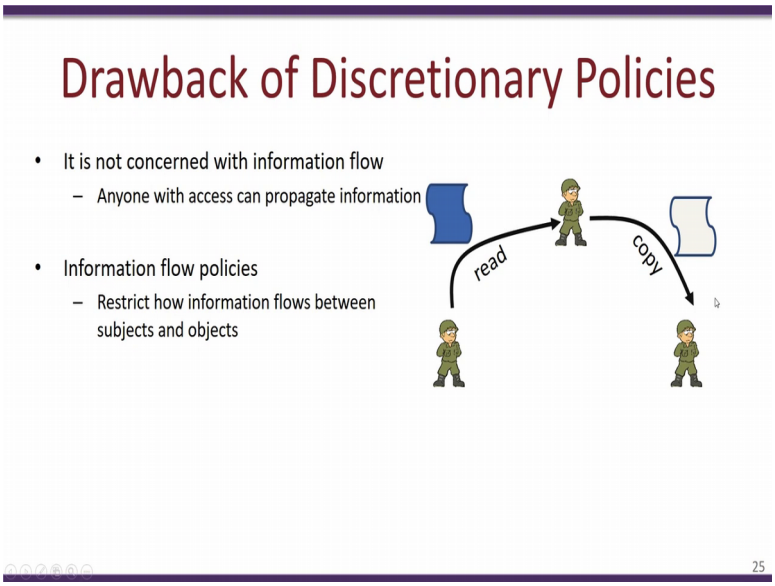
Information Security 5 Secure System Engineering
Professor Chester Rebeiro
Indian Institute of Technology Madras
Mandatory Access Control
Mod05_Lec30

Hello and welcome to this lecture in the course for secure system engineering, in the previous lecture we have been looking at access control mechanisms in particular we have been looking at discretionary access control and we also looked at the mechanisms in Unix Linux systems where discretionary access control mechanisms are implemented, now there are certain drawbacks of discretionary access control mechanisms, in this lecture we will look at the drawback of discretionary access control and then look at a stronger access control mechanism which is based on information flow, so we start this lecture the drawbacks of discretionary access control.

(Refer Slide Time: 1:04)



So essentially let us say that we have three subjects A, B and C and A is the owner of a file and he gives the access to B to read the file, from the previous lecture we know how this is made possible with something as rudimentary as the access control matrix, essentially in the access control matrix the cell corresponding to this object the file and the subject would have the ownership present in it, now since the subject is the owner of that file, he can grant access to another subject B to read the file and this is done by entering the read attribute in the cell corresponding to the subject B and this specific file.

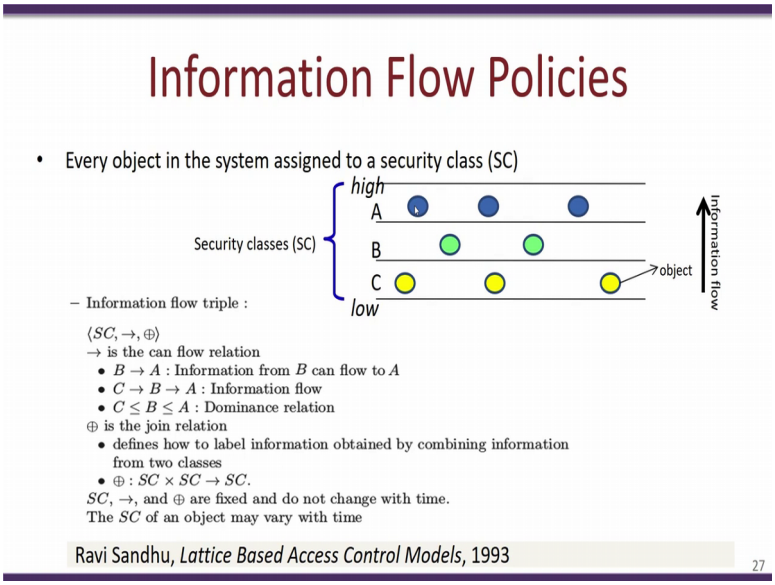
So what discretionary access control would permit is that B can only read to the file, it cannot write or execute or do any other operation on this particular file, further assuming that this subject B is the only non-owner who has access to this particular file, it would mean that no one else in that particular system would be able to read the file, so what discretionary access control does not check is that this subject B could make a copy of the file and create a totally new file and this file can be then pass on to other subjects.

Thus what we see is that the file which was created by subject A and meant to be read only by subject B the information in that file also passes to other subjects like C who was not supposed to have actually got the information from that file, so essentially the main drawback of discretionary access policies is that it is not concerned with information flow, it cannot do checks to prevent subject B from copying the contents of this particular file to another subject, in this particular lecture we look at the stronger form of access control based on information flow policies, with these policies it will prevent subject B from passing on the information to any other subject.

(Refer Slide Time: 3:43)

Another problem with discretionary access policies is the issue with Trojan horses, essentially when a subject B you can assume that subject B is a process running in a system, so when the subject B is affected by a Trojan horse, the Trojan would get to inherit all the subjects privileges.

(Refer Slide Time: 4:09)



With information flow policies every object in the system is assigned to a specific security class, for example over here we see three security classes A, B and C, the object in the security class A that is essentially these the blue objects, the objects in the security class B on the green objects and the object in the security class C are these yellow objects, now what the system would provide is some rules which would permit information to flow between these security classes.

