Operating System Security : Security Policies

Sarika Choudhary
M.tech (Network Security)
School of Engineering & Sciences
BPS Mahila Vishwavidyalaya
Sonepat, Haryana, India.
scpreety98@gmail.com

Abstract—Security is the primary concern in the modern world. The main focus of this paper is the security of our information and its supporting infrastructure. By keeping the computer system secure we can provide the security to the computerized information and vital to that is the operating system.

In order to have a secure operating system it must be supported by the suitable computer architecture. If the technology from which the OS is built and on which it is supported is not secure then there is no confidentiality in the security of the OS and of the information it maintains for the users.

This is the short overview of OS Security. In this paper we will discuss about the security policies that can be supported by the system.

Keywords-OS, infrastructure, integrity, scheduling, security

I. INTRODUCTION

Basically operating systems are the software that provides access to the much hardware like CPU, Memory etc. We can consider a program that allows a user to enter a password. The OS provides access of Hard Disk on which program is stored, and provides access to the memory so that program can be loaded and it may be executed. Display device is used to show the user how to enter the password. Mouse and Keyboards are used to enter the password. Now there are multiple devices that can be used smoothly, we're very thankful to the function of OS.

Operating system runs program in processes. OS permits one process to be run at a time. Now-a-days OS uses concurrency in processes means while a computer waits for a user to enter the password, other processes may be run and can access system device as well. These systems are called timesharing systems and today they are our default OS

To build a successful OS, we consider three major tasks:

- OS must provide efficient resource mechanism such as memory management, network protocol stack etc. that defines how processes use the hardware and software resources.
- Scheduling access to computer resources means access of resources should be controlled.
- The problem of ensuring the security of the processes that are running on the system.

Security becomes an important issue because computer system interacts in a variety of ways and the sharing of data among multiple users is a fundamental use of computer systems. For providing the security to the OS, the goal is the development of secure operating system and if we use the software from the trusted supplier we can make our system secure.

A. Characterstics of trusted software

- Functional correctness
- Enforcement of integrity
- Limited privilege
- Appropriate confidential level

B. Some security definitions

- "a computer is secure if you can depend on it and its software to behave as you expect" Garfinkel et al. (2003)
- "the ability of a system to protect information and system resources with respect to confidentiality and integrity" Ross (1999)
- "deals with the prevention and detection of unauthorized actions by users of a computer system" Gollman (1999)

- "a secure system is a system on which enough trust can be put to use it together with sensitive information" Olovsson (1992)
- "concerned with the protection of valuable assets from harm, which is a significant negative consequence to the asset … security deals with malicious harm, which is harm resulting from attacks or probes by someone or something playing the role of attacker" Firesmith (2004)

