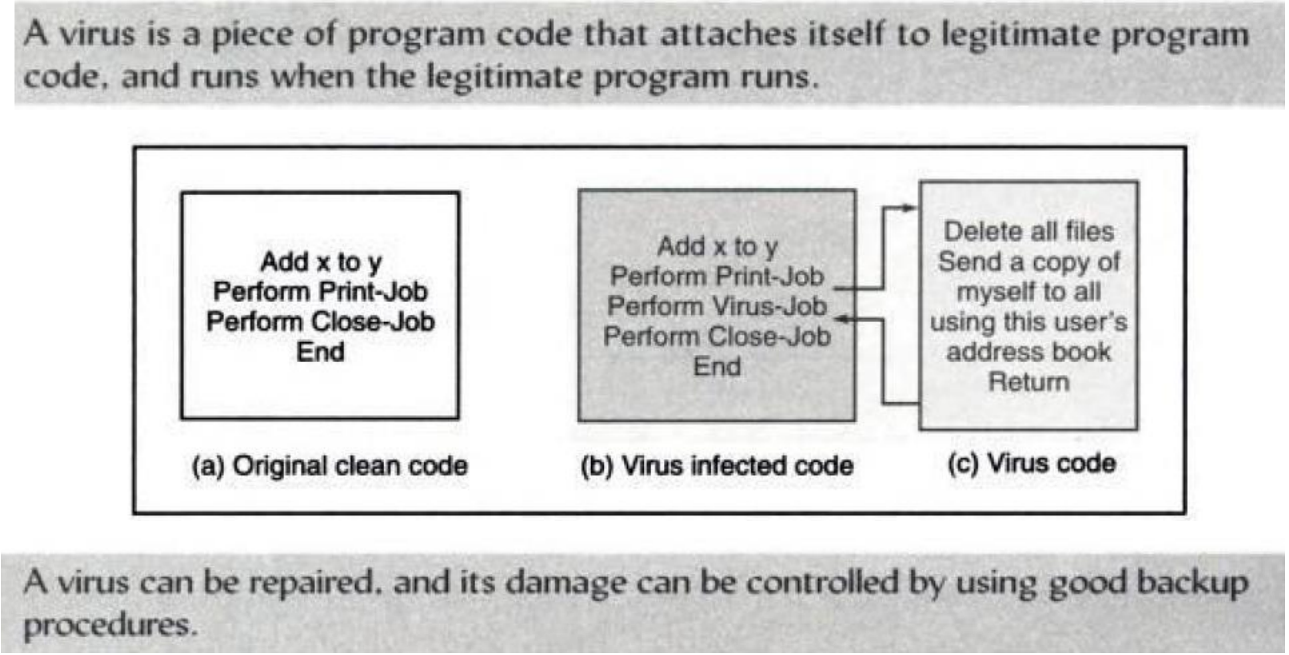
- Hackers
- **Information access threats:** Intercept or modify data on behalf of users who should not have access to that data.
- **Service threats:** Exploit service flaws in computers to inhibit use by legitimate users.

- Security Attacks can happen in Application Level or Network Level



Virus

- Virus: can launch attack at any level



A virus is a piece of program code that attaches itself to legitimate program code, and runs when the legitimate program runs.

(a) Original clean code

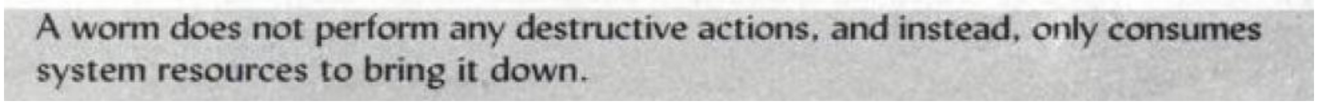
(b) Virus infected code

(c) Virus code

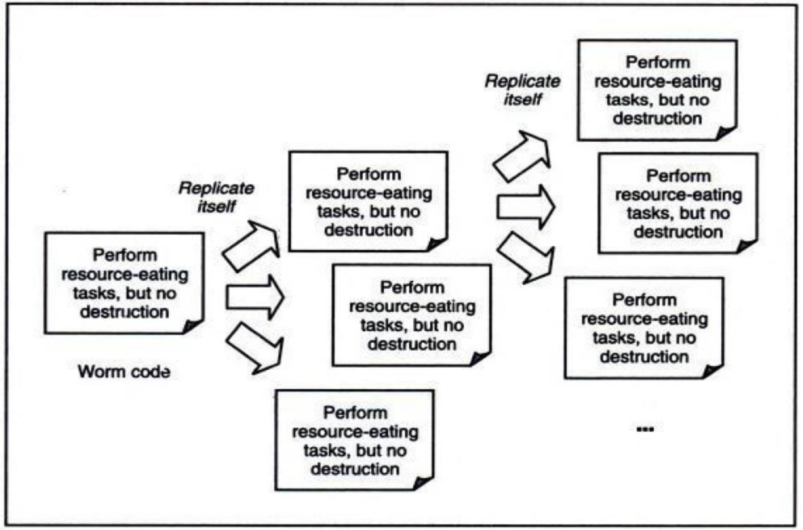
A virus can be repaired, and its damage can be controlled by using good backup procedures.