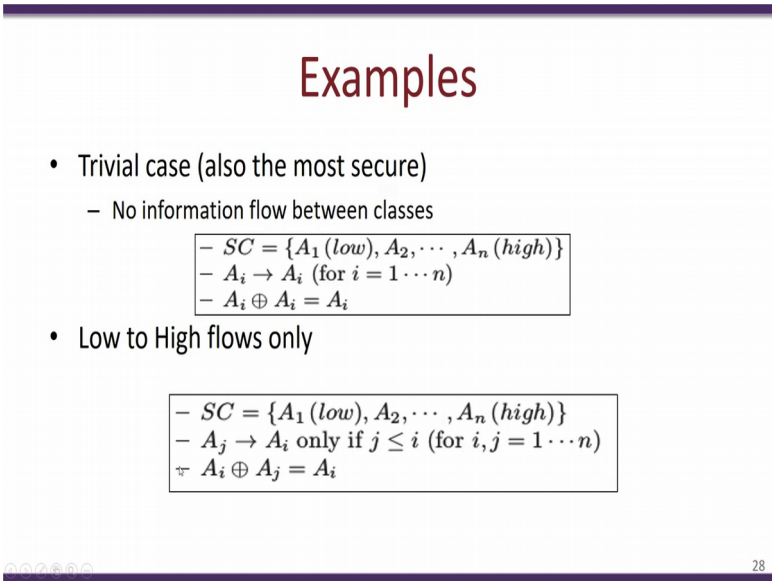
So this information flow is defined by this triple security class, flow operator which is this arrow sign and then join relationship, so we can actually define rules to decide how information should flow across the security classes, for example if we write something like this B flows to A, it would mean that information from B can flow to A that is information from B flow to this security class A, similarly we could also write something like this where information from C flows to B and information from B flows to A.

Another way of representing the same thing is by using this so called dominance relation, in this notation what we say is that A dominates B and B dominates C, this is because A can obtain all the information of objects present in B and therefore A dominates B, further we can obtain all the information present in security class C and therefore B dominates C, further we also define something known as the join relation, so this join relation defines how to legal information obtained by combining information from two classes.

Suppose let us say that we take a particular object present in security class B and take another object present in security class A, suppose we actually create a third object which is based on

these two objects that is the green object and the blue object, so the join relation would define the security class for this third object.

(Refer Slide Time: 6:56)



Let say this with some examples, so will take the most strictest form of information flow and show how we can define a particular case where no information can flow between classes, so that is this example over here and what we see in this example is that we define security classes by the set A1 to AN, where A1 is the lowest security class and AN is the highest security class, then we define that information can flow from AI to AI and nowhere else.

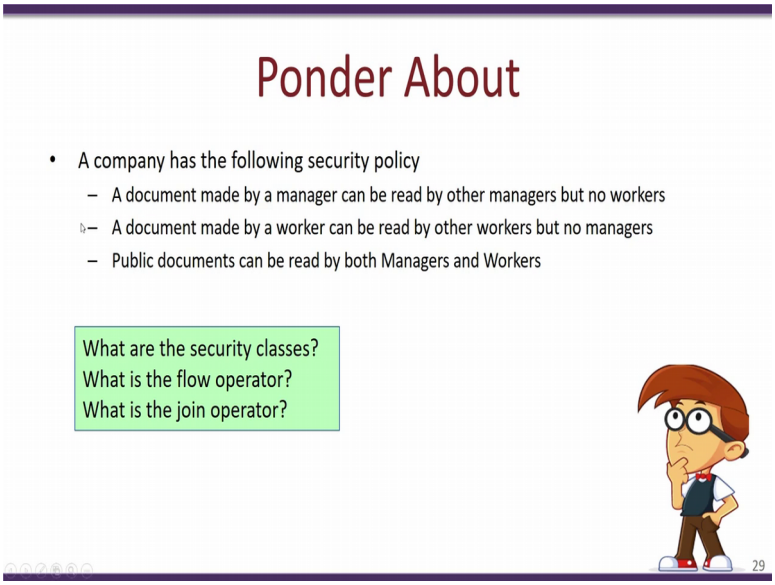
So note and we are defining the information flow in such a way that information can flow only between objects in a specific class and not across different security classes, we also hence define the join relation as follows where AI joins with AI will give you other object in AI itself, so what it means is that if we take two objects in a certain security class and we join is two objects it would create a third object the same security class.

Now let us relax this strong assumption where we do not want to have information flow between classes, we will see another example where we only permit information flow from a lower security class to a higher security class and not vice versa, so as before we define security class A1 to AN ranging from low to high and define the flow operation as follows.

A of J flows to A of I only if J is less than or equal to I this would permit information flow from a lower class to a higher class, similarly the join relationship is defined as follows, AI joins with AJ would give you AI that is when you join information from a lower security

class with a higher security class the net result is an object the higher security class, so note that with this example what we are achieving is information flow from low to high only.

