Comparative Evaluation of Access Control Models

by

Paige Langmead

Presented in partial fulfillment of the requirements

for

Departmental Honors

in the

Department of Computer Science and Information Technology

Hood College

April 2022

Abstract

In cybersecurity, access control models dictate what actions a person can perform, which programs they have permission to execute and overall, the level and type of access of information technology resources. This work compares a number of the most widely used access control models and analyzes their suitability of deployment in different contexts. To perform the analysis, several key background access control mechanisms are described and analyzed. The first result from this analysis is the realization that there is no dominant model that can be suitable across all environments. It is therefore important for access control models to be selected that match the needs of a particular environment. The more in depth analysis focuses on the direct comparison of specific access control models, Bell-Lapdula, Biba, Clark and Wilson and Lampson's Access Matrix. The result from this analysis is that the Biba model is the most robust and most secure integrity model, especially due to its perfect connection with the Bell Lapadula confidentiality model. These findings are significant as comparing the expressive power of access control models is a fundamental problem in information security.

Introduction

With the use of technology in every facet of daily life, it is imminent that security be in place to protect from various potential threats such as hackers, viruses, and identity theft. Access control ensures that confidential information cannot be accessed without proper authorization. The implementation of access control mechanisms can take many forms, using varying technologies and levels of complexity. Access control is considered as the first line of defense to mitigate the risk of unauthorized access to systems and information. As such, it is a critical component supporting the fundamental Cybersecurity principles expressed by the Confidentiality, Integrity, and Availability (CIA) triad [29]. Practically, contemporary concepts and frameworks like zero trust security depend heavily on access control methodologies to constantly verify and enable access to organizational networks and systems without the risk of information leaks and other compromises from internal and external sources [9].

Authorization and authentication are used extensively in these models, and they are implemented or enforced in all resources, such as networks, devices, and systems. Authorization verifies a user's identity before giving them access to the system while access control determines which resources a user may access based on the user's privileges. Once a user's identity is confirmed, access control authorizes the level of access and permitted actions based on the user's credentials [2]. The most generic form of authentication is the use of passwords which is referred to as single *factor authentication*, although more secure authentication mechanisms are in demand, such as multi-factor authentication [10] to provide more secure ways to verify user identity.

An access control model describes who can be granted access to certain data and resources within an organization. There are four main models of access control: *discretionary,*

mandatory, role-based, and *attribute-based* access control [2, 3, 11] and in most organizations, more than one type is often used. These models rely heavily on a distinction between a *subject* and an *object* which in the context of information security, an example of a subject is a user, and an object is a file [2]. When a subject attempts to use an object, an access control list (ACL) may be checked to ensure if the subject has permission to use that object. ACLs are described as a logical access control model and contain rules to grant or deny user access to networks, systems, devices and any other information technology asset. It is safe to assume that any user on a multi-user system is operating under an access control model whether they are aware of it or not.

The general area of this work is in access control models. There are several different types of access control which include discretionary access control(DAC), mandatory access control(MAC), role-based access control(RBAC), and rule-based role-based access control (RB-RBAC). DAC is very well known and used in operating systems such as Microsoft's Windows. RBAC created “groups” and is used in environments such as Linux. MAC is the most secure access control model and meets all criteria of the CIA triad. RB-RBAC is not as well-known, but it is important to include in this analysis and comparison as it meets the proper criteria. The area is broad, so the focus of the work is based on the comparison of four well-known models: the Bell-Lapadula, Biba, Clark andWilson, and Lampson’s Access Matrix that fall under some of the above mechanisms.

In the next section, Background, we provide brief descriptions of the most important access control mechanisms and models. Section 3 contains our Analysis where we focus on the specific models of interest and their comparison. In Section 4 Discussion we are taking models with the same focus and comparing them with one another along with the situations they might work best in. In Conclusion, we summarize our findings and offer some avenues for future work.

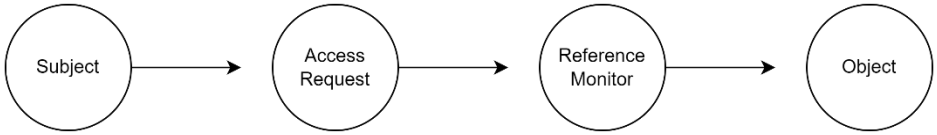
Background

Access control deals with five elements: *subjects*, *objects*, a *model*, a *security policy,* and *access rights*. A subject is an entity which can access objects and subjects cause information to flow among objects or change the system state [2]. Users can have multiple subjects, each possessing different permissions which can be active at the same time. An object is a resource to which access is controlled and frequently, the owner of an object is also its creator [4]. Each object has its own list of mappings, relating the set of entities (subjects) requesting access and the set of actions each entity can take on a resource (object) [1]. A model is a formal presentation of the security policy enforced by the system and is useful for proving theoretical limitations of a system. A security policy on the other hand is the statement of required protection for information objects. Access rights describe the set of actions each entity can take on a resource and typical examples of this include the ability to “read,” “write,” and “delete.” Security policies are the statements of required protection for information objects [2].

The general access control model allows one to control the ability of a subject to access objects through requests and controlling access to objects with a general reference monitor (Fig.

1). A reference monitor is a set of design requirements on a reference validation mechanism that, as a key component of an operating system, enforces an access control policy over all subjects and objects. A reference validation mechanism is always invoked, tamper-proof, and small enough to be subject to analysis and tests, the completeness of which can be assured [28].

