DISTRIBUTED OPERATING SYSTEMS

UNIT V

SECURITY

Security in Distributed Operating Systems

The objective of any security system is the ability to keep a secret. This is as true automated systems as much as it is for people. It is as important to keep the information secret when it is stored as well as when it sent over a network.

A secure system is the one that can be trusted to keep secret, and important word is "trusted". Trusts can be defined as a confident reliance on the integrity, honesty or justice of another.

Trust refers to the ability of the application to perform actions with integrity and to perform its functions on a continuing basis.

The Security goals of a computer system re decided by its security policies and the methods used to achieve these goals are called security mechanisms.

Distributed system security is fundamentally more complex than stand-alone system security. Current computer security concepts assume that trusts is assigned to a distributed system element on the basis of viewpoint. This security mechanism for distributed file systems solves many of the performance and security problems in existing systems today.

The Common Goals of Computer Security:

1. **Secrecy-Information with in system must be accessible only to authorized users.**
2. **Privacy-Misuse of information must be prevented.**
3. **Authenticity-When a user receives some data, the user must be able to verify its authenticity.**
4. **Integrity-Information within the system must be protected against accidental destruction or intentional corruption by an unauthorized user.**

Communication Security-In a distributed system, the communication channels that are used to connect the computers are normally exposed to attacks who may try to breach the security of the system by observing, modifying or disturbing the communications.

Wireless networks are even more vulnerable to monitoring by intruders because anyone with a scanner can pluck the radio signals out of the air without being detected.

Communication security safeguards against unauthorized tampering of information while it's being transmitted from one computer to another through the communicational channels.

Two other aspects of communication security are Authenticity of communicating entities and integrity of messages.

Potential Attacks to Computer Systems

The term Intruder or attacker is commonly used to refer to a person or program trying to obtain unauthorized access to data or a resource of a computer system.

An intruder may be a threat to computer security in many ways that are broadly classified into two categories,

- Passive Attacks
- Active Attacks

Passive Attacks

- Browsing
- Inferencing
- Masquerading

Intruder: person/program vying for unauthorized access to data. Intruder access unauthorized information from a computer system but not cause harm to the system.

Browsing: Intruders here attempt to read stored files, traverse message packet on the network, access other process memory, etc.

Inferencing: The intruder records and analyses past activities and access methods and uses this information to draw inferences

Masquerading: an intruder Masquerades as an authorized user or a program to gain access to unauthorized data or resource.

Active Attacks

- Virus
- Worm
- Logic bomb
- Integrity attack
- Authenticity attack
- Delay attack
- Replay attack
- Denial attack

Virus: is a small computer program that needs to be executed by either running it or having it loaded from boot sector of a disk.

• An intruder writes a useful program and attaches the virus to it, such as when the program executed the virus is also executed.

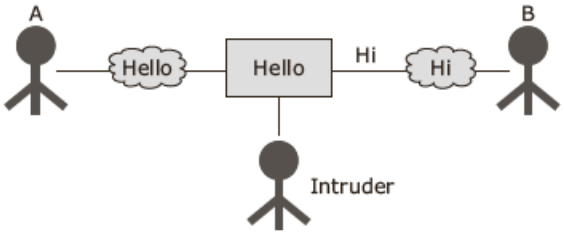
Worm: A worm is a small piece of software the uses computer network and security holes to replicate itself.

Virus vs worm

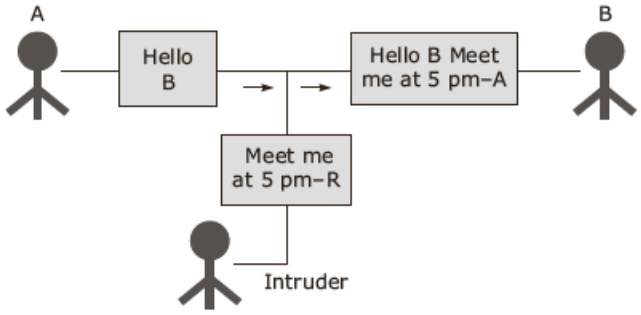
Criteria of differentiation	Virus	Worm
Program	Program fragment	Complete program
Existence and execution	Does not exist nor can execute independently, needs a host program	Exists and executes independently
Spread	From one program to another	From one computer to another

Logic bomb: is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. When 'exploded' may be designed to display a message, delete or corrupt data.

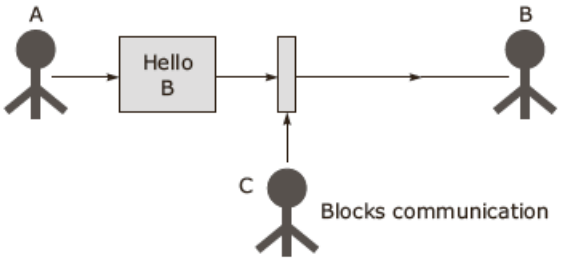
Integrity attack: An intruder can change the message while it is traveling in the communication channel and the receiver may interpret it as original message.