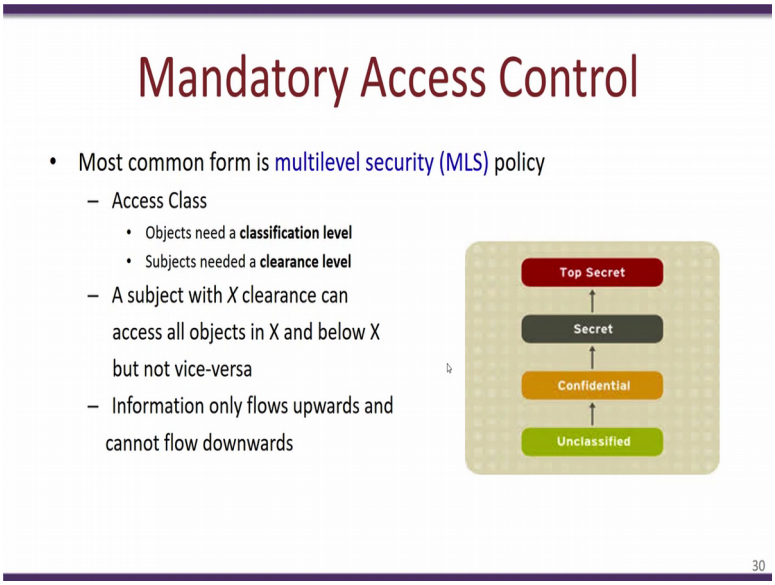
(Refer Slide Time: 9:31)



So this is something you can think about is assume that there is a company which has the following security policy, a document made by a manager can be only read by other managers in the company and no worker should be able to read that particular document, document made by a worker can be only read by other workers in that particular company and no manager should have any access to read that particular document.

Further around a third class of documents which are known as public documents, so these public documents can be read by the both the managers as well as the workers, now you have to think about how would you define security classes for this particular company, what is the flow operator to achieve this particular security policy, further what should be the join operator achieve this particular security flow policy.

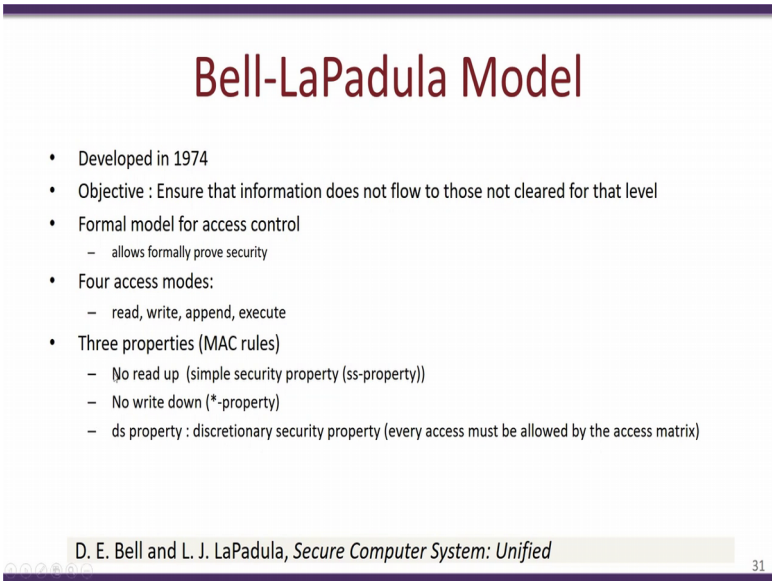
(Refer Slide Time: 10:41)



We will now look at the mandatory access control mechanism, so the MAC or the mandatory access control mechanism is the most common form of a multi-level security policy or an MLS policy, in this particular policy we define four access classes, these are top-secret, secret, confidential and unclassified, every object in the system is given a particular classification level that is an object the system could be either classified as top-secret, secret, confidential or unclassified.

Similarly every subject like a user of that system is also given a particular clearance level, so for an example if a subject X is present in that system, that subject get a clearance level of top-secret, secret, confidential or unclassified, based on this clearance and classification levels we can then define rules to decide which subject can access which object.

(Refer Slide Time: 12:01)

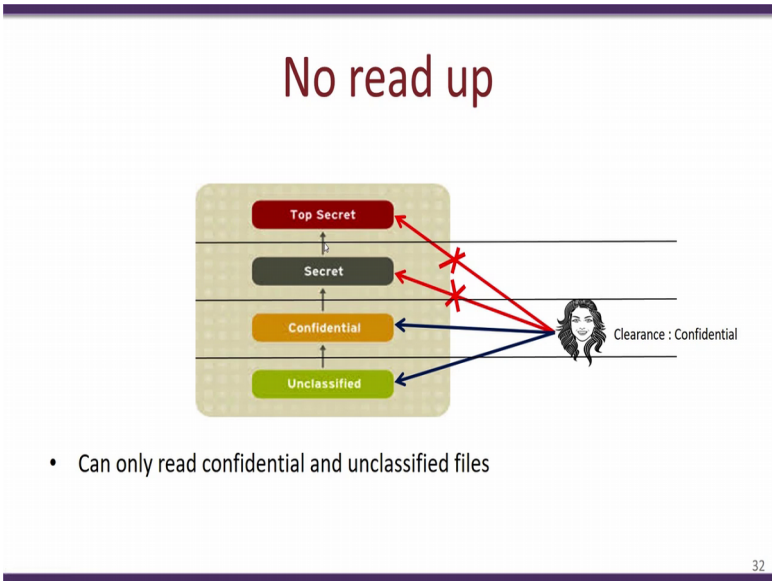


So one of the most common forms of the MLS policy Bell-LaPadula model, so this was developed by Bell and LaPadula and this was developed in 1974, the objective of this particular model is to ensure that information does not flow to those are cleared for that level, so the Bell-LaPadula model provides three properties or three rules, so Bell-LaPadula model is the first model for access control which allows to formally prove security in assistant.