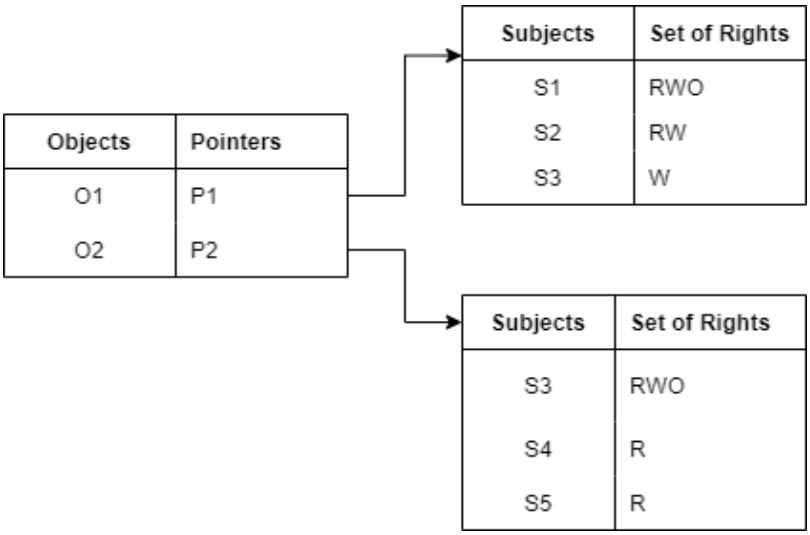
Figure 1: The General Access Control Model- Dictates who is allowed to access and use objects



Access Control List

An access control list (ACL) is one of the most common and oldest access control mechanisms currently in use that implement Lampson's Access Matrix. An ACL associates the permitted operation to an object and specified all the subjects which can access that object, along with their rights to that object (Fig. 2) [2].

Figure 2: Access Control List- A visual representation of which rights subjects have to objects. In this figure, R stands for read, W stands for write, and O stands for own.



Objects	Pointers
O1	P1
O2	P2

Subjects	Set of Rights
S1	RWO
S2	RW
S3	W

Subjects	Set of Rights
S3	RWO
S4	R
S5	R

Another way to view ACL is corresponding to a column of the access control matrix. An access control matrix is a table in which each row represents a subject, each column represents an object, and each entry is the set of access rights for that subject to that object [28] (Fig 3). These lists provide a straightforward way of access to a particular user or group. Each entry in the list is listed as a pair (subject, set of rights) (Table 1). These lists are normally implemented directly or as an approximation in modern operating systems [2].

While the ACL is a very readable way to express access control, access rights management based on individual entities can be difficult. This is because subjects are not individually granted access to objects: typically, for a certain object, there are several subjects with access to the object. To remedy this, users can be associated with groups and users access rights are then derived from the groups' access rights [3].

Lampson's Access Matrix

The expression of the model uses a mechanism based on a two-dimensional matrix to represent subjects on rows and objects on columns (Fig 3) . Each matrix entry contains access attributes which specify access privileges held by subject to object. Implementation using such a matrix is based on the idea that access rights can be defined individually for each combination of subject and object. There is an assumption in this type of matrix of de facto ownership of an object by the subject that created it. This allows the subject to modify Access matrices which can be represented as a list of triples (subject, object, access right), but searching for many triples is not effective [3]. Lampson's Access Matrices were an early concept for but fails to scale in environments with too many subjects or objects. Its use creates a large sparse matrix because typically, most subjects do not have access to some object leading to storage implementation inefficiencies [3, 23].

Figure 3: Access Control Matrix- Each entry shows which rights each subject has to particular objects.

		Objects	
		O1	O2
Subjects	S1	RWO	
	S2	RW	
	S3	W	RWO
	S4		R
	S5		R

Discretionary access controls

In this model, control restricts accessibility to objects based on the identity of the subject or groups to which they belong. The owner of an object, who is usually the creator, has discretionary authority over who can access the created objects [3, 4]. The model operates under the condition of having one owner per object and the object can only be destroyed by its owner. Discretionary access control uses an access control matrix to check authorization requests and

determine whether the user can be granted access to the requested object. Each user has an access combination of read, write, execute, and other permissions. The controls are discretionary, which means that a user with discretionary access can grant authorization to other subjects [2, 3].

Table 1: Access Control Matrix- A large visual representation of all subjects, objects, and access rights

	Objects			
	Employee Income File	**Volunteers File**	**Employee Application Files**	**Inventory**
Jeremy	Read Write Own	Read Write		Read
Tim	Read	Read Write Own	Read	Read
Susan	Read Write		Read	Read Write Own
Kelly		Read	Read Write Own	Read Write

This model is considered the least restrictive, and easier to manage and implement but introduces several weaknesses. The most serious weakness is the transitive access granting, a misuse of trust that causes issues with control, that comes with this policy and makes information assets vulnerable to Trojan horse attacks, a vulnerability that is not present with other models, such as mandatory access controls [3]. A Trojan horse is a type of malware which leads users to believe it is legitimate allowing the hacker to gain access. However, this type of access control is still useful and may be suitable for organizations with limited resources or those storing small or no amounts of sensitive information.

Role Based Access Controls

In this model, access is based on the user's assigned roles in the organization.

RBAC is an established and well documented [5] model. National Institute of Standards and Technology (NIST) standard INCITS 359-2012 [13] addresses RBAC and defines as a role a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role.

Each user is assigned a role, where access rights are grouped by role name, and the use of resources is restricted to individuals authorized based on their role [2]. Roles are granted based upon a user's competence and responsibilities and user access rights are determined by the role.

RBAC is considered policy neutral as it is used to articulate a security policy rather than embodying a particular security policy [4]. This allows adjustments to be made easier to this

security policy than with other systems. If an organization adopts new operations, then new roles and access rights may need to be established. A key information security practice is the implementation of *least privilege* which dictates that a user should be given no more privilege than necessary to perform their job. This concept requires identifying job functions, calculating the minimum number of privileges needed, and restricting the user to only this set of privileges [2]. In RBAC, objects are assigned to groups and users can be members of multiple groups which would, in turn, give them access rights to privileges in these groups. Despite its many advantages, the one disadvantage of RBAC is that by dividing users into categories based on certain roles it is more difficult to define granular access controls for each individual user [1]. Labels are used to enforce access control over individual subjects.

Rule-Based Role-Based Access Control

This model adds rules into the already successful role-based access control model to make it more flexible and efficient.

