A Survey of Computer Security Models

S.K.Muttoo[1], Sushil Kumar[2], NidhiTyagi[3]
[1]*Department of Computer Science, Delhi University, Delhi-110007*
[2]*Shobhit University, Meerut, UP-250110*
[3]*Shobhit University, Meerut, UP-250110*

[1]skmutto@cs.du.ac.in
[2]kumar.sk106@gmail.com
[3]mnidhity@rediffmail.com

ABSTRACT
A security model maps the abstract goals of the security policy of information system by specifying information flow necessary to enforce the security policy. The security model that characterize the security goal in a form, which are then mapped to system details. The security model takes the requirement and provides the necessary mathematical formulas, relationships, and structure to be followed to accomplish the security goal. This paper gives brief introduction of security model from the beginning.

KEYWORDS
Security, access control, information flow, confidentiality, subject, object, integrity, security policy, roles, permission

.

1. INTRODUCTION

Computer systems contain many resources which are called objects. The objects are assigned to the users or programs termed as subjects. Objects may be hardware (i.e. Memory, CPU etc.) orsoftware (as files, programs etc.).Subjects are end users or other programs. Protection refers to a mechanism for controlling the access of subject to object. Security refers to measure of integrity of the system. Computer security model provide controlled access to programs and data stored in computer system. [6]
The access to the data must be prevented from any unauthorized user. A secure system is one whose resources are accessed and modified as per the security policy. The access control of the security models are defined by using the concept of lattice. This paper illustrates the various security models and reviews their conceptual and theoretical structure.
The paper is divided into 9 sections.In Section 2 we describe the Bell-Lapadula security model. Section3 deals with Biba model. In Section4 considers unification ofBell-Lapadula and Bibamodel.In Section5 we describe Take grant protection model. Section6 describes Clark Wilson model. In the subsequent sections we have described various. security models viz Harrison Ruzzo Ullman, Role based access control.

2. BELL LA-PADULA MODEL

The Bell-LaPadula[1] conceptualize the model of state machine.A state machine has a set of well-defined states and the transition among these states.A system state is said to be secure if the subjects access the objects according to the security policy. Every state transition retain security bygoing from one secure state to another. And hence proves that the system meets the expectation of a security model. The BLP model examines the information flow when a subject modifies the object. The BLP model involves the set of subject(S), the set of objects (O), and the set of various access operations (A).The access operations include execute, read, append and write. A lattice L is defined of security levels with a partial ordering ≤ (dominates). [5]
The state of the system is used for checking its security, so the set of model has to capture all current permissions and all current instances of subjects accessing objects. This leads to a rathermore complicated state set B x M x F, where,

- B=P(SxOxA) is the set of current accesswhere ,P stands for power set . An element bϵB is a collection of tuples(s,o,a), indicating that subject s currently performs operation 'a' on object 'o'.M is the set of access permissions matrices M=(M_{so}) sϵS ,oϵO.
- F = L_C x L_SxL_O is the security level assignments. An element fϵF is a triple (f_s,f_c,f_o), where
- f_s : S ⟶ L gives the maximal security level each subject can have,
- f_c : S ⟶ L gives the current security level of each subject,
- f_o: O ⟶ L gives the classification of all objects.

The current level of a subject cannot be higher than its maximal level, hence f_c '≤ ' f_s, in words "f_s dominates f_c".[6]
The Bell-LaPadula model focuses on data confidentiality and controlled access to classified information.

[1] *S.K.Muttoo, Department of Computer Science , University of Delhi, Delhi*
Email: [1] skmutto@cs,du.ac.in
[2] *Sushi kumar, Department of Computer Science , Shobhit university, Merrut*
Email: [2]kumar.sk106@gmail.com

This journal is cited as : **JIMS 8i-Int'l J. of Inf. Comm. & Computing Technology(IJICCT)**

2.1 PROPERTIES

We state the properties without proof:-

1. The Discretionary Access Control (DAC) Property –the DAC property states the use of an access matrix to describe the discretionary access control.