There are four access modes read, write, append and execute, so these four access modes are defined between subjects and objects, in another words these four access modes are defined for clearance levels and classification levels, so it would say that a subject with a certain clearance level can access objects in a certain classification level.

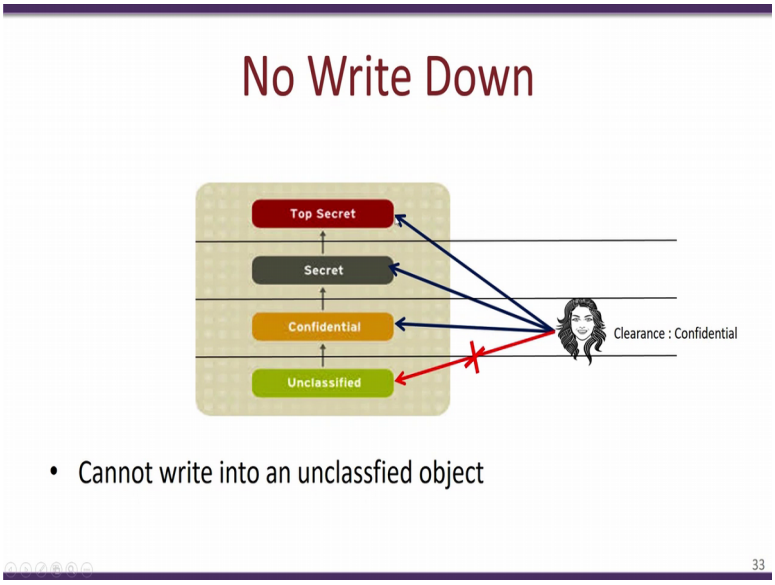
So Bell-LaPadula model defines three different properties, it defines no read up or also known as the simple security property or the SS property, it also defines a second property known as no right down or the star property and finally it defines discretionary security property which mediates every access based on the access matrix, so let us look at what these two policies are no read up and no right down

(Refer Slide Time: 13:42)



Essentially with no read up this is what happens, let us say you have a subject with a clearance level of confidential, so with no read up it would mean that this subject cannot read any objects having a high classification level, so for example this subject will not be able to read any secret objects or any top-secret objects, on the other hand this subject which has a clearance levels of confidential can read all the objects which are classified as confidential as well as all the objects which are unclassified, thus we see that information flow is only restricted from a lower classification level to a higher classification level and not vice versa.

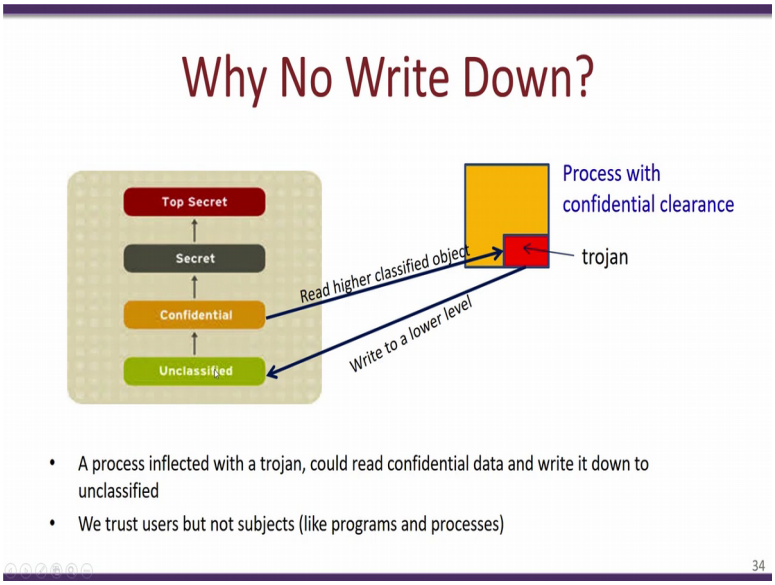
(Refer Slide Time: 14:43)



Additionally the Bell-LaPadula model also has is second property known as no right down, so what this particular property means is that while a subject with a clearance level of

confidential can write objects in confidential level or secret level or top-secret level, it will not be able to write to any unclassified objects, now this particular property is a bit difficult to understand, essentially what we are restricting here is that a user with a certain clearance level cannot right to objects which are at a lower classification level, on the other hand this particular subject can write to all objects at a higher classification level.