Rules and roles are combined and significantly enhance the traditional RBAC model. This model reduces the efforts for identity management and access control administration. In RBAC, permissions can only be assigned to subjects, not objects but in RB-RBAC, access rights grouping is possible using rules instead of roles. Rules consist of a condition on the left-hand side (LHS) and the right-hand side (RHS). When the left-hand side is true, the right-hand side is executed. For example, an administrator may regulate access hours to the building. Therefore, if you arrive during business hours, access to the building will be granted. If it is not business hours, access will be denied. Rules make it possible to give one or more access rights to a whole group of users, which makes RB-RBAC a powerful model [5]. Combining rules with roles also allows for the possibility of creating role hierarchies, further extending flexibility in expressing organization-specific structures. All these advantages tend to reduce administration efforts but there are also some drawbacks. An inherent problem with rule-based systems is the difficulty to predict the impact of rule changes. They also lack the capacity of roles to build “business roles” which contain all permissions for a specific business function [5].

Mandatory Access Controls

In this model policy decisions are made by a central authority, not the object owner, and the owner cannot change access rights. This is a method based on restricting access to resource objects. One of the important goals of MAC is to enforce flow policies to ensure confidentiality and integrity and they were specifically designed to prevent Trojan horse vulnerabilities. Integrity prevents the unauthorized modification or destruction of information. This is mainly because subjects cannot declassify objects or share access to classified objects. For the accessibility portion of MAC, a two-step approach is used. The first step includes checking each

subject's access privileges which are stored in a discretionary access control (DAC) matrix [3] like the access control matrix (Table 1).

Then, the operation must be authorized by the MAC policy, which subjects have no control over. Within this model, security levels are assigned to subjects and objects. In objects, the security levels, known as security classification or labels, reflect how sensitive the information contained within them is. These classifications include *top secret*, *secret*, *confidential*, and *classified* [12]. In subjects, the security levels, known as *security clearances*, reflect how trustworthy a subject is by measuring how likely they are to disclose sensitive information to uncleared subjects.[3].

With classification levels, some information flows are more important than others because of their consequences. For example, a top-secret subject writing to an unclassified object is more dangerous than the information flow of the same subject writing in a secret object. The access history of subjects to objects and the resulting possible information flow could have an impact on their security levels [25]. Information can be transferred not only directly, but also by association and aggregation.

With subjects, we can distinguish between trusted and untrusted subjects. Trusted subjects can be trusted not to compromise security; other subjects are labeled as untrusted [12]. The labels of trusted and untrusted correspond with a subject's clearance level. Therefore, a user can only be granted access if their clearance is equal to or higher than an object's classification. Once a user is granted access, they may not share this information with anyone who has a clearance lower than the classification. An example of this occurs in military security, where an individual data owner does not decide who has a top-secret clearance, nor can the owner change the classification of an object from top secret to secret [2].

Bell-Lapadula

The Bell-Lapadula (BLP) model is the most well-known security model designed to secure a multi-user operating system. The model is based on access permissions that are defined by a matrix control approach and various security labels. These labels can range from "Top Secret" being the most confidential down to "Unclassified" being the lowest confidential label. Labels are placed on objects to determine which subjects have access to them.

In this model, users at a higher level can only write at a higher level and not at a lower level, but they are able to read at a lower level (read down). This is so users are not able to access information above their security clearance. This is known as an upward flow of information which means that information at a higher level cannot be seen by a lower level.

The BLP model captures the aspects of confidentiality of access control using mandatory access control mechanisms. This model uses separation of tasks by giving classified subjects and objects colors according to their security level (confidentiality) [24]. Although throughout time

there have been various model variations, most of the core aspects have remained unchanged. Some of these are [6]:

(a) basic subject object access model which has at least read and write access modes,
(b) the structure and comparison of sensitivity levels,
(c) the simple security property and some form of the property,
(d) and a set of transition rules corresponding to the operating system kernel calls that influence the access state.

Biba

This model was designed as an analogy to Bell-Lapadula, except its purpose is to preserve integrity, rather than confidentiality [3]. In this instance, integrity reflects trustworthiness and credibility. To do so, subjects and objects are classified by levels of integrity. The Biba model uses mandatory access control, along with discretionary and non-discretionary policies. Discretionary means that the owner of the resource in question may grant or deny access to that object. Nondiscretionary policies restrict access based on sensitivity of information using labels.Like the BLP model, the Biba model also uses labels to prohibit the modification of data, and to mark integrity levels to the subjects and objects (Example 1) [7]. The data marked with a higher level of integrity is treated as more accurate and more reliable. Consequently, data with a lower level of integrity are considered less reliable. This model uses separation of tasks, with subjects and objects separated to ensure integrity [24]. Users with a lower clearance can read high level information and users with high levels of clearance are able to write for low levels of clearance. The idea of this is so that users cannot corrupt files or other resources in a higher level of security. This works in reverse of the Bell Lapadula model as information in the Biba model can only flow downward, going from high security levels to low security levels.

Example 1

In a retail shop, if the store manager decides to change the percentage of an on-going sale, they have the right to do so. This change of the sale percentage is data with a high level of integrity. Therefore, everyone in the store working for the manager has permission to trust that information. Similarly, if a low-level store employee sends a message about a change in percentage of the sale, then that data is not to be trusted because it has a low level of integrity. Therefore, no one above the low-level store employee would has permission to trust that information.

Clark andWilson

The Clark and Wilson model is an integrity model like the Biba model. designed to ensure consistency between internal data and external requirements [3]. It uses the principle of *separation of tasks*, which states that whoever commits the transaction and the one who carries it out must be different entities (Example 2) [3]. Separation of duties refers to the principle that no user should be given enough privileges to misuse the system on their own. Clark and Wilson partitioned all data in a system into constrained and unconstrained data items for which integrity must be ensured.

Example 2:

A transaction, the promotion, assistance of a customer in sale of a product at a retail store can and may be carried out by a salesperson. But the transaction is "committed" after the customer pays and receives a receipt. In other words, committing a transaction means that the transaction is completed and recorded on the system of record.