Worm

- Worm does not modify a program, only replicates itself again and again



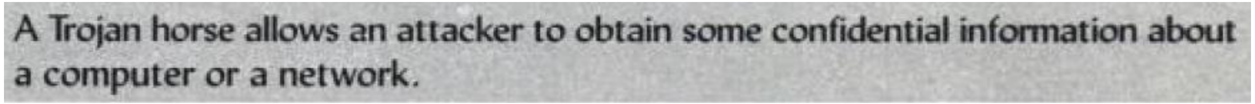
A worm does not perform any destructive actions, and instead, only consumes system resources to bring it down.



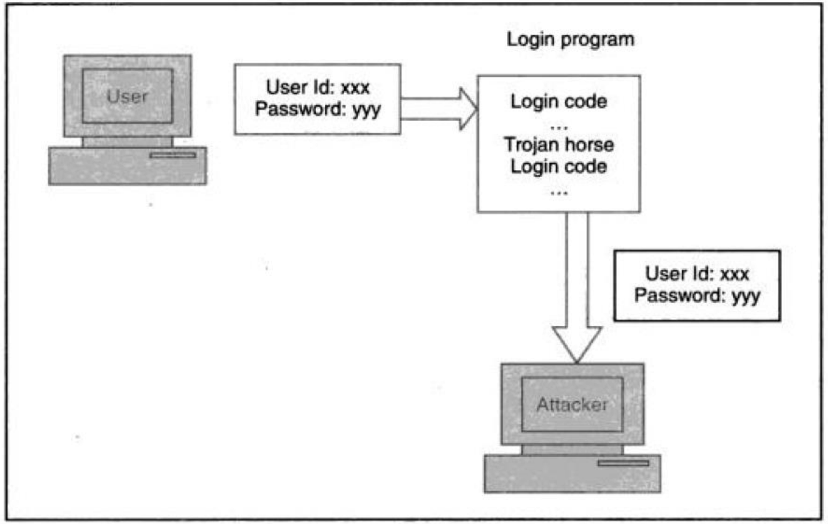
Perform resource-eating tasks, but no destruction
Worm code
Replicate itself
Perform resource-eating tasks, but no destruction
Perform resource-eating tasks, but no destruction
Perform resource-eating tasks, but no destruction
Replicate itself
Perform resource-eating tasks, but no destruction
Perform resource-eating tasks, but no destruction
Perform resource-eating tasks, but no destruction
...

Trojan Horse

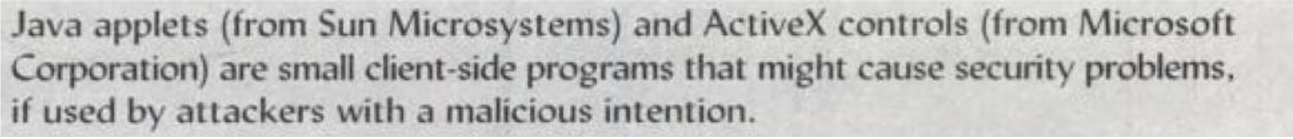
- Does not modify code or replicate; sits silently to reveal confidential info



A Trojan horse allows an attacker to obtain some confidential information about a computer or a network.