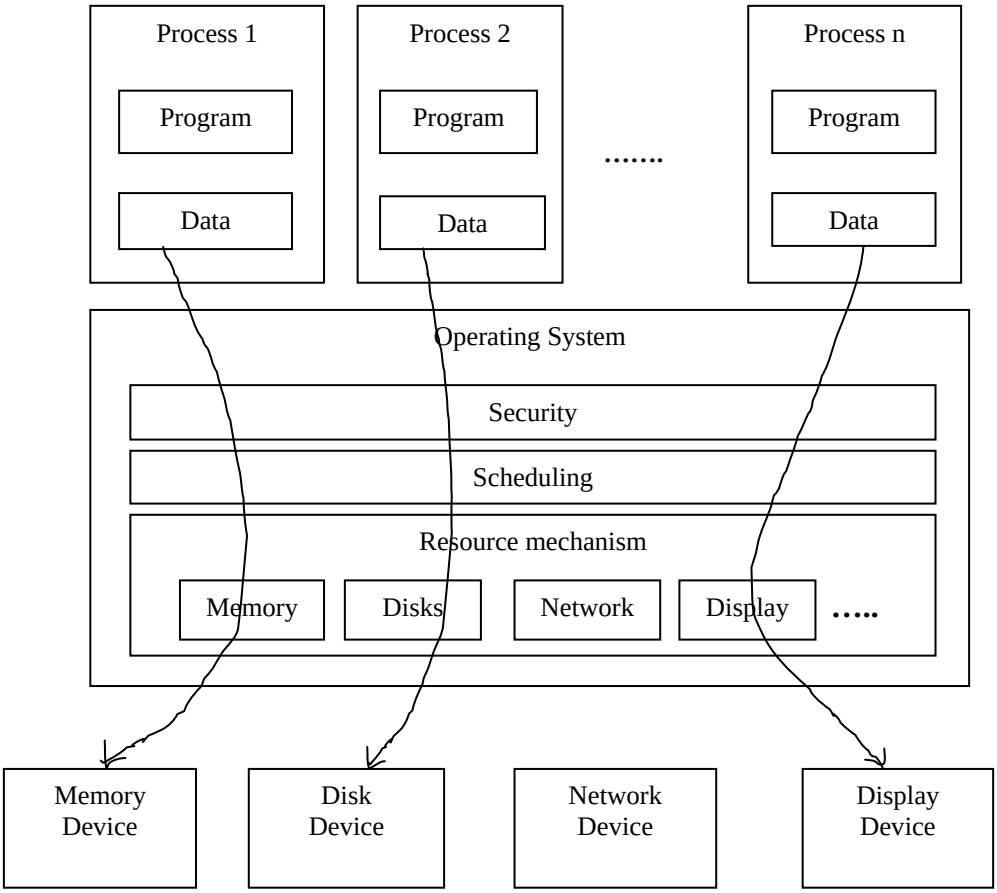


Figure: An operating system runs security, scheduling, and resource mechanisms to provide processes with access to the computer system's resources.

C. Security services provided by operating system

- Resource Security
- Service Security
- Communication Security
- Authentication of users
- Authentication of resources
- Privacy
- Anonymity
- Other security services

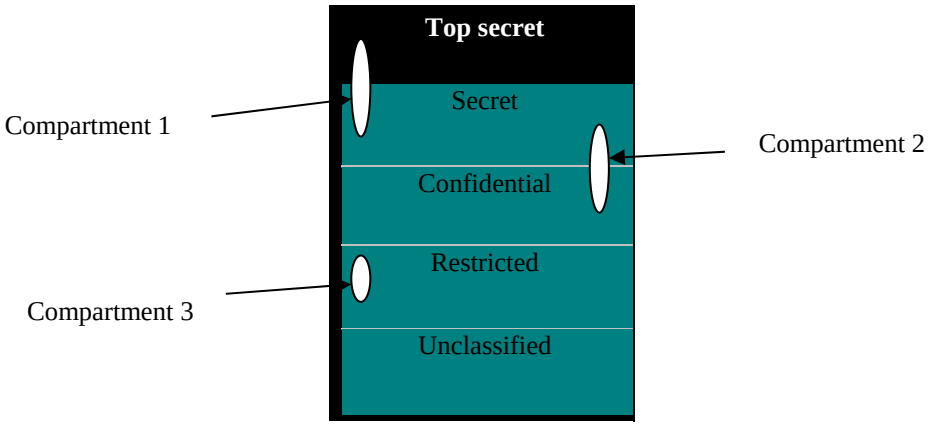
II. SECURITY POLICIES

If we want to know about the security that we expect from the operating system we must be able to state the security policies of operating system. A statement of the security we expect the system to enforce. Basically there are two security policies:

A. ***Military security policy:*** It is the basis of trusted OS development. It protects the classified information. It protcets each piece of information that is ranked at a sensitivity level. There are basically five sensitivity levels, such as: Unclassified, restricted, confidential, secret and top secret. We can form a hierarchy of sesitivity into increasing order. For e.g. top secret information is more sensitive than the unclassified information and confidential is less sensitive than the secret.

In this, there is a rule that is ***need-to-know rule:*** according to this access to sensitive data is allowed only to the subjects who need to know them for completing their jobs (work). If each piece of information is associated with one or more projects/jobs so it is called ***compartments***. Compartments help enforce need-to-know restrictions so that people can access only those information that is relevant to their jobs.

Relationship between compartments and sensitivity levels:



Combination of rank and compartment is called class or we can say classification of piece of information.

$$\text{Class} = \langle \text{rank, compartments} \rangle$$

Now we introduce a relation $\leq$, called dominance, on the sets of sensitive objects and subjects. For a subject d1 and an object d2,

$$d1 \leq d2 \text{ iff } \text{rank1} \leq \text{rank2}$$

$$\text{Compartment1} \subseteq \text{compartment 2}$$

For e.g. <restricted, Pakistan > $\leq$ <secret, India >

Military security enforces both sensitivity requirements and need-to-know requirements. This security policy applied to subjects and objects means users and documents.