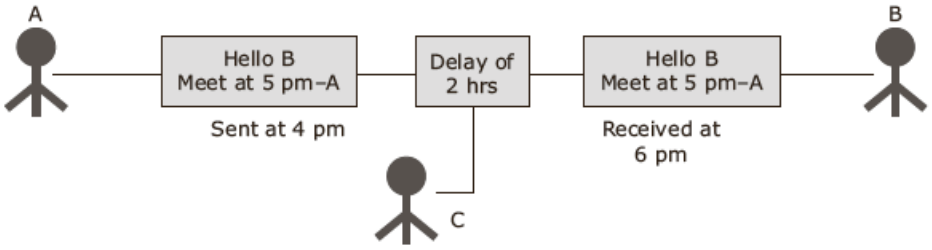
Authenticity attack: An intruder can illegally connect to computer network , impersonate and insert bogus message with valid address in the system . These will then be delivered as genuine message.



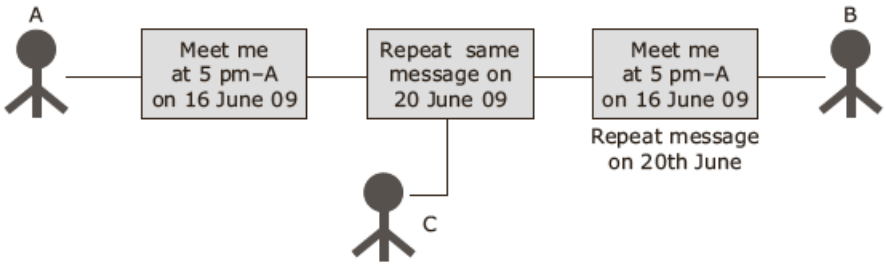
Denial attack: an intruder might partly or completely block communication path between two processes.



Delay attack: an intruder can delay the message delivery that can make it useless to receive if it is received late.



Replay attack: an intruder retransmit an old message that is accepted as new message by the receiver.

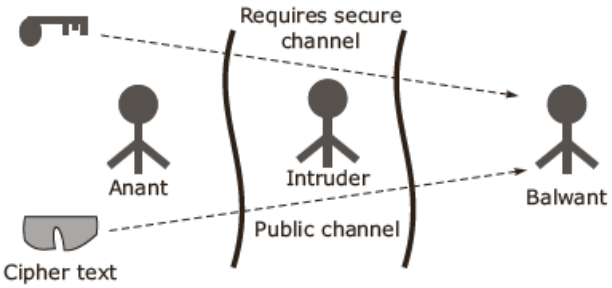


Confinement problems

Prevention of such leakage of information is called confinement problem.

The following types of channels can be used by a program to leak information:

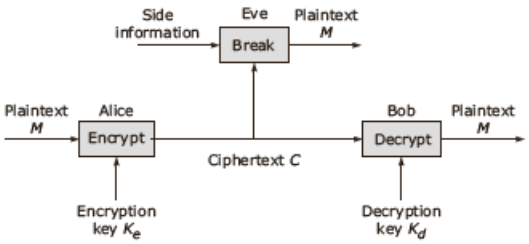
1. Legitimate channel
2. Storage channel
3. Covert channel



Cryptography

Cryptography: is defined as a means of protecting private information against unauthorized access in case where physical security is difficult to achieve.

Two basic operations: encryption and decryption.



There are two board classes of cryptosystem based on whether the encryption and decryption keys are the same namely symmetric and asymmetric systems.

- Symmetric cryptosystem: uses the same key for both encryption decryptions.
- Asymmetric cryptosystem: the key for both encryption decryptions are different but they form unique.

- The encryption algorithm has following form:

$$C = E(P, K_e)$$

Where P =plaintext to be encrypted
K_e=encryption key
C =resulting ciphertext

- The decryption algorithm has following form:

$$P = D(C, K_d)$$

Where C = ciphertext to be decrypted
K_d= decryption key
P =resulting plaintext

Secure channels

A secure channel protects senders and receivers from against:
1. Fabrication
2. Modification.
3. Interception.

To have a secure communication we should have:
1. An authentication of communicating parties.
2. Ensure data integrity and confidentiality

Authentication

Deals with verifying the identity of users before allowing them to access a resource. This mechanism prevent unauthorized user from accessing the system resource.

Identification: is the process of claiming a certain identity by a user
Verification: is the process of verifying the user's claimed identity.

Authentication in distributed system can be categorized into following:

1. User login authentication
2. One-way authentication of communicating entities
3. Two-way authentication of communicating entities

User login authentication

Deals with verifying the identity of the user by the system while logging in.
• Correct user identification during login becomes essential since all access control decisions and accounting functions depend on this identity.
• For ensuring security, a password-based authentication system must have the following mechanisms:

1. Maintain secrecy of passwords
2. Make passwords difficult to guess
3. Limit damage due to a compromised password

1-Maintain secrecy of passwords:

- User must keep the password secret from external world.
- Hiding the character displayed when the user logs in to the terminal.
- Password table is protected and accessible only to the Authentication program and the entries in password table are encrypted.