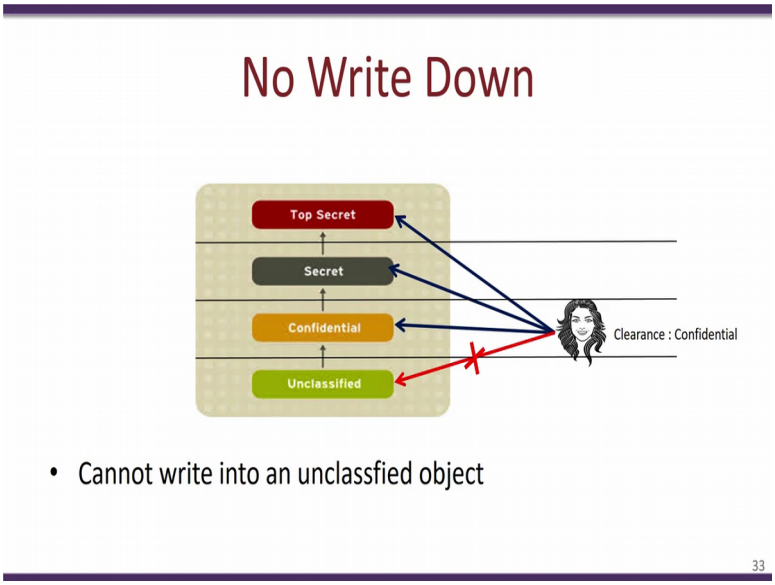
(Refer Slide Time: 15:28)



Now in this particular slide we will see why the Bell-LaPadula model defines no right down, let us assume that we have a process over here which is having a confidential clearance, this meant to say this particular process can read objects that are classified as confidential, now let us assume that this process is infected by a malware or a Trojan as we know when this Trojan executes it inherits all the privileges of its parent process, in this case the Trojan will run with a clearance of confidential.

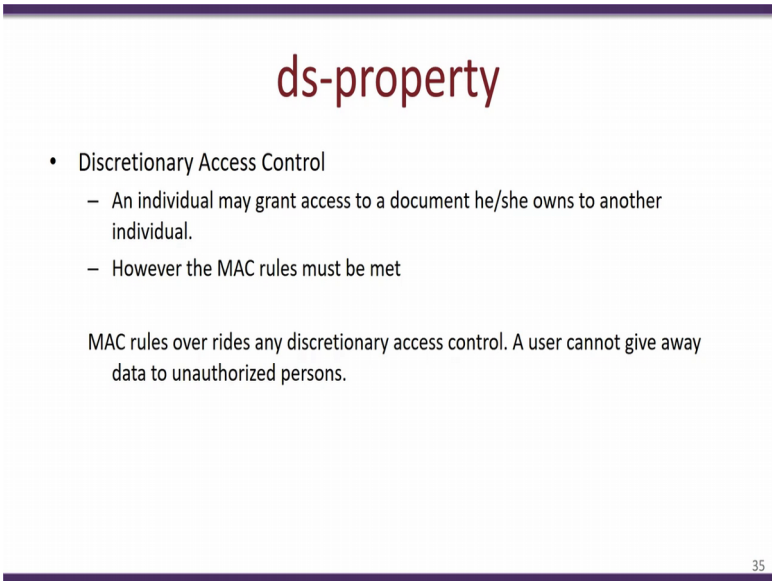
Therefore the Trojan can read all the confidential files, now what the Trojan can do if there is no right down policy what this Trojan could do is that it could write this confidential files to the classified level, thus we see that there is a flow of information from confidential to unclassified, in order to prevent such flows from a higher classification level to a lower classification level the Bell-LaPadula model defines the node right down policy.

(Refer Slide Time: 16:46)



So another thing to notice over here is that while the Bell-LaPadula model prevents writing to files which are at a lower classification level, it does not prevent writing to files at higher classification levels, so this means at subject with a clearance of confidential can write files which are secret and top-secret, however this subject will not be able to read the other files, so this particular rule in the Bell-LaPadula model is added so as to achieve a formal proof of security.

(Refer Slide Time: 17:23)



The third property which the Bell-LaPadula model defines is the DS property which stands for discretionary access control, so what it say is that even though you have a mandatory access control or a MAC layer defined, nevertheless you should still have a discretionary

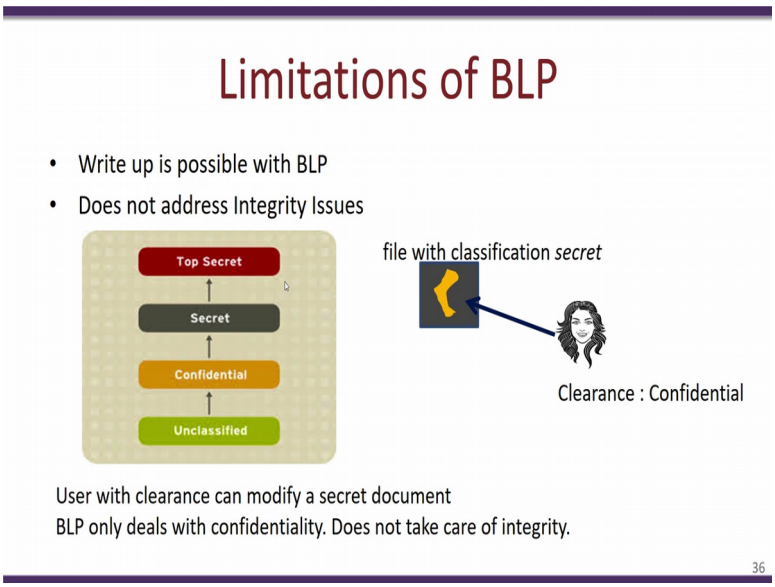
access control mechanism in your system, essentially the MAC rules overwrite the discretionary access control policies, a user cannot give away data to unauthorised persons.