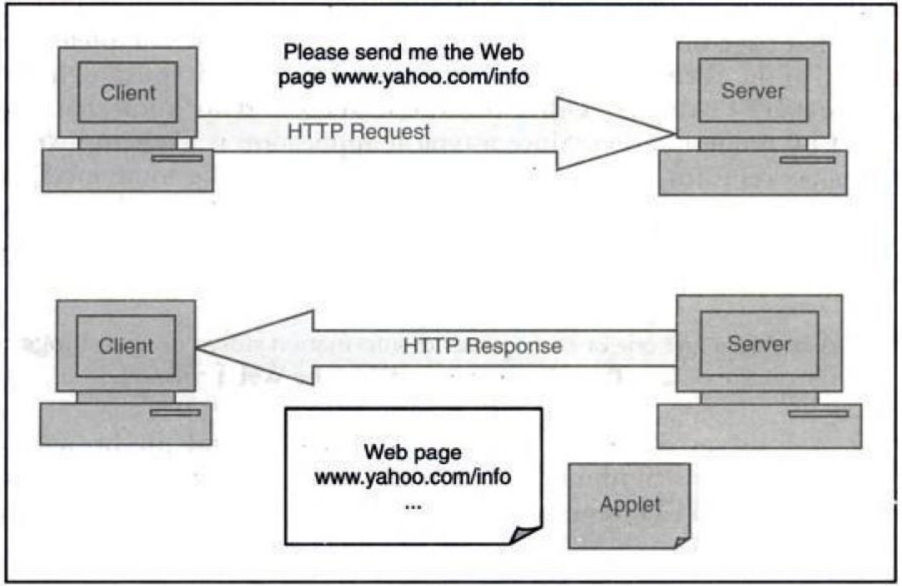


Applets and ActiveX controls



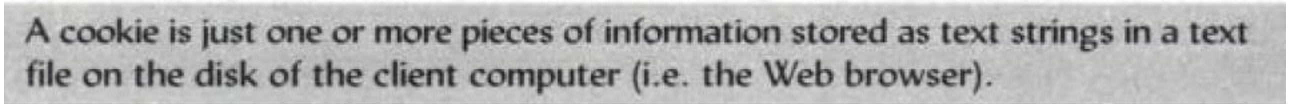
Java applets (from Sun Microsystems) and ActiveX controls (from Microsoft Corporation) are small client-side programs that might cause security problems, if used by attackers with a malicious intention.

- Programs executed inside browser
- Used to do some processing at client side or periodically request some information from the server using *client pull*

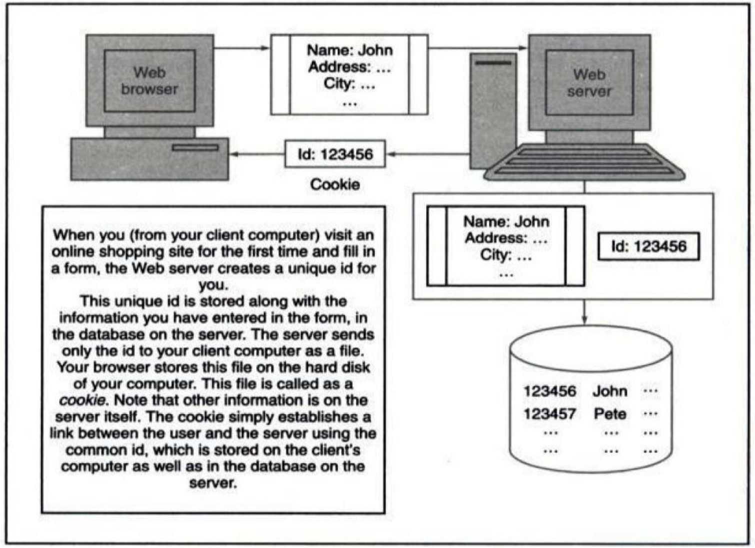

Client
Please send me the Web page www.yahoo.com/info
HTTP Request
Server
Client
HTTP Response
Server
Web page www.yahoo.com/info ...
Applet

Cookies

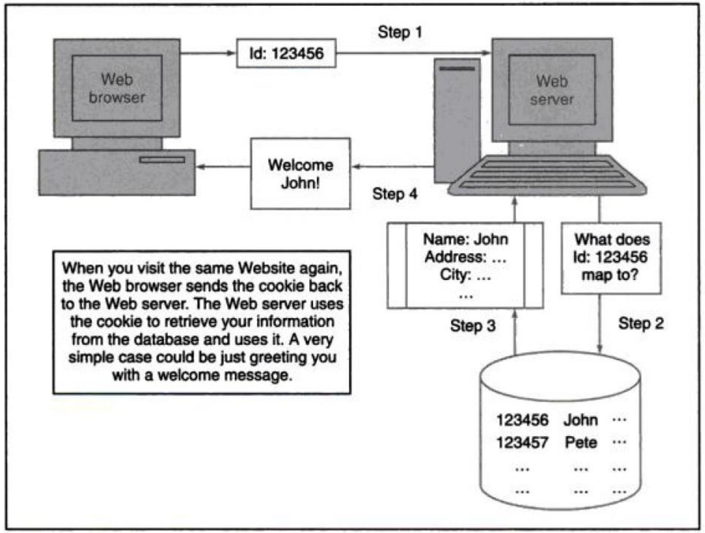
- HTTP is stateless; cookies are used for identification purpose to maintain state information



A cookie is just one or more pieces of information stored as text strings in a text file on the disk of the client computer (i.e. the Web browser).



When you (from your client computer) visit an online shopping site for the first time and fill in a form, the Web server creates a unique id for you.
This unique id is stored along with the information you have entered in the form, in the database on the server. The server sends only the id to your client computer as a file. Your browser stores this file on the hard disk of your computer. This file is called as a *cookie*. Note that other information is on the server itself. The cookie simply establishes a link between the user and the server using the common id, which is stored on the client's computer as well as in the database on the server.



When you visit the same Website again, the Web browser sends the cookie back to the Web server. The Web server uses the cookie to retrieve your information from the database and uses it. A very simple case could be just greeting you with a welcome message.