Two procedures are then applied to these data items. The first procedure known as the integrity verification procedure (IVP), verifies that the data items are in a valid state. The data items are known to be in a valid state when they are what the users or owners believe them to be because they have not been changed. The second procedure is the transformation procedure (TP) or well-formed transaction, which changes data from one valid state to another. If only the TP can change the data items, integrity will remain. In this model, to be sure that integrity is continuous, certain integrity monitoring and integrity preserving rules are needed. These preserving rules are also known as enforcement rules and include enforcement of validity, enforcement of separation of duty, user identity, and initiation [8].

Analysis

In this section, we will attempt to analyze just four of the many different access control mechanisms We will look at the various aspects of each model to identify advantages and disadvantages for each one. The analysis will be done of the Bell Lapadula model, Biba model, Clark and Wilson model, and Lampson's Access Matrix. After each model has been analyzed, we will then group them by focus to begin comparing them to one another. It is pointless to compare models of different focus because they have different purposes. When separated, each model will be compared based on its adequacy and completeness, assumptions made, the central theme, secrecy, and advantages and disadvantages.

Bell Lapadula

This model was the first and most widely used multi-level security model. It uses mandatory access control and is commonly used to enforce the U.S. Department of Defense (DoD) multilevel security policies [16, 17]. By enforcing this model, a subject can have access to

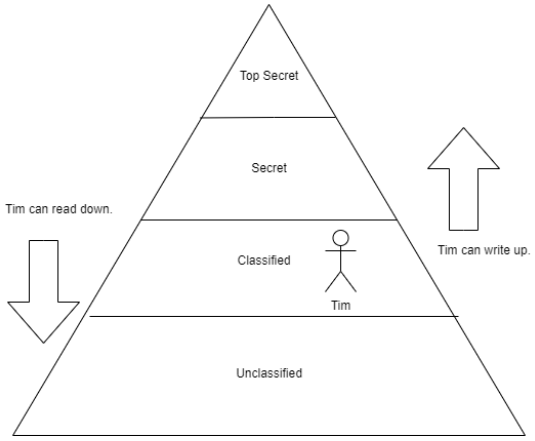
an object if and only if the subject is authorized to access the object by both the multi-level security policy (mandatory access control) and the discretionary access control policy. The multi-level security policy ensures the confidentiality requirements are met and the discretionary access control policy ensures the flexibility of access control policies [15]. When classified information is involved, the semantics of the classification of the object and the clearance of the subject are important to ensure that it does not fall into the hands of the wrong subject. This model can easily be summarized with two axioms: *no read up* and *no write down*, meaning that a subject cannot read objects above their clearance level and no subject can lower the classification level of a subject (Fig 4). This model was recently reformulated and now focuses primarily on the information flow possible in a formally specified set of functions [14].

Bell Lapadula is most frequently used in the military. Its greatest advantages are the built-in strict security classification and the protection of data against Trojan horse attacks [16]. The model has three security properties and when they are all satisfied, the system can be labeled as secure. These are:

(a) The simple security (*ss-property*) enforces a no read or write up policy,
(b) The star (**-property*) enforces a no append or write down policy and,
(c) The discretionary security (*ds-property*) is a property which verifies the system uses an access matrix to enforce DAC.

This system is convenient because it downgrades all subjects and objects to the lowest level and then enters all access rights in all positions of the access control matrix [26]. However, the model's limitation is that it does not take integrity into consideration, nor does it provide a method to manage classifications as it assumes that all objects are assigned with a classification type and the classification never changes.

Figure 4: Bell Lapadula Model- No read up and no write down property example



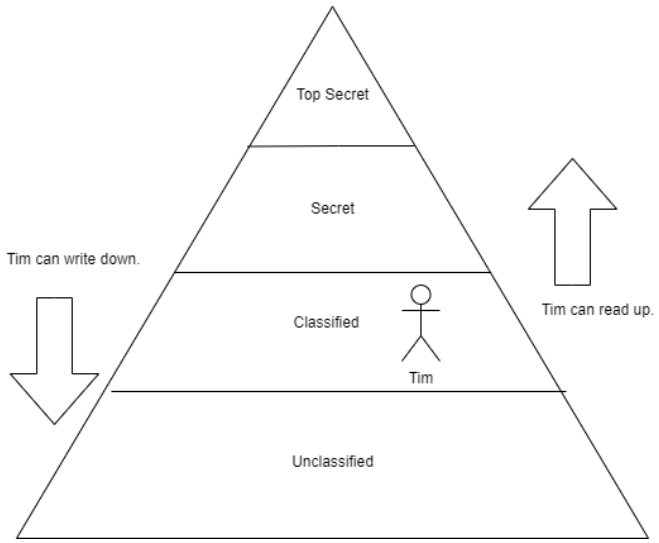
Biba

This model was created shortly after the Bell Lapadula model with a focus on addressing its lack of information integrity. The main objective is to prevent unauthorized users from making modifications to information. Each subject and object have an integrity level associated with it.

The model consists of four access modes: *modify*, *observe*, *invoke*, and *execute. Modify* allows a subject to write to an object, where *observe* allows a subject to read an object. *Invoke* allows one subject to communicate with another subject and *execute* allows a subject to execute an object, which is usually executing a program. This model enforces a flow of no write up and no read down, which is the opposite of the Bell Lapadula model (Fig 5) [17].

This model is used in commercial operating systems such as Microsoft's Windows Vista operating system and other commercial application settings where data integrity is more important than confidentiality [16, 17]. The model is simple and easy to implement and offers several different policies. But the model's flaw is the complete lack of including confidentiality as a consideration and not providing any mechanisms to support the granting and revocation of authorization. To use this model, all computers in the system must support the labeling of integrity for both subjects and objects. To date, there are no network protocols which support this labeling, which causes problems with the model in a network environment [17].

Figure 5: Biba Model- No write up and no read down ideology example



Clark and Wilson

This model focuses on data integrity by using transactions. It uses well-formed transactions to allow systems to move from one consistent state to another and addresses all three integrity model rules: (a) preventing unauthorized users from making modifications, (b) preventing authorized users from making improper modifications (separation of duties), and (c) maintaining external and internal consistency (well-formed transactions).