2-Make passwords difficult to guess:

To keep passwords secret in distributed environment:

A. Use long passwords
B. Include special character in password
C. Avoid passwords used earlier

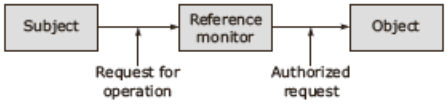
3-Limit damage due to a compromised password:

The users must change the password periodically and this change should not make password guessing easy.

Access Control

- General Issues in Access Control.
- Firewalls.
- Secure Mobile Code.

General Issues in Access Control



Subjects

Can best be thought of as being processes acting on behalf of users, but can also be objects that need the services of other objects in order to carry out their work.

Objects

Can be hardware objects (*e.g.* CPU, memory segment and printers) or software objects (*e.g.* file and program).

Reference monitor

Records which subject may do what, and decides whether a subject is allowed to have a specific operation carried out.

Access Control Matrix

- A common approach to modelling the access rights of subjects with respect to objects.
- Each subject is represented by a row in this matrix, each object is represented by a column.
- Disadvantages :

Considering that a system may easily need to support thousands of users and millions of objects that require protection Many entries in the matrix will be empty: a single subject will generally have access to relatively few objects.

Design issues

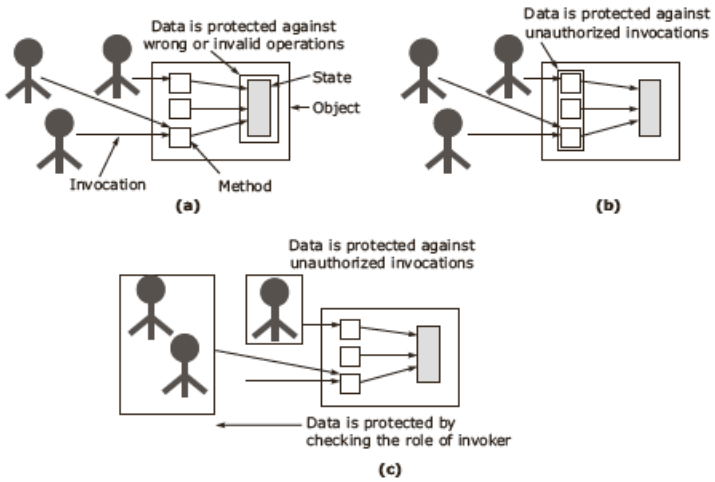
The major design issues in building secure distributed system are:

- Focus of control.
- Layering of security mechanism.

Focus of control

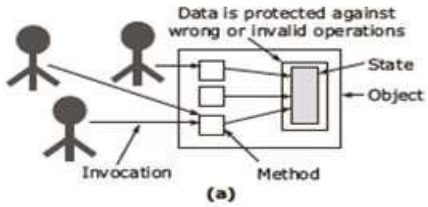
The are three approaches that can be followed to protect a distributed application:-

- Protection against invalid operations on secure data
- Protection against unauthorized invocations
- Protection against unauthorized users



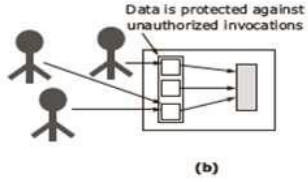
Protection against invalid operations on secure data

Protecting the data that is associated with the application,
i.e. insure data integrity .



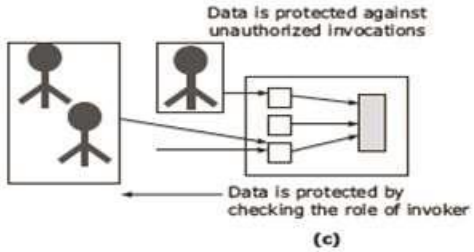
Protection against unauthorized invocations

Specifying which operations can be invoked and by whom and when the data resources are accessed.



Protection against unauthorized users

• Specifying which users should be allowed to access the application irrespective of the operation to be performed.
• Roles are defined for the users and once that role is verified , access to the resource is either granted or denied.



Layering of security mechanism

One of important aspect of designing secure system is to decide which level the security mechanism should be placed.
Security mechanism is normally placed in middleware in a distributed system.

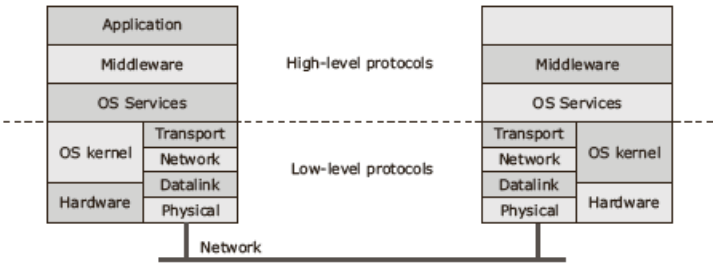


Figure 10-5 Layered organization of a distributed system