Now with the discretionary access control policies are subject may grant access to a document that he or she owns to another individual, however this can only be permitted provided the MAC rules are meant, so for example say that a particular subject as a top-secret clearance level, so this means that, that particular subject can read or write two files which are marked as top-secret.

Now the discretionary access control present in the Bell-LaPadula model would permit that this particular top-secret user could use the access matrix to grant rights to other, so what this means, with the discretionary access control mechanism is particular user can grant rights for the top-secret objects to other users, however since the MAC rules also have to be met that is the no right down and that is the no read up and no right down it would mean that this particular user get only grant access to subjects which are at the same top-secret level.

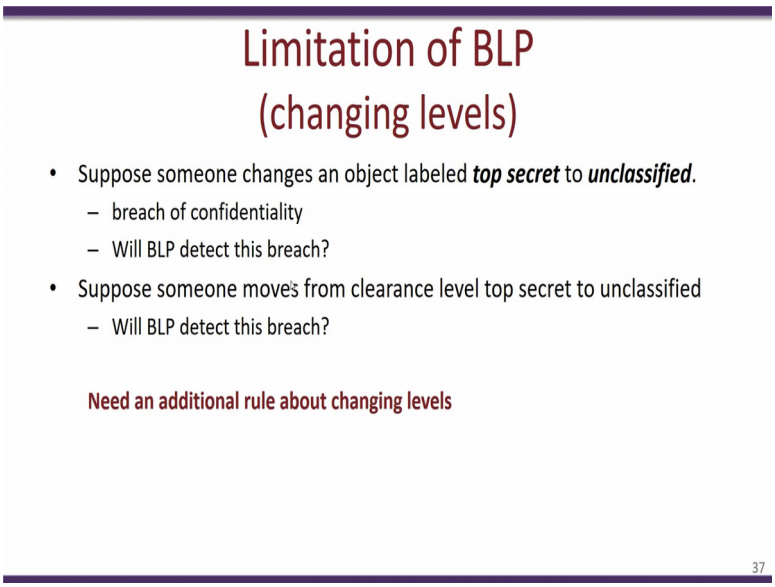
So for example this subject will not be able to grant a read access to another subject who is marked as unclassified, so I subject with a clearance level of top-secret will not be able to grant read access for a document to another subject who has an clearance level of unclassified, so this would ensure that even though the discretionary access control mechanisms are present in the system, the mandatory access control mechanisms would prevent unauthorised flow of information across the various clearance levels.

(Refer Slide Time: 20:12)



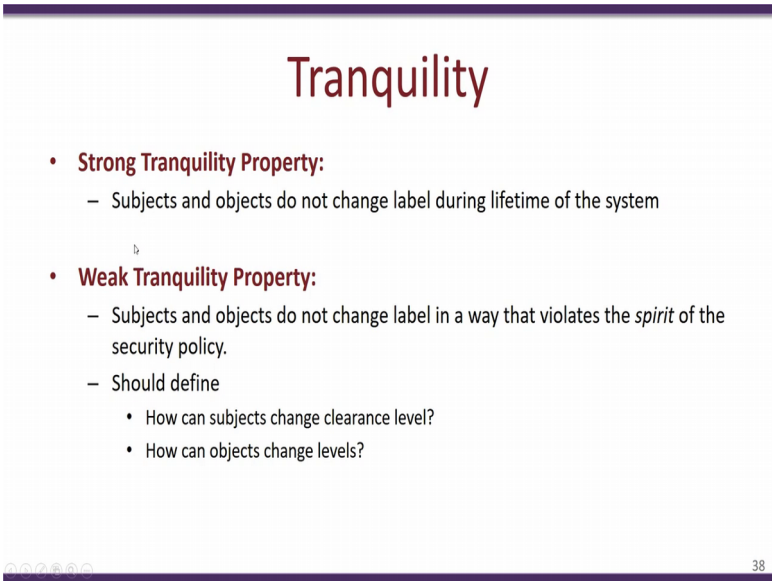
The limitations of the Bell-LaPadula model is as follows, first as you would have noticed that the Bell-LaPadula model permits a user with a clearance of confidential to write two files which is marked as secret or top-secret, now this could cause integrity issues, the Bell-LaPadula model is only concerned with confidentiality it is design to permit users with the right clearance level access right documents with the correct location level.

(Refer Slide Time: 20:50)



Another limitation of the Bell-LaPadula model is the case when there is a change of levels, let us assume that a user has a clearance of top-secret a particular company, now after sometimes let us assume that user leaves the company, so what should happen is that user should move from top-secret to an unclassified clearance, so this could lead to a breach of confidentiality, it would mean that top-secret information present in the company is now accessed by unclassified users, so the Bell-LaPadula model would not be able to detect this breach, therefore an additional rule would require whenever there is a change of levels.

