MUINDE GEOFREY MUNGUTI

94231

ICS 4 B

ISSD ASSIGNMENT ONE

1. **Chinese Wall Model** is a model based on access control confidentiality. It builds on three levels of abstraction, namely: Objects, which contain information about only one company, Company groups, which collects all objects concerning a particular company, and conflict classes, which clusters the groups of objects for competing companies.

The model restricts access based on the following two properties:

**Simple security policy** – A subject ***s*** can be granted access an object ***o*** only if the object is in the same company dataset as the object already accessed by ***s***, that is, “within the wall” or belongs to an entirely different conflict of interest class.

**\*-Property** – Write access is only permitted if access is permitted by the simple security rule , and no object can be read which is in a different company dataset than one for which write access is requested and contains information which is not sanitized.

**Application in enterprise systems.**

The Chinese model is applied in enterprise systems in which if one subject serves several companies. The companies may be competitors, in which, accessing certain information in one company could lead to a compromise in that company if their information is fed to their competitors. This model will ensure that if someone has accessed certain information in a certain company, then they cannot be granted access to similar information in a competitor company.

***Example***

If an IT company wants to reverse engineer a certain system. They can group their developers into two groups. One group reverse-engineers the system to have the original code and document how to implement the system. Then the other group uses the existing documentation to write new code of a similar system. Members in either group cannot serve on the other group. This is an example of a Chinese wall model.

1. Clark-Wilson Model is a model that focuses on upholding integrity. The security model maintains that only authorized users should make and be allowed to change the data, unauthorized users should not be able to make any changes, and the system should maintain internal and external data consistency.

The model requires **well-formed transaction,** which is defined as a transaction where the user is unable to manipulate data arbitrarily, but only in constrained ways that preserve or ensure the integrity of data.

**Application in enterprises**

This model is applied in accounting or banking systems that value integrity of data because data which is not true in such enterprises could lead to huge loses or lack of accountability which is not a scenario so friendly in such fields.

1. **The Information Flow model**is an extension of the state machine concept and serves as the basis of design for both the Biba and Bell-LaPadula models, which are discussed in the sections that follow. The Information Flow model consists of objects, state transitions, and lattice (flow policy) states. The real goal of the information flow model is to prevent unauthorized, insecure information flow in any direction. This model and others can make use of guards. Guards allow the exchange of data between various systems.

**Application in enterprises**

The information flow model is used mostly in enterprises that use distributed systems in which it ensures integrity of data flowing through the system. This ensures that at no point is there any data which is not similar on all the systems, say servers that are in use. Data flow from server to client is also made secure so the data is not corrupted.

2.

Security Enhanced Linux (SELinux) is an implementation of a Mandatory Access Control permission system (MAC) in the Linux kernel. In order to restrict among other things, the ability to process, access or perform other operations on system objects to the least permission possible while still allowing for the modification of this model. The AppArmor is another MAC which in addition to the features provided by SELinux, includes a learning model that allows system to learn how specific applications behaves and sets limits by configuring profiles for safe application usage. The use of SELinux and AppArmor in provision of MAC above, the original DAC structure is that these two methods bring about flexibility. This is in a way such that these methods allow least permission possible while still allowing for modification and also have a learning node that allows systems to learn unlike DAC that is strict such that a user one cannot access another user’s files .  
 Another reason for using the above methods in MAC over DAC is that they provide security and reduce risk as they allow minimum permission to perform a task whereas DAC provides more risk as data is accessible to all users that should not have access. The above methods can be applied it typical system such that SELinux can be used to reinforce security by allowing users with enough permission to do a task. AppArmor can also be used to learn about a system a reinforce on the weaknesses.

3.

[**Role-based access control**](https://en.wikipedia.org/wiki/Role-based_access_control) (RBAC) is an access control method based on defining employee roles and corresponding privileges within the organization. The idea of this model is that every employee is assigned a role. Every role has a collection of permissions and restrictions. An employee can access objects and execute operations only if their role in the system has the relevant permissions (Mask, 2018).

[**Attribute-based access control**](https://en.wikipedia.org/wiki/Attribute-based_access_control) is a model that evolved from RBAC. This model is based on establishing a set of attributes for any element of your system. A central policy defines which combinations of user and object attributes are required to perform any action. (Mask, 2018).

The table below compares the key characteristics of RBAC and ABAC.

|  |  |  |
| --- | --- | --- |
| Characteristic | RBAC | ABAC |
| Flexibility | (For small and medium-sized organizations) | Available |
| Scalability | Not quite | Available |
| Simplicity | Easy to establish roles and permissions for a small company, hard to maintain the system for a big company | Hard to establish all the policies at the start, easy to maintain and support |
| Support for simple rules | Yes | Yes |
| Support for complex rules | Available | Available |
| Support for rules with dynamic parameters | No | Available |
| Customizing user permissions | (Every customization requires creating a new role) | Yes |
| Granularity | Low | High |

4.   
Defense in depth security architecture emphasizes on controls that are designed to protect the physical, technical and administrative aspects of a network. The physical control includes security measures to prevent physical access to Information systems, such as security guards, locked doors, secured perimeters amongst others.  
 The technical control includes use of software, such as firewall appliances or antivirus program to secure the network from any software related attacks. Data protection methods are reinforced in this layerThis includes things such as rest encryption, secure data transmission ,hashing, and encrypted backups. There also is the technical defense in which the network is reinforced by perimeter defenses which include firewall, intrusion detection system and intrusion prevention system.

The administrative control is based on policies or procedures that dictate interaction of employees and the system, for example instructing the workers to label sensitive data as confidential . It enforce policies and procedures such that the system is not left in a vulnerable state. However much the two layers above are reinforced if the policy and procedures are not reinforced then the system is unsafe. The three layers complement each other in all possible ways to ensure the system is always in a secure state.

References.

Cyber Defense. (n.d). Clark-Wilson Model. Retrieved May 12, 2019, from <http://luizfirmino.blogspot.com/2006/07/clark-wilson-model.html>

Mask, E. (2018). *Role-based Access Control vs Attribute-based Access Control: How to Choose*. Ekransystem.com. Available at: <https://www.ekransystem.com/en/blog/rbac-vs-abac>. Accessed 13 May 2019.