These rules are enforced by using an access triple (subject, software transformation procedures, and object), separation of duties, and auditing (Table 2) [17].

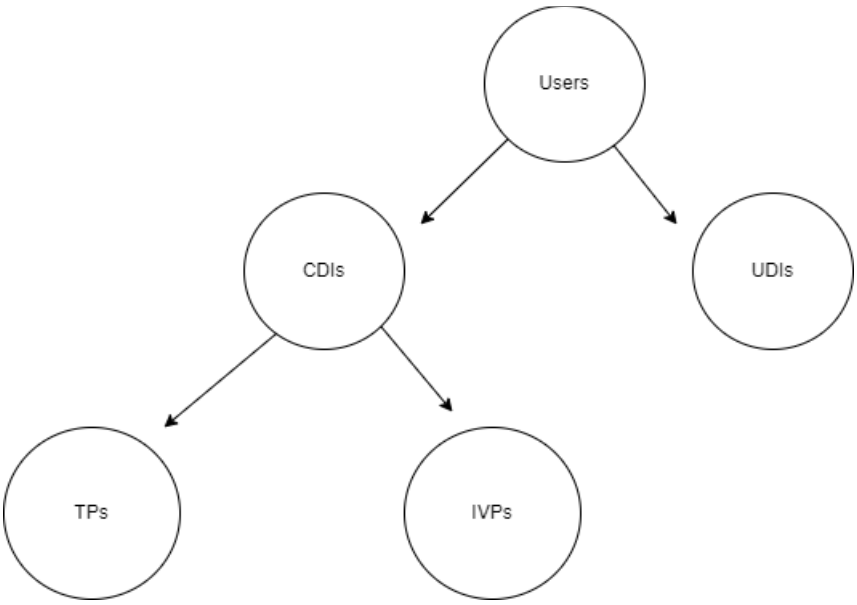
Table 2: Access Triples- Three Part Relationship between subject, object, and access rights

Subject	Object	Access Rights
Jeremy	Employee Income File	Read, Write, Own
Jeremy	Volunteers File	Read, Write
Jeremy	Inventory	Read
Tim	Employee Income File	Read
Tim	Volunteers File	Read, Write, Own
Tim	Employee Application File	Read
Tim	Inventory	Read

The model's elements include users, transformation procedures, constrained data items, unconstrained data items, and integrity verification procedures (Fig 6) [27]. Transformation procedures or TPs are programmed abstract operations such as debit or credit. Constrained data items (CDIs) can be manipulated only by transformation procedures. Unconstrained data items (UDIs) can be manipulated by users via primitive read and write operations. Integrity verification procedures (IVPs) run periodically to check the consistency of CDIs with external reality. The model also includes certification and enforcement rules. The certification rules ensure that the IVPs and TPs are certified to be correct, while the enforcement rules ensure that the system maintains a list of relations of the form and a list of all CDI for which each TP is certified [27].

The Clark and Wilson model is mostly applied in business settings. The triple integrity protection is the main advantage of using this model along with the highlighting that there is more to integrity than the Biba model, which in turn, has also played a significant role in its wider acceptance by the information security community [16, 27]. However, its main disadvantage is that it does not take data confidentiality into consideration. Another criticism is that this model is too static and centralized as only the main authorized person can change any type of authorization within the model. An additional disadvantage is that no further information was given on how the certification of integrity verification procedures and transformation procedures should be performed without including complex and costly formal code analysis. This model also tends to place a greater responsibility on the administration body for determining adequate separation of duty throughout the system, which can become error prone [18].

Figure 6: Clark and Wilson Model- Visual representation of the flow of the Clark and Wilson model



Lampson's Access Matrix

Lampson defined the idea that a protection state is represented by an access matrix, in general [19]. An access matrix consists of a set of subjects, a set of objects, a set of operations, and a function, which determines the operations that a subject can perform on an object [19]. The matrix is two-dimensional where the set of subjects form one axis, and the set of objects form the other axis. The entries in a matrix show the access rights and operations which a subject has and may perform on an object. The columns of the matrix are known as access control lists, while the rows of the matrix are known as capability lists. The model also defines operations which determine which subjects can modify cells of the matrix. By looking at the rows in this access matrix, individuals can see all the operations a subject is authorized to perform [19]. In the context of computer operating systems, it must be ensured that the protection domain of each process satisfies the system security goals of secrecy and integrity where the protection domain of each process refers to the protected memory area that each process must operate and the objects it may access during the run-time execution of a program [19].

Access control matrices are separated into columns (access control list) and rows (capability list). The advantages and disadvantages of each of these are opposite of one another. In an access control list, it is easy to see who has access to an object, but difficult to see what objects the subject can access [2]. ACLs scale up well and work efficiently with distribute systems [21]. In a capability list, it is easy to see what objects a subject can access, but difficult to see who has access to an object [2]. Because a capability list working at subject level, it is good for granting rights to a subject [21]. The main disadvantage which comes with using a matrix is that in a large system, the matrix will be enormous in size and mostly sparse. This may cause the matrix to be confusing and laborious to look through.

Table 3: Comparing Focus Areas Amongst Models- It is important that the focus area is taken into consideration as it is pointless to compare models without the same focus.

Model	Focus Area
Bell-Lapadula	Confidentiality
Biba Clark and Wilson Lampson's Access Matrix	Integrity

Integrity

The three models which have a focus area of integrity are the Biba model, the Clark and Wilson model, and Lampson's Access Matrix. Because each model uses unique approaches to meet the integrity goal, there must be a framework to establish a common ground. This will allow for a fair comparison of the models [20]. The areas in the framework are:

1. The definition of integrity used in the model
2. Concepts on which the model is based
3. Advantages and disadvantages of the model

The definition of integrity used in the model

1. Adequacy and completeness
2. Assumptions

The definition of integrity used in the Biba model treats integrity as a relative measure rather than an absolute. One of the differing ideas in the Biba model is that the system must only perform to the designer's intent, whatever that may be. This makes the Biba model very flexible and able to conform to different individuals' needs. Because of this, the responsibility for integrity is placed on the ability of the creator to design a system in which integrity can be achieved [20]. Due to this, the model is lacking in detail and specificity. It is general enough to be applied to any system. A model can be considered complete if based on its environment it is suitable for DoD applications. A model is adequate if it is attempting to take protective measures that are commensurate with the unauthorized access of information.