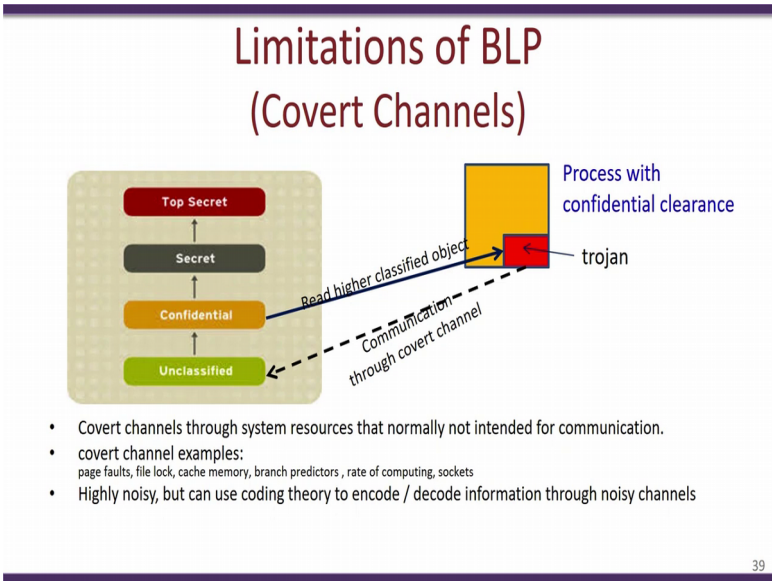
(Refer Slide Time: 21:44)



In order to achieve this there is an additional rule known as the tranquillity properties which are defined for the Bell-LaPadula model, there are two forms of the tranquillity property, strong tranquillity property and weak tranquillity property, a strong tranquillity property is defined that subjects and objects do not change labels during the lifetime of the system, if the particular subject is having a clearance of say top-secret, then a particular subject would remain in the a top-secret clearance for the entire duration of the system.

Further similar way if an object is defined as say confidential then the object will remain confidential for the entire lifetime of the system, so a weaker tranquillity property is defined as follows subject and objects do not change label in a way that violates the spirit of the security policy, essentially this weak tranquillity property should define our subjects and objects can change levels so that the Bell-LaPadula properties are not violated, while proving the security of the system with this strong tranquillity property in be easily done, proving the security with weak tranquillity property becomes much more difficult.

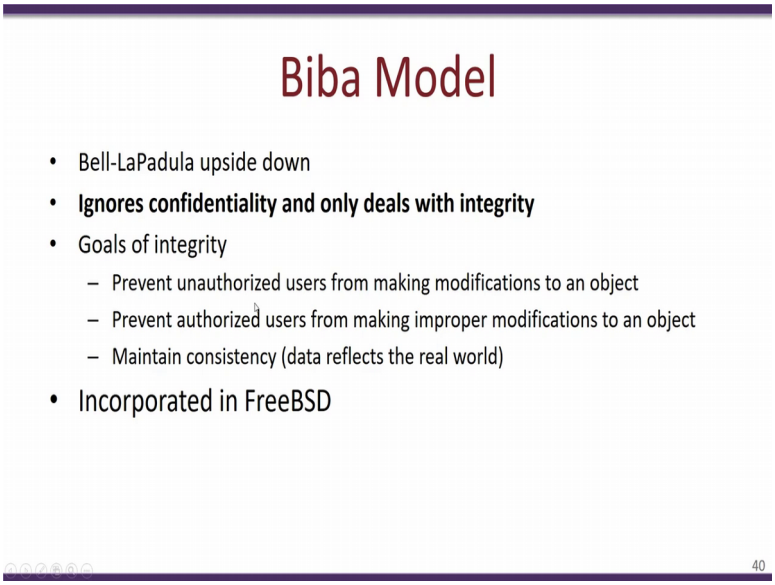
(Refer Slide Time: 23:18)



Another limitations of the Bell-LaPadula model is with respect to covert channels, so let us say that you have this particular process which is running with a clearance of confidential, now the Bell-LaPadula model would ensure at this particular process or any Trojan running within this particular process does not transfer information which is confidential to the unclassified level, however in spite of the Bell-LaPadula model in place communication may still occur so what is known as covert channels.

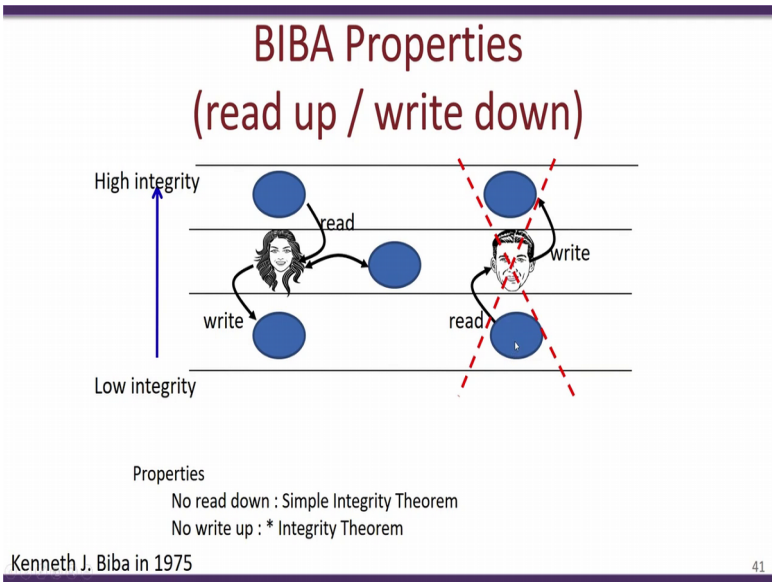
So covert channels are essentially a channel for communication which is not intended by design, for example the user page faults, file lock, cache memory, branch predictors and so on can be use as covert channels, so these channels although they are highly noisy can still be used to transfer information from one classification level to another unauthorised classification level inspired of the Bell-LaPadula model or any other such MLS model crescent, in a later lecture we will look at an example of a covert channel and will also see how a covert channel works in practice.