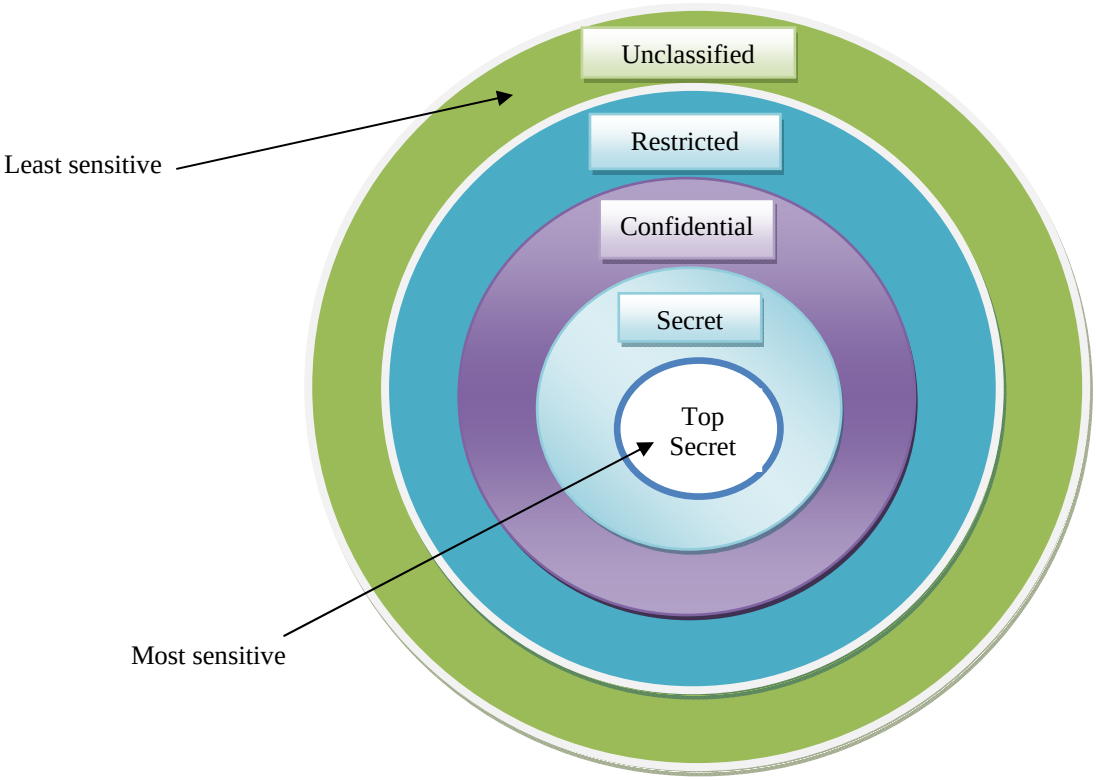


Figure: Hierarchy of Sensitivities.

B. ***Commercial security policy:*** Commercial world is less hierarchical structured than the military world. There are many same concept as military policy in commercial. Commercial enterprises have always security concern. They always worry about that any industry will reveal the information about their new product that is under development. For e.g. a large university may be divided into department, each responsible for number of projects. There may be some responsibilities such as accounting and personnel activities. There are different degree of sensitivity such as public, proprietary or internal.

Public < proprietry < internal

Means public is less sensitive than proprietry and proprietary is less sensitive than internal. Internal have the highest sensitivity degree.

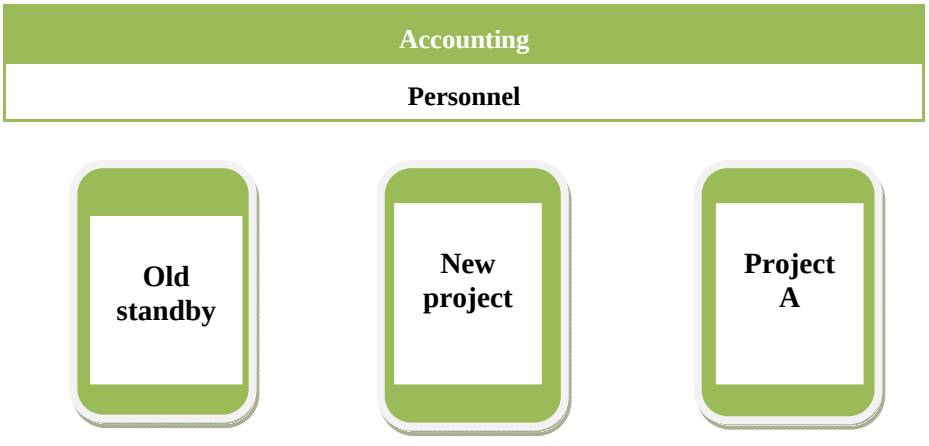


Fig: commercial view of sensitive level.