The assumptions made in the Biba definition are [20]:

1. The system being evaluated is designed in a way that integrity can be achieved.
2. There has been external verification performed on the system to ensure that it is functioning properly.
3. Classification labels exist for integrity levels. These labels are like the levels attached to the security classifications used for military information.

The definition of integrity used in this model is adequate, but not complete.

The definition of integrity used in the Clark and Wilson model is based on prevention of unauthorized manipulation of data. This model involves special integration verification

procedures and transformation procedures. Data that is in a valid state, maintains that state, which ensures the integrity of that data. This definition is broad enough to be applied to various systems. On the downside, there is no method addressed for determining whether the data is initially in a valid state. The concept of valid state serves to isolate the data and label it as worthy of protection. Without a method to determine this, it is difficult to set limits to items that need protection. This model is both complete and adequate.

The assumptions in the definition of the Clark and Wilson model are [20]:

1. Data is initially received in a valid state. There is no mechanism available within the model to test for validity, it is simply assumed.
2. The initial Integrity Verification Procedure (IVP), which confirms that the objects requiring protection meet certain conditions, is assumed to be a valid process itself.
3. The object and the real-world object which it represents correspond closely. For example, the recording of a financial recording (the objects) reflects and corresponds closely to the real-world transaction that transpired.

The definition of integrity used in Lampson's Access Matrix is based on defining access permissions between specific subjects and objects. This is the most fundamental model of protection. Changes to the state of a system are carried out through commands which can execute primitive operations on the authorization state, in other words, a subject can change permissions for other subjects to allow the writing to an object. The ability to specify commands provides flexibility as different administrative policies can be considered by defining appropriate commands [22].

The assumptions in the definition of Lampson's Access Matrix are:

1. It is implemented as a 2D array and represents static access permissions. Static permissions define existing object types and objects which enables the defining of which subjects have access to which objects.

The concepts on which the model is based

1. Central theme
2. Secrecy

The theme of the Biba model is the development of a hierarchical lattice, expressing order, based on partially ordered sets, which is used to identify authorized subjects and separate subjects by type. This allows Biba to implement the "no write up, no read down" restrictions. This implementation is effective in preventing modifications by unauthorized subjects. This restriction is implemented using both mandatory and discretionary controls. Within the model, there are classification levels which assign data to various levels. Labels can be either military or commercially oriented. The use of mandatory and discretionary access controls along with the assignment of labels supports the central theme of this model. It takes the Bell-Lapadula model and creates its dual for integrity. The mechanisms in the BLP model are incorporated in Biba

which allows both models to be implemented simultaneously. BLP uses properties such as the simple security property and the star property to ensure confidentiality. This ties an integrity policy and a confidentiality policy together which allows for a great protection policy for access control and modification control of data [20].

The Clark and Wilson model is built on two premises: the well-formed transaction and separation of duty [20]. A well-formed transaction prohibits unauthorized manipulation, which preserves the integrity of the data. It is a requirement that the transaction be designed in a way that the well-formed label may be applied. Separation of duty is necessary to preserve a correspondence between data objects and the real-world objects which they represent. This separation prohibits unauthorized manipulation by breaking an operation into multiple sub parts and requiring that each of these parts be executed by different subjects. An example of this is often encountered in real life in bureaucracies that require multiple people (subjects) with different authorizations to be involved to carry out a transaction, like issuing a new passport. Due to this, no one subject may execute an entire operation. This helps to prevent malicious tampering with objects with one exception, namely when there is collusion among subjects. This also helps to preserve the integrity of the data while at the same time establishing an access control mechanism. This model relates to secrecy in that it can limit the objects a subject can access [20]. This is also known as a method of disclosure control. Because of this, this model has a strong relation to secrecy.

The goal of Lampson's Access Matrix is to analyze the complexity of determining an access control policy. There are three approaches to implementing the matrix in a practical way.

1. Authorization Table
2. Access Control List (ACL)
3. Capability List

An authorization table is nonempty entries of the matrix which are reported in a table with three columns: subjects, actions, and objects. Each tuple corresponds to an authorization. This table is used in database management systems (DBMS) where authorizations are stored as relational tables of the database. An access control list is where the matrix is stored by column. Each object is associated with a list indicating for each subject the actions a subject can perform on an object. In capability lists, the matrix is stored by row, the opposite of ACLs. Each user has associated a list indicating for each object, the accesses that the subject is allowed to perform on the object [22]. Lampson's Access Matrix uses the ACL approach. Each object has a monitor to validate every user's access to that object by checking for the appropriate access rights [23].

Advantages and disadvantages of the model

1. Description of strengths and weaknesses
2. Correction to deficient areas

The notable strength of the Biba model is that it is the first attempt to treat integrity as the dual of secrecy. This gives it a high measure of compatibility with military security policies and models, like BLP. This compatibility allows for integration of this model into DoD standards for data protection. Another strength of this model is the offering of a variety of policies for both mandatory and discretionary controls. This variety increases the probability of successful integration of an integrity policy as part of a security plan.

The notable weakness in this model is that it is designed for implementation in systems featuring ring architecture, which means the policies are tailored for this system and are not applicable for implementation using anything other than Multics. Multics stands for multiplexed information and computing service which is an early time-sharing operating system. The ring policy is designed to address attempts by subjects to directly modify objects. It fixes integrity levels of subjects and objects and holds these levels constant.

To correct the noted weakness in Biba, feasibility of application to systems featuring other types of architecture must be determined. The model can be adapted to other architectures without major modifications and the principles of the model are valid for application to any kind of system, even though the specific details are not [20].