2. The Simple Security(SS) Property – states that a subject cannot read an object which is at a higher security level than of a subject. (no read-up).

3. The *-property ("star"-property) - states that a subject at a given security model should not write to any object at a lower security level than of a subject.(no write-down).

4. Tranquility principle -The tranquility principlestates that the security levels do not alter during the operation of the system. And so states that the security levels never change as to breach the security policy.[6]

2.2 LIMITATIONS

1. The BLP security model only addresses the confidentiality.

2. Security level of objects is static.
3. The tranquility principle restricted its suitability to systems where security levels are static.

4. The BLP security model is very tough to employ in real life as categorization of data changes time to time. [12]

3.BIBA MODEL

The Biba[8] model addresses integrity. The security modelislike BLP model follows the concept of a state machine and having a lattice (L,≤) of integritylevels. Integrity manages the correctness of data The two functions fs:S L and fo: O L are defined which specifies the integrity levels to subjects and objects. These levels make the basis for defining integrity policies that refer to the corruption of ‘clean’ high level entities by ‘dirty’ low level entities. In the integrity lattice, information flows downside. Biba defines two main rules .The first rule states that a subject cannot write data to an object at a higher integrity level(no write up).The second rule states that a subject cannot read data from a lower integrity level(no read down).[6]

3.1 STATIC INTEGRITY LEVELS

Mirroring the tranquility property of BLP, we can state policies where integrity levels never change. The following two integrity properties are the dual of the mandatory policies.

1. Simple integrity : if a subject s can modify object o, then $f_o(o) \leq f_s(s)$(no write up).

2. Integrity * : if a subject s can read object o, then s can have write access to some other object p only if $f_o(p) \leq f_o(o)$ (no read down).[2]

3.2 DYANAMIC INTEGRITY LEVELS

The next two integrity properties automatically adjust the integrity level of an entity if it has come into contact with low level information.

3.2.1Subject low watermark property:this property states that a subject s can read any object o. the object o can be at any integrity level and the new integrity level of the subject is defined as infimum($f_s(s)$,$f_o(o)$), where $f_s(s)$ and $f_o(o)$ are the integrity levels.The integrity levels are before the operation.[6]

3.2.2Object low watermark property: this property states that a subject s can modify an object o. an object o can be at any integrity level andThe new integrity level of the object is defined as infimum($f_s(s)$,$f_o(o)$), where $f_s(s)$ and $f_o(o)$ are the integrity levels The integrity levels are before the operation[6].

The integrity level infimum($f_s(s)$,$f_o(o)$), the greatest lower bound of $f_s(s)$ and $f_o(o)$, is well defined because we are dealing with a lattice of integrity levels. This security model is directed toward data integrity (rather than confidentiality) [2]

3.3ADVANTAGES AND DISADVANTAGES

There are a number of benefits that come from using the Biba model. The first benefit of the model is that it is fairly easy to implement the integrity policy as compare to Bell-La Padula.And the other benefit is that biba security model many polices that can be used as per the requirement.

If the strict integrity property is too restricting, one of the problem with this model is selecting the right policy. The dynamic policies could be used in its place.TheBiba model is not without its drawbacks. For this reason, the Biba model

should be combined with another model. A model such as the Bell-LaPadula could be used to complement it. [7]

4.BLP AND BIBA MODEL

BLP model[12] focus on the security of information systems from the perspective of information confidentiality, while view of Biba Model is protecting integrity of information. To an information system, only emphasizing confidentiality or integrity cannot guarantee truthful information. So by combining confidentiality and integrity of these security models, Ravi S Sandhu[13] has a security model which handle both confidentiality and integrity with lattices. From the analysis of BLP model and Biba model, access of the subject to the object is mainly based on sensitive label to determine the flowing direction of information, considering sensitive labels of confidentiality and integrity together. In the following, we will establish access control concept lattice theory with sensitive label combining confidentiality and integrity.[10]

Definition 1 *SO = SUO* is called as a component set in computer systems, where *S* is a subject set and *O* is an object set.

