Security and Protection

1

Outline

- Design Principles of Security
- Domain Protection Mechanism
- Access Metrics Mechanism
- Access Control List
- Trojan Horse, Trap Door, Virus and Warms program threats

2

Design Principles of Security

Section - 1

3

Design Principles of Security

- Principles of least privileges:
  - This principle states **how the privileges are to be granted to a subject**.
  - A **subject should be given only those privileges that it requires** for completing a task.
  - For example, if a subject requires append rights to an object then it must be given only the append rights and not the write rights.
- Principles of fail safe defaults:
  - This principle states that **unless the subject is given explicit access to the object it should be denied access to that object**.
  - This means that the **default access to object is none**.
  - All the access **rights should be given explicitly granted**.
- Principle of economy of mechanisms:
  - This principle states that **security mechanism should be as simple as possible**.
  - If **design is simple** there are **fewer chances for errors**.
  - The checking and testing procedure becomes simpler.

4

Design Principles of Security

- Principles of complete mediation:
  - This principle states that **all the accesses to object be checked in order to ensure that they are allowed**.
  - Whenever a subject attempts to read an object the OS mediate the action.
  - First it determines if the subject is allowed to access the object.
  - If so it provides resources for reading the object.
  - If the subject reattempts the read operation then it checks if the subject is still allowed to read the object and then allows for reading.
- Principle of open design:
  - This principle suggests that **complexity doesn't add security**.
  - This principle states that the **security of mechanism should not depend on the secrecy of its design or implementation**.
- Principles of separation of privileges:
  - This principle states that the **access of an object should not depend only on fulfilling a single condition**.
  - There should be **multiple conditions required to grant privilege** and two or more system components work together to enforce security.

5

Design Principles of Security

- Principles of least common mechanism
  - This principle states that the **amount of mechanism common to and depending on multiple users should be kept to the minimum possible**.
- Principles of user acceptability
  - This principle states that the **mechanism used for protection should be acceptable to the users and should be easy to use**.
  - Otherwise, the user may feel a burden to follow the protection mechanism.

6

Domain Protection Mechanism

Section - 2

7

Domain Protection Mechanism

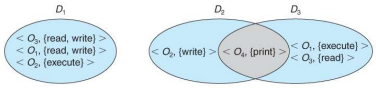
- A computer system is collections of objects and processes and these objects and processes are needed to be protected.
- Each object has unique name by which it is referred and finite set of operations that processes are allowed to carry out on it.
- There should be **some way to prohibit processes from accessing objects that they are not authorized to**.
- Operations that are possible depend on the object.

Object	Operations
CPU	Execution
File	Read, Write
Semaphore	Up, Down
Tape Drive	Read, Write, Rewound

8

Domain Structure

- A protection domain **specifies the resources that a process may access**.
- Each **domain defines a set of objects and the types of operations that may be invoked** on each object.



- A **domain** is defined as a **set of < object, {access right set} >** pairs.
- Note that **some domains may be disjoint while others overlap**.
- The association between a process and a domain may be static i.e. fixed set of resources available to a process throughout its life time or dynamic.

9

Access Metrics Mechanism

Section - 3

10

Access Metrics Mechanism

- The **model of protection can be viewed as an access matrix**, in which **columns represent different system resources and rows represent different protection domains**.
- Entries within the matrix indicate what access that domain has to that resource.

Object Domain	F1	F2	F3	Printer
D1	Read		Read	
D2				Print
D3		Read	Execute	
D4	Read Write		Read Write	

- Each cell of matrix represents set of access rights which are given to the processes of domain means each entry(i, j) defines the set of operations that a process executing in domain Di can invoke on object Oj.

11

Access Metrics Mechanism

- According to the above matrix:
  - there are four domains
  - four objects- three files(F1, F2, F3) and one printer
  - A process executing in D1 can read files F1 and F3.
  - A process executing in domain D4 has same rights as D1 but it can also write on files.
  - Printer can be accessed by only one process executing in domain D2.
  - The mechanism of access matrix consists of many policies and semantic properties. Specifically, We must ensure that a process executing in domain Di can access only those objects that are specified in row i.

Object Domain	F1	F2	F3	Printer
D1	Read		Read	
D2				Print
D3		Read	Execute	
D4	Read Write		Read Write	

12

Access Metrics Mechanism

Object Domain	F1	F2	F3	Printer	D1	D2	D3	D4
D1	Read		Read			Switch		
D2				Print			Switch	Switch
D3		Read	Execute					
D4	Read Write		Read Write		Switch			

- When we switch a process from one domain to another, we execute a switch operation on an object(the domain).
- We can control domain switching by including domains among the objects of the access matrix. Processes should be able to switch from one domain (Di) to another domain (Dj) if and only is a switch right is given to access(i, j).
- According to the matrix: a process executing in domain D2 can switch to domain D3 and D4. A process executing in domain D4 can switch to domain D1 and process executing in domain D1 can switch to domain D2.

13

Access Control List

Section - 4

14

Access Control List

- An Access Control List (ACL) is a **table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file**.
- Each object has a security attribute that identifies its access control list.

15

Trojan Horse, Trap Door, Virus and Warms program threats

Section - 5

16

Trojan Horse

- A Trojan horse is a **standalone malicious program which may give full control of infected PC to another PC**.
- Trojan horses may make copies of them, steal information or harm the host computer systems.
- The Trojan horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer.
- Trojans are designed for different purpose like changing your desktop, adding silly active desktop icons or they can cause serious damage by deleting files and destroying information.
- Trojans are also known to create a backdoor on your computer that gives unauthorized users access to your system, possibly allowing confidential or personal information to be compromised.
- Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. Means Trojan horse viruses differ from other computer viruses in that they are not designed to spread themselves.
- Most popular Trojan horses are
  - Netbus, Subseven, Back Orifice, Beast, Zeus, The Blackhole Exploit Kit, Flashback Trojan.

17

Trap Door

- A trap door is a **secret entry point into a program that allows someone that is aware of the trap door to gain access without going through the usual security access procedures**.
- We can also say that it is **a method of bypassing normal authentication methods**.
- It is also known as back door.
- Trap doors have been used legally for many years by programmers to debug and test programs.
- Trap doors become threats when they are used by dishonest programmers to gain unauthorized access.
- It is difficult to implement operating system controls for trap doors.

18

Virus

- A computer virus is a **computer program that can replicate itself and spread from one computer to another**.
- Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by other computers.
- A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.
- Viruses can also replicate themselves.
- All computer viruses are manmade.

19

Worms program threats

- A worm is a **program which spreads usually over network connections**.
- Unlike a virus which attaches itself to a host program, worms always need a host program to spread.
- Worms are not normally associated with one person computer systems.
- They are mostly found in multi-user systems such as UNIX environments.
- A classic example of a worm is Robert Morris is Internet worm 1988.

20