The definition of integrity used in the Clark and Wilson model relates to integrity as a concept within the context of a computer system. The model identifies the features of a computer system in which integrity is the main goal. The model provides basic rules that must be established and implemented in systems which are used to maintain integrity. Another strength of this model is it is easily understood by the commercial world and not just militarily. This means it has more potential and outreach.

The weakness which limits this model the most is that its requirement for integrity verification procedures (IVPs) needlessly complicates the certification process. A weakness of this model is its inability to have integrity controls internally. The dual process used in this model (certification and enforcement) takes both internal and external environments of the system. This means that data is verified externally before it is allowed to enter the system. Unfortunately, the system may accept data that has been entered incorrectly by either accidental or malicious means. Also, this model is only applicable at a single level of granularity, which is the degree of the detail at which an object can be protected. The inability of implementation in a multi-granular environment limits the models' range of applicability.

The main limitation of this model is that certification is needed for procedures that access protected data There is a need for procedures to be certified for proper functioning. There is an assumption made that the data in the model is received in a valid state and is therefore worthy of protection. This assumption works well for the data, but it does not work for the certification of the procedures. Unfortunately, this limitation cannot be overcome without having an adverse effect on the proper functioning of the mechanisms in the model [20].

The most notable strength of Lampson's Access Matrix is its simplicity, elegant structure, and amenability to various implementations. The capability-based method is efficient, simple, and flexible. The validity of access can be easily tested, there is natural correspondence, and users are allowed to define certain parameters. The access control list method has easy revocation, easy review of access, and provides two ways to control propagation of access rights (self-control and hierarchical control). It is simple to remove the subject's entry from the object's control list and it is easy to directly examine the access control list of a specific object.

The most notable limitation to this model is that the matrix itself is likely to be very sparse. Any direct implementation of the matrix is likely to be storage insufficient. Limitations of the capability-based method are the control of propagation, the difficulty of access review, the revocation of access rights is difficult, and there is a garbage collection problem such as the tidying up of the matrix entries once changes, deletions, and revocations have taken place. One limitation of the access control list method is the poor execution efficiency due to the list needing to be searched for every access to a protected object. This method also can require enormous amounts of storage.

The storage insufficiency can be improved by decomposing the access matrix into rows (columns) and assigning the access rights contained in rows (columns) to their respective subjects (objects). This approach is known as the capability-based method (access control list method). To solve the limitation of poor execution efficiency in the access control list method, we can use a shadow register. A shadow register is used for the purpose of holding data to be used at another time. To solve the issue of requiring substantial amounts of storage in the access control list method, a protection group technique will limit the number of entries in an ACL by lumping subjects into groups which therefore reduces the overheads of storing and searching lengthy ACLs [23].

Discussion

The Biba model is the most powerful of the integrity models due to how it intertwines with the Bell Lapadula model. These models were both designed with the intention of complementing one another and when put together, they make the perfect security pair of integrity and confidentiality. The Biba model is extremely flexible as it can be changed based on the needs of the implementor. The Biba model and Clark and Wilson model are both types of Mandatory Access Control which make them more secure than Lampson's Access Matrix.

The Clark and Wilson model is especially useful in terms of preserving the correct data. The Biba model allows subjects who are authorized to make modifications to objects at any time, where Clark and Wilson does not allow unauthorized modifications to objects by subjects even if they are authorized. This is essential in always presenting and preserving the correct data. This is broad enough to allow this model to be implemented in various systems, like Biba, but in a more efficient way. Unfortunately, this model cannot determine if data is initially in a valid state. Due

to this, Biba is a more secure model when it comes to data integrity. In this model, no one subject can execute an entire operation which allows for a stronger integrity of data by not allowing one subject to ruin an entire object.

While Lampson's Access Matrix is adequate it could be considered a special use only model. Every subject within the organization has access to view who has access to objects, which could raise concerns in situations where the authorization of subjects needs to be kept confidential. The matrix can also be considered special use due to its sparseness in certain situations. In larger organizations, much of the matrix is empty, which can reduce readability and cause confusion, for example, as to whether objects are at all accessible. Therefore, the matrix is best suited for smaller, tight-knit organizations.

Conclusion

Integrity access control models ensure that all data is protected from unauthorized changes, which helps to ensure everything is reliable and correct. The Biba model is the best integrity access control model especially when it is combined with the Bell Lapadula confidentiality model. With this being said, each of the models have their own advantages over one another which can make it difficult to deem one better than the other. The Clark and Wilson model does not allow unauthorized modifications to objects by subjects, even if they are authorized. The Biba model does allow these modifications to be made, which could potentially make the data unstable if a subject is wrongfully authorized. The Clark and Wilson and Biba model both fall under the category of mandatory access control while Lampson's Access Matrix does not. The Access Matrix can be seen as more of a special use model due to its sparseness when implemented in large organizations.

For areas to further explore, the implementation of access control models in various situations would be interesting to research more about. Different organizations tend to have unique needs which makes all access control models valid for different organizations. The research done on access control devices used in information security has not been covered enough and would serve as a challenging yet rewarding research project.

References

[1] E. Sahafizadeh and S. Parsa, “Survey on access control models,” Iran, Tech. Report. 2010.

[2] V. Hu, D. Ferraiolo, D. Kuhn. *Assessment of Access Control Systems.* Gaithersburg, MD: 2006.

[3] T. Mudarri, S. Abdo Al-Rabeei, “Security fundamentals: access control models,” Technical University of Kosice, Tech. Report. August 2015.

[4] S. Osborn, R. Sandhu, and Q. Munawer, *Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies*, 02-May-2000. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/354876.354878. [Accessed: 16-Feb-2022].

[5] A. Kern and C. Walhorn, *Rule Support for Role-Based Access Control*, 01-Jun-2005. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/1063979.1064002. [Accessed: 16-Feb-2022].