(Refer Slide Time: 24:43)



So will look at another example of an MLS model now so this is known as the Biba model and essentially it is the Bell-LaPadula model upside down, while the Bell-LaPadula model is only concerned with confidentiality and is not bothered about integrity, the Biba model on the other hand is mainly concerned with integrity, so the main role of the Biba model is to prevent unauthorized users from making modifications to an object.

(Refer Slide Time: 25:16)

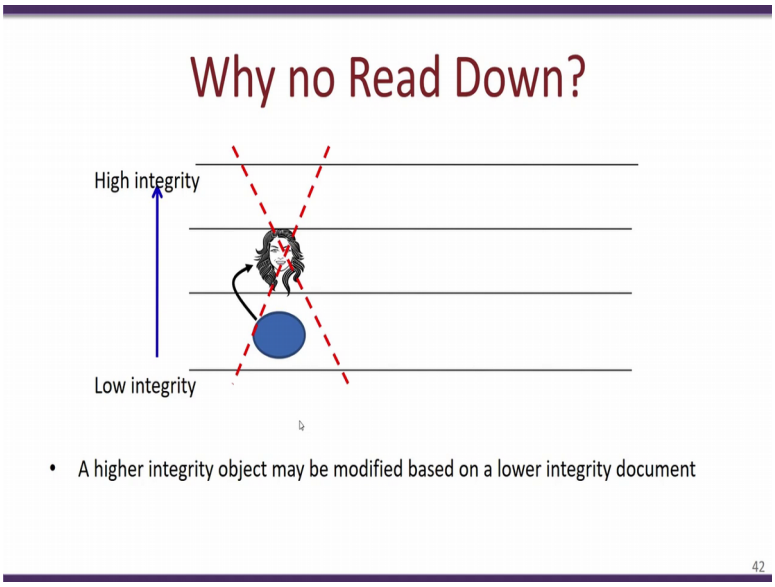


The Biba property was proposed by Kenneth J Biba in 1975 and it defines two rules in addition to the DS rule, the first rule is no read down or the simple integrity theorem, while the second rule is no write up or the star integrity theorem, so with the simple integrity theorem a particular subject with a certain clearance could read objects which are at a

clearance, it can also read objects at the same clearance and it can right to objects at a lower clearance.

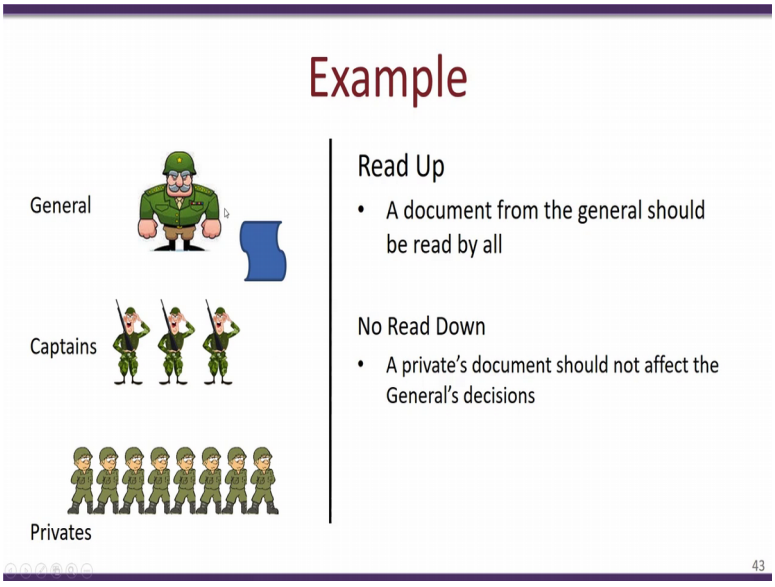
So you see the path of information flow, information flow can go from a higher clearance level to a lower clearance level on the other hand what the Biba property does not permit is the no read up and the no write up, in other words the Biba model would prevent information flow from a lower level to a higher level.

(Refer Slide Time: 26:24)



So why does the Biba model prevent read down, essentially if read down is permitted then a higher integrity object may be modified by a lower integrity document.

(Refer Slide Time: 26:39)



So for example let us say we have a hierarchy like this of general, captains and private, so when you apply the Biba model to this that is a document created by let us say the general should be readable to all subjects at a lower level, further the Biba model also defines the property for no read down, so what this means is that a file created by the captains cannot be read by the general.

So the Biba model as such is adopted in several operating systems, essentially it would ensure that system files can be read by all users in the system, however the system files will not be able to be modified by any of the underprivileged users, in the next lecture in this course we will look at more details about covert channels, we will take an example of a cache covert channel and see how information can flow from say one entity to another entity in an unauthorised manner. Thank you.