Definition 2 *SC = CLUILUCK* is called as a security class set, where *CL* is a confidentiality label set, *IL* is an integrity label set and *CK* is a categories set.Partial order relation exists between the elements of set *CL*, for examples, *CL*= {TS (Top Secret), S (Secret), C(Confidential), U (Unclassified)}, where U ≤ C ≤S≤TS.Partial order relation ≤ also exists between the elements of set *IL*, for examples, *IL*= { C (Crucial), I(Important), U (Unknown)}, where U ≤ I ≤ C. The elements in set *CK* represent functions, department, and so on. There don not exist ordinal relation between elements, for example, *CK*= {finance, production, marketing}.In the following, formal context in formal concept analysis theory will be extended to computer access control model.[14]

Definition 3 A triple *AK*= (*SO*, *SC*, *IR*) is called an access control context, where *SO* is a component set, *SC* is a security class set, *IR* is a binary relation between *SO* and *SC*. For an arbitrary component x ϵ *SO*, a security class *y*ϵ*SC*,

xIRy represents that component *x* has security class *y*.

Definition 4 In an access control context, for xϵ*SO*, y1, y2ϵ*SC*, the elements in security class set have the following dependency relations:

1) If y1,y2ϵ*CL*, y1'≤'y2, when $x_1 Ry_2$holds, $x_1 Ry_1$ holds;

2) If y1,y2ϵ*IL*, y1'≤'y2, when $x_1 Ry_1$holds, $x_1 Ry_2$ holds.

From definition 4, the dependency relations of security class include:

1) in a confidentiality label set, if a component has higher confidentiality label, then the component has lower confidentiality label automatically in access control context;

2) On the contrary, in an integrity label set, if a component has lower integrity label, then the component has higher integrity label automatically in access control context.

Definition 5 In an access control context, if a binary pair*AC*= (*A*, *B*) satisfies *A* = *g* (*B*), *B* = *f* (*A*), then we call the binary pair (*A*, *B*) as an access formal concept, where *A* is an element of the power set *P*(*SO*) and is called as extension offormal concept *AC*; *B* is an element of the power set*P*(*SC*) and is called as intension of formal concept *AC*. In addition,all of the access formal concept set in access control context*AK*is marked as *CS*(*AK*). By the definition of mapping *f* and *g*, in an access formal concept A*C* = (*A*, *B*), the subjects and objects of the computer system having security class set B are all in extensionA, and all the subjects and objects in extension A have security classes included in intension B.[13]

5.TAKE GRANT PROTECTION MODEL

The take-grant protection model was introduced by Lipton and Snyder[10] in 1977.The two access rights are defined in this model:- take and grant. These two access rights control the read and write operation. Thus these two access rights handle the information flow which leads to safeguarding entities of a system.

Take grant model is implemented using the rules defined by directed graphs.

5.1LIMITATIONS

The Take Grant model also has some following limitations:-

- does not deal with the integrity issue.
- unprotected to attacks such as Trojan horse.
- Another problem with the model is the number of nodes in the graph, as the number of nodes and arcs increases it will be hard to define a graph and prove to be secure.

6.CLARK WILSON MODEL

The Clark–Wilson[3] integrity model provides a basis for defining and analyzing an integrity policy for a computing system. The model is based on the integrity of information and the notion of transaction. It aims to protect the information integrity. Information integrity is preserved by safeguarding the data items in a system from any illegal access. An integrity policy describes how these data items must be protected while the system transit from one system state to other. The model defines two rules:- enforcement rules and certification rules. These rules (enforcement and certification rules) define data items and processes that lays down the foundation for an integrity policy. The base of the model is depend upon the concept of transaction.[1]A well-formed transaction is a sequence of operations that takes a system from one stable state to another stable state.

In this model the integrity policy notifies the integrity of the transactions and information. To separate the duty requires

that both the certifier of a transaction and the implementer must be different entities.

