Prove Theorem 6-1 of Bishop's for the strict integrity policy of Biba's model.

Theorem 6-1. If there is an information transfer path from object $o_1 \in O$ to object $o_{n+1} \in O$, then enforcement of the low-water-mark policy requires that $i(o_{n+1}) \leq i(o_1)$ for all $n > 1$.

Answer:

The notion of an information transfer path is defined as[4]:

Definition 6-1: An information transfer path is a sequence of objects o_1, ..., o_{n+1} and a corresponding sequence of subjects s_1, ..., s_n such that s_i reads o_i and s_i writes o_{i+1} for all i, 1 $\leq i \leq n$.

If there is an information transfer path from object $o_1 \in O$ to object $o_{n+1} \in O$, we assume that every read and write action should be conducted as per the sequence in *Definition 6-1*. According to the rules of Strict Integrity Policy (class note page 33) in Biba's model:

Step1:

For $s_n \in S$ can read $o_n \in O$ if and only if $i(s_n) \leq i(o_n)$ which is also known as "no reads down". The property states that a subject can read an object only if the integrity level of the subject is less than the integrity level of the object.

For $s_n \in S$ can write $o_{n+1} \in O$ if and only if $i(o_{n+1}) \leq i(s_n)$ which is also known as "no writes up". This property states that a subject can write to an object only if the object's integrity level is less than or equal to the subject's level.

According to definition 6-1, information transfer path rules that s_i reads o_i and s_i writes o_{i+1}, the above-inequality can be derived from the definition of the above Strict Integrity Policy.
Combining the above two inequality statements, and by transitivity therefore, $i(o_{n+1}) \leq i(o_n)$.

Step2:

Applying the Strict Integrity Policy again,

For $s_{n-1} \in S$ can read $o_{n-1} \in O$ if and only if $i(s_{n-1}) \leq i(o_{n-1})$ known as "no reads down".
For $s_{n-1} \in S$ can write $o_n \in O$ if and only if $i(o_n) \leq i(s_{n-1})$ known as "no writes up".

Again, by transitivity, therefore subject s_{n-1}, $i(o_n) \leq i(o_{n-1})$.

Step3:
By using mathematical induction: for all $n > 1$ the integrity requirements should be $i(o_{n+1}) \leq i(o_n) \leq \ldots \leq i(o_1)$. Therefore, the Theorem 6–1 has been proved!

ex2

The integrity level of subjects will remain unchanged if we elevate the object levels to be above the subject's level instead of lowering the subject's integrity level.

Exercise 3

Give an example that demonstrates the integrity level of subjects decreases in Biba's low-water-mark policy. Under what conditions will the integrity level remain unchanged?
Answer:

The example will use the read function under the Biba's low-water-mark policy.

Assuming that there is a set of integrity level {ISP (System Program), IO(Operational), ISL(System Low)} (from the highest to lowest) in system. Assuming that there are two integrity categories {ID (Development), IP(Production)}.

The subject-to-integrity and object-to-integrity tables we designed are as follow:

Subject	Integrity levels (for read function only)
Ordinary users	(ISL, { IP })
Programmers	(IO, { ID})
System manager	(ISP, { IP, ID })

Object	Integrity levels
Development code	(ISL, { ID })
Production code	(IO, { IP })
System programs	(ISP, { IP, ID })

As shown in tables, After system manager read production code, the integrity level of system manager will be altered into IO as i'(s) = min(i(System manager), i(Production code)). Similarly, the integrity level of system manager will become ISL after he reads the development code, which results in integrity level of subjects decreases in Biba's low-water-mark policy. This example illustrates that the integrity level will decrease when using Biba's rule.

If the integrity level remains unchanged, the subject S with the integrity level i(s) can only read the objects whose integrity level are no less than i(s). In our table above, the programmers can only read production code or system programs.

ex3

Exercise 4

Suppose a system used the same labels for integrity levels and categories as for security levels and categories. Under what conditions could one subject read an object? Write to an object?

In the Bell-LaPaula security model, the labels for security levels of the subjects are: Top Secret, Secret, Confidential and Unclassified. The categories of the objects are also labeled the same.

In order for a subject (s) to read an object (o), the condition must be: iff L(s) dom L(o) and s has the permission to read o. In addition, the "no reads up" rule applies.

In order for the subject to write an object, the condition must be: iff L(o) dom L(s) and s has the permission to write o. In addition, the "no writes down" rule applies.

In the Biba's integrity model, the labels for the integrity level are: Highly trusted, Medium trusted, Low trust. The categories of the objects are also labeled the same.

In order for a subject (s) to read an object (o). the condition must be: s can read o if and only if i(s) ≤ i(o) and follows a "no reads down" rule.

In order for the subject to write an object, the condition must be: s can write to o if and only if i(o) ≤ i(s) and follows a "no writes up" rule.

The rules are shown in table:

	Bell-LaPaula security	Biba integrity
subject s read object o	iff L(s) dom L(o)	i(s) ≤ i(o)
subject s write object o	iff L(o) dom L(s)	i(o) ≤ i(s)

ex4不用看

ex5

Exercise 6

Explain why the system controllers in Lipner's model need a clearance of (SL, {D, PC, PD, SD, T}).

Answer:

The Lipner's model leverages two components: Bell-LaPadula security model and Biba integrity model. As such, the Lipner's model consists of two security clearance: AM, SL (ordered from highest to lowest) and five categorie: D, PC, PD, SD, T. In Lipner's model, the system controllers have clearance as follows: (SL, {D, PC, PD, SD, T}).

According to the rules of Bell-LaPadula security model, subject S can read an object O if and only S dom O (or no reads up) while subject S can write to O if and only if O dom S (or no writes down).

For read right, system controllers have SL security level in all the categories[5] because they have the responsibility to monitor, control or govern the processes and data in the system. Therefore, system controllers have to have read access to all objects, including development code, production code/data, tools and system programs.

System controllers have no write access to development code, production code/data, tools and system programs, preventing above-mentioned objects from modification by the system controllers. However, the system controllers have downgrade privilege because they need to install code after it is certified for production so that other parties cannot write to it[6].

ex6

Construct an access control matrix for the subjects and objects of Lipner's commercial model. The matrix will have entries for *r* (read) and *w* (write) rights. Show that this matrix is consistent with the requirements listed in Section 6.1.

sol:

SL<AM
ISL<IO<ISP

read if i(s) <= i(o)
write if i(o) <= i(s)

{null}

is a subset of

{SP} {SD} {SSD}

are subsets of

{SP,SD} {SP,SSD} {SD,SSD}

are subsets of

{SP,SD,SSD}

{null}

is a subset of

{ID}

is a subset of

{IP}

is a subset of

{IP,ID}

Subject/Objects	Development code / Test Data	Production code	Production Data	Software Tools	System Programs	System programs in modification	System & Application Logs	Repair
Ordinary Users		R	RW	R	R			RW
Application Developers	R		R					
System Programmers					RW			
System Controllers	W	W	W	W	RW			W
System managers and auditors	W		W		R	W	W	W
Repair		R						RW

ex7
ex8 不用看
ex9 阐述lipner
ex10-12 不用看