In commercial security policy projects introduce a degree of sensitivity. Staff members on old standby project have no need to know about the new projects but staff members on the new projects have access to all the data from old standby project.

There are basically two difference between military and commercial security policy:

- Outside the military, there is no formalized notion of clearances.

- When there is no clearance concept so rules of allowing access are less regularized.

Integrity is as important as confidentiality. In many instances military security policy provides confidentiality and commercial security policy provides integrity of data. Policies for integrity are less significant than for confidentiality. There are some ***examples of commercial security policy***:-

1) Clark Wilson commercial security policy: Integrity is as important as confidentiality. Clark and Wilson introduce a policy for well formed transaction, which they assert are as important in their field as is confidentiality in military realm.

For understanding this policy we consider a company that orders and pays for goods. Process for this will be:

- A purchasing clerk creates an order for a supply, sending copies of the order to both the supplier and the receiving department.
- The supplier ships the goods, which arrive at the receiving department. A receiving clerk checks the delivery, ensures that the correct quantity of the right item has been received, and signs a delivery form. The delivery form and the original order go to the accounting department.
- The supplier sends an invoice to the accounting department. An accounting clerk compares the invoice with the original order (as to price) and the delivery form (as to quantity) and issues a check to the supplier.

In this the sequence of activities are important. Performing these steps in order and authenticated the individuals who performed the steps constitute a well-formed transaction. The goal of Clark Wilson policy is to maintain consistency between the internal data and external user's expectations of those data.

2) Separation of duty: It is the second commercial security policy. It involves separation of responsibilities. Lee , Nash and Poland added into Clark and Wilson security policy.

For understanding the policy we consider an example of small company ordering goods. In the company there must be many people who are authorized to order goods, receive the goods and write a check. In this policy we would not want the same people to do the these three tasks so we establish a policy that specifies the three authorized persons for doing three tasks such as ordering the goods, receive the goods and write a check, even though any of three might be authorized to do any of three task. But at a time only one person is assigned to perform one task. This required division of duties or responsibilities that is called seperation of duty.

3) Chinese wall security policy: It is defined by Nash and Brewer. It is used for commercial needs for information access protection. A conflict of interest exists when a person in one company and obtain a personal and important data about products of another company or competitive company.

In this security policy there are three levels of abstractions.

- Objects (lowest level): lowest level is objects such as files. Each file contains information about a particular company.
- Company groups (middle level): in this object concerning about a particular company grouped together.
- Conflict classes (highest level): in this all groups of objects for competing companies are grouped together.

For e.g. with this model, we can form conflict classes with one or more company groups. Suppose you are in advertising company with many clients in several fields like chocolate, bank and airlines. You want to store data and you also want to prevent your employees from revealing information about a client to the competitor client. So establish a rule that nobody can see the sensitive information about competitive companies.

Using this security policy we can create three conflict classes with six company groups.

Conflict classes= {Cadbury, Kitkat} and {PNB, SBI, RBI} and {Indian airlines}

In this, there is a simple access policy: - a person can access any information as long as that person has never accessed information about a different company in the same conflict class. Means access is allowed if either the object requested is in the same company group.

Chinese wall confidential policy is inspired by commercial policy. It is not like other policies which focus on the integrity. In this access permissions change dynamically. If a subject accesses some objects, other objects that have been previously accessed are subsequently denied.

III. PROPERTIES OF SECURITY POLICIES

There are many properties that are provided by security policies:

- Confidentiality
- Integrity
- Availability
- Confinement
- Identity
- Anonymity
- Non-repudiation

IV. CONCLUSON

In this paper we studied about operating system and its policies. Operating system is the heart of modern computers. OS must provide mechanism for both separation and sharing and provide mechanisms that must be robust and easy to use. We always most concern about the security of the system. Through security policies and models, the essential component of systems is identified. In this paper we've studied variety of policies. This type of knowledge about operating system security policies can help to secure our system very efficiently, whereas the policies covered confidentiality and integrity.

REFERENCES

[1] Book: Security in Computing, Fourth Edition By Charles P. Pfleeger
[2] http://www.csse.monash.edu.au/~rdp
[3] Clark, D.D. and Wilson, D.R. (1987) A comparison of commercial and military computer security policies, Proc. IEEE Symp. On Security and Privacy, pp.184-194.
[4] www.wikipedia.org
[5] www.cs.columbia.edu
[6] www.giac.org
[7] www.computerprep.com
[8] www.cse-cst.gs.ca
[9] www.ibm.com