[6] J. Millen, “Editor's preface to the Bell-Lapadula model,” *Journal of Computer Security*, vol. 4, no. 2-3, pp. 229–231, 1996.

[7] N. Balon and I. Thabet, *The Biba Security Model*, 27-Mar-2004. [Online]. Available: http://nathanbalon.com/projects/cis576/Biba_Security.pdf. [Accessed: 16-Feb-2022].

[8] S. Q. Blake, *The Clark-Wilson Security Model*, 17-May-2000. [Online]. Available: http://moreilly.com/CISSP/Dom2-1-clark.pdf. [Accessed: 16-Feb-2022].

[9] J. Kindervag, *Build Security into Your Network’s DNA: The Zero Trust Network Architecture*, 05-Nov-2010. [Online]. Available: http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf. [Accessed: 18-Feb-2022].

[10] A. Ometov, S. Bezzateev, N. Makitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, *Multi-Factor Authentication: A Survey*, 05-Jan-2018. [Online]. Available: https://www.mdpi.com/2410-387X/2/1/1. [Accessed: 18-Feb-2022].

[11] V. Hu, D. Ferraiolo, R. Kuhn, A. Friedman, A. Lang, M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft),* 2013. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.298.3381&rep=rep1&type=pdf. [Accessed: 18-Feb-2022].

[12] S. Osborn, *Mandatory Access Control and Role-Based Access Control Revisited,* 1997. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/266741.266751?casa_token=AwCNqUacDkYAAAAA:QXr9LnI1nfCWcLkoWZ0M8J_3z6PIlLGwj5mMqlluRXjRGSAPrbBxpZdOHAwh4kfUGRbe6ARTcSjT. [Accessed: 18-Feb-2022].

[13] I. T. L. Computer Security Division, "Role based access control: CSRC," *CSRC*. [Online]. Available: https://csrc.nist.gov/Projects/Role-Based-Access-Control. [Accessed: 23-Feb-2022].

[14] C. Landwehr, *Formal Models for Computer Security*, 03-Sep-1981. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/356850.356852?casa_token=r6v9kNWEDAkAAAAA:X4UhE3DdNcVTdFVNM8bKDKRdcbEEhRoF94TbXFxb7e19KUQD0BJkyh-JSBIrYQO7_aArn9pxnCkA. [Accessed: 25-Feb-2022].

[15] D. Chadwick, *On the Modeling of Bell Lapadula Security Policies using RBAC*, Jul-2008. [Online]. Available: file:///C:/Users/paige/Downloads/RBACZhoa.pdf. [Accessed: 25-Feb-2022].

[16] M. Toapanta, J. Nazareno, R. Tingo, F. Mendoza, A. Orizaga, and E. Mafla, *Analysis of the Appropriate Security Models to Apply in a Distributed Architecture*. [Online]. Available: https://iopscience.iop.org/article/10.1088/1757-899X/423/1/012165/pdf. [Accessed: 25-Feb-2022].

[17] "Bell-Lapadula Model: A MAC model for ... - icet.ac.in." [Online]. Available: http://www.icet.ac.in/Uploads/Downloads/MOD2.pdf. [Accessed: 25-Feb-2022].

[18] P. Garnaut and J. Thompson, *Review of Data Integrity Models in Multi-Level Security Environments*, Feb-2011. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.979.266&rep=rep1&type=pdf. [Accessed: 27-Feb-2022].

[19] *Kaufman, C., Perlman, R. and Speciner, M., Network Security (Private Communication in a Public World), 2nd edition, Prentice Hall, 2002.*

[20] T. R. Ivan, *Comparison of Data Integrity Models*, Mar-1991. [Online]. Available: https://calhoun.nps.edu/bitstream/handle/10945/43739/ADA243770.pdf?sequence=1&isAllowed=y. [Accessed: 27-Feb-2022].

[21] *Courses.cs.washington.edu*. [Online]. Available: https://courses.cs.washington.edu/courses/cse451/03sp/lectures/5-30_david_ryan.txt. [Accessed: 27-Feb-2022].

[22] "Access control: Policies, models, and Mechanisms - Springer." [Online]. Available: https://link.springer.com/content/pdf/10.1007%2F3-540-45608-2_3.pdf. [Accessed: 01-Mar-2022].

[23] "Access matrix model, capability list, Access Control List," *Protection: Basic Models*. [Online]. Available: https://courses.cs.vt.edu/~cs5204/fall99/protection/protection.basic.html. [Accessed: 01-Mar-2022].

[24] S.-B. Lee, Y.-H. Kim, J.-W. Kim, and C.-Y. Song, *A Design of MAC Model Based on the Separation of Duties and Data Coloring: DSDC-MAC*, 17-Jan-2020. [Online]. Available: https://thescipub.com/pdf/jcssp.2020.72.91.pdf. [Accessed: 01-Mar-2022].

[25] *(PDF) information flow-based security levels assessment ...* (n.d.). Retrieved March 23, 2022, from https://www.researchgate.net/publication/304351845_Information_flow-based_security_levels_assessment_for_access_control_systems . [Accessed: 23-Mar-2022].

[26] "12/4/20151 Computer Security models – an overview. - ppt download," *SlidePlayer*. [Online]. Available: https://slideplayer.com/slide/8720781/. [Accessed: 23-Mar-2022].

[27] R. Castillo, "Topic Clark-Wilson model Ravi Sandhu. - PPT video online download," *SlidePlayer*, 31-Oct-2017. [Online]. Available: https://slideplayer.com/slide/677490/. [Accessed: 23-Mar-2022].

[28] C. S. R. C. C. Editor, "glossary," *CSRC*. [Online]. Available: https://csrc.nist.gov/glossary. [Accessed: 30-Mar-2022].

[29] Fenrich, Kim. *Securing Your Control System: the "CIA Triad" Is a Widely Used Benchmark for Evaluating Information System Security Effectiveness*, Penn Well Publishing Corp, Feb. 2008, link.gale.com/apps/doc/A177028777/AONE?u=anon~37a0fd8d&sid=googleScholar&xid=37d30246.