The Clark Wilson model defines numerous data types which specify both data items and processes that operate on those data items. The main data type in the Clark–Wilson model is a Constrained Data Item (CDI). Another data type is Integrity Verification Procedure (IVP) which make sure that all CDIsin the systemare valid at a certain state. All Transactions within the system are defined by Transformation Procedures (TPs) to enforce the integrity policies. A Transition Procedure must carry the system from one stable state to another stable state. TPs takes as input a CDI or Unconstrained Data Item (UDI) and produces result as a CDI. UDIs represent system input. A TP must make sure that it transmit all permissible values of a UDIs to a right CDI via some certification.[14]

7.THE CHINESE WALL MODEL

The Chinese wall model proposed by Brewer and Nash [4] models access rules in consultancy business where analysts have to ensure that no conflicts of interest arise when they are dealing with different clients. Informally conflicts arise because clients are direct competitors in the same market or because of the ownership of companies. The Chinese Wall security policy is perhaps as significant to some parts of the commercial world as Bell and La Padula's policies are to the military. It can be most easily visualized as the code of practice that must be followed by a market analyst working for a financial institution providing corporate business services. Such an analyst must uphold the confidentiality of information provided to him by his firm's clients; this means he cannot advise corporations where he has insider knowledge of the plans, status or standing of a competitor. Analysts have to adhere to the following security policies:
There must be no information flow that causes a conflict of interest. Conflict of interest do not only arise from objects currently accessed but also from objects that have been accessed in the past. We therefore need a means of recording the history of subjects' actions. For this purpose, we introduce a Boolean S x O matrix N with,

Ns,o = true , if the subjects is allowed to access to object o,
False, if the subject s has never access to object o.

If you set Ns,o = false for all s ϵ S and all o ϵ O, you have secure initial state.

The first security policy deals with direct information flow. We want to prevent a subject from being exposed to conflict of interest. Therefore, access is granted only if the object requested belongs to:
A company dataset already held by the user , or
An entirely different conflict of interest class.

8.THE HARRISON RUZZO ULLMAN MODEL

In this section we discussed The Harrison-Ruzzo-Ullman(HRU)[12] model. The HRU model describes about the access rights that how they can be altered. HRU model also states that how subjects and objects are created and deleted. The HRU model defines an authorization system which deals with the access rights. BLP ,BIBA and any other model discussed so far does not state policies for changing access rights for creation and deletion of subjects and objects.The HRU model consists of a set of subjects *S*, a set of objects *O*, a set of access rights *R*, an access matrix $M = (Mso)\ s\varepsilon S,\ o\varepsilon O$, the entry *Mso* is the subset of *R* specifying the rights subject *s* has on object *o*.[11]

9.ROLE BASED ACCESS CONTROL MODEL

In the role-based access control model the access policies depend on the roles of a particular person. Users have specific roles (such as teacher ,student, librarian etc.). In the role-based access control model, the permissions to perform certain operations is assigned to specific roles instead of assigning permission to each user directly. The mechanism for defining the roles of a particular user must include the inputs from the organization in the perspective of users view[15].There are three rules defined for RBAC as:
1.Role assignment: A subject must be assigned a role and only after it can entertain permission.
2.Role authorization: the role of a subject must be authorized. This rule make sure that the user can perform only those task for which they are authorized.
3.Permission authorization: A subject is permitted only if the permission is authorized for the subject as per the assigned role.
Taking consideration of rules 1 and 2, the rule 3make sure that the users can entertain only those permissions for which they are authorized as per the role.While defining an RBAC model, the following terms are taken into consideration:-

- S (Subject) = A user or a system agent and A subject can have multiple roles.
- R (Role) = A user's Job function which defines an authority level and A role can have multiple permission.
- P (Permissions) = a mode of access to an object or a resource and A permission can be assigned to many roles.
- SE (Session) = A mapping involving S, R and P
- SA (Subject Assignment) and PA (Permission Assignment)

- RH (Role Hierarchy). Role Hierarchy is defined as a partially ordered Role hierarchy. It is also shown as: ≥ (The a ≥ b means that a inherits the permissions of b.)

So by taking above definitions into consideration, RBAC is implemented. A constraint takes place while inheriting the permissions from opposing roles, so in this way it can be defined for dividing the duties or responsibilities. For example, the same person should not be allowed to both create a login account and to authorize the account creation. Thus, using set theory notation:
PA⊆P X R and is a many to many permission to role assignment relation.SA⊆ S X R and is a many to many subject to role assignment relation.
RH ⊆R X Ra subject may have multiple simultaneous sessions with different permissions.[16]

CONCLUSION

In this paper we have studied various formal models for security. Formal models for computer security are needed in order to organize the complexity inherent in both "computer" and "security." The formal models for security Bell La Padula which captures policies for confidentiality (Bell La Padula) and for integrity (Biba, Clark Wilson). Some models apply to environments where polices are static (Bell La Padula) , other consider dynamic changes of access rights (Chinese Wall).Formal security models like Bell La Padula have a prominent place in high assurance security evaluations.Informal models like Clark Wilson are more of descriptive framework for expressing security policies. The take-grant protection model is a formal model used in the field of computer security to establish or disprove the safety of a given computer system that follows specific rules. The Harrison-Ruzzo-Ullman model outlines how access rights can be changed and how subjects and objects should be created and deleted. Current implementation of security is based on role-based access control. In Role based access control, access decisions are based on the roles that individual users have as part of an organization.

FUTURE SCOPE

we propose to implement all these security models for university security system as university based access control model.

REFRENCES

[1]Bell, David Elliott and LaPadula, Leonard J. (1973). Secure Computer Systems: Mathematical Foundations (PDF). MITRE Corporation
[2] Carl.E.Landehr,Formal Models for Computer Security, Naval Research Laboratory, Washington DC.
[3] Clark, David D.; and Wilson, David R.; A Comparison of Commercial and Military Computer Security Policies; in *Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy (SP'87), May 1987*
[4] D. Brewer and M. Nash. The chinese wall security policy. In Proc. 10thIEEE Symposium on Security and Privacy, pages 206–214, May 1989.
[5] David Elliott Bell, Looking Back at the Bell-La Padula Model,2005.
[6] D.Gollmann, Computer Security, John Wiley & Sons, 2003.
[7] Dr. David F.C. Brewer and Dr. Michael J. Nash, the Chinese wall security policy
GAMMA SECURE SYSTEMS LIMITED,9 Glenhurst Close, Backwater, Camberley, Surrey, GUI 7 9BQ, United Kingdom.
[8] K. J. Biba, "Integrity Considerations for Secure Computer Systems."The MITRE Corporation. Tech. Rep.: MTR-3153, 1977
[9] Lipton, Richard J.; Snyder, Lawrence "A Linear Time Algorithm for Deciding Subject Security" . *Journal of the ACM* (Addison-Wesley) **24** (3): 455–464 ,1977
[10]M. Bishop. Computer Security: Art and Science. Addison Wesley, 2003.
[11]M.H. Harrison, W.L. Ruzzo, and J.D. Ullman.Protection in operating systems.*Communicationsof the ACM*, 19(8):461–471, 1976.
[12] Peter Y. A. Ryan, Mathematical Models of Computer Security
[13]RathnakarAcharya, Dr. V. Vityanathan ,Dr. Pethur Raj Chellaih**,**Secured Information Accessbased on Bell LaPadula Model A Case of Novel Publishing Company,Volume 11– No.8, December 2010
[14]Ravi.S.Sandhu, Lattice based access control models, George Mason University
[15]Sandhu, R., Coyne, E.J., Feinstein, H.L. and Youman, C.E. (August 1996). "Role-Based Access Control Models"(PDF). *IEEE Computer* (IEEE Press) **29** (2): 38–47.
[16]YolantaBeresnevichiene, A role and context based security Model, *Technical Report* Number 558 ,Computer Laboratory UCAM-CL-TR-558 ,ISSN 1476-2986