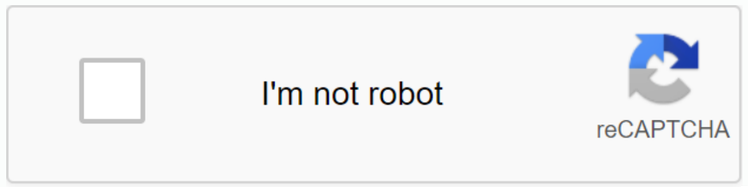

Continue

Bell-lapadula model access modes

This page is under construction. The Bell-Lapadula model of protection systems deals with the control of the flow of information. It is a linear non-discretionary model. This protection model consists of the following components: A set of items, a set of objects, and an access control matrix. Several ordered security levels. Each item has a clearance, and each object has a rating that maps it to a security level. Each item also has a current clearance level that does not exceed its ground clearance. Thus, an item can only be changed to a clearance level below the assigned clearance level. The set of access rights granted to an item are as follows: Read-only: The item can only read the object. Add : The item can only write to the object, but it cannot read. Perform : The subject can execute the object, but cannot read or write. Read-Write: The subject has both read and write permissions for the object. Control attribute: This is an attribute given to the item that creates an object. Because of this, the creator of an object can transfer one of the four above-mentioned access rights to that object to any subject. However, it cannot pass through the control attribute itself. The creator of an object is also called the object controller for that object. Limitations imposed by Bell-Lapadula Model: The following restrictions are imposed by the model: reading down: An item can only read access to objects whose security level is below the subject's current clearance level. This prevents an item from accessing information that is available at a higher level of security than the current authentication level. writing: A subject has added access to objects whose security level is higher than the current clearing level. This prevents an item from transferring information to levels lower than the current level. The Bell-Lapadula model complements the access matrix with the above restrictions to provide access control and information flow. For example, if an item has read access to an object in the access matrix, it may still not be able to exercise that right if the object is at a security level higher than its clearing level. Bell and Lapadula modeled the behavior of a protection system as a final state machine and defined a set of state transitions that would not violate the security of the system. The following actions secure a secure system: gain access: Used by an item to initiate access to an object (read, add, perform, etc.) release access: Used by an item to give up an initiated access. access: The controller of an object can give an item a specific access (to that object). Unp canonizing: Object controller can revoke a designated access (to that object) from an item. create object: Allows an item to activate an inactive object. object: Allows an item to disable an active object. change security security a subject that can change its clearance level (below an originally assigned value), but certain conditions must be met before the above operations can be performed. For example, an item can only exercise grant and revoke rights to an object if it has control attributes to that object. Bell-Lapadula is a simple linear model that exercises access and information flow control through the above restrictive properties and operations. But it has a disadvantage of security levels of objects is static. The characteristics of this model may become too restrictive in cases where certain operations are outside the context of the protection system. Question 1) What is the effect of reading down and writing up restrictions imposed by the Bell-Lapadula model? 2) Why is a subject's current clearance level only lower than its original assigned clearance level? 3) Write down the conditions to be met for each of the seven operations to be performed. 4) Why is the Bell-Lapadula model non-discretionary model? Singhal,M. and Shivaratri,N.: Advanced concepts in operating systems , McGraw-Hill, 1994. Peterson,J.L. and Silberschatz,A.: Operating System Concepts, 2nd ed, Addison Wesley, 1985. Landwehr, C.E, formal models of computer security, ACM Computing Surveys, September 1981 harsh@csgrad.cs.vt.edu Go back to the operating system page. Next: Capability-Based Systems Up: Protection Earlier: Unix This discussion is taken from HongHai Shen's thesis. The Bell-LaPadula Model (BLM), also called the multi-level model, was proposed by Bell and LaPadula to enforce access control in government and military applications. In such programs, topics and objects are often divided into different security levels. An item can only access objects at certain levels that are determined by his security level. For example, two typical access specifications are as follows: 'Non-classified employees cannot read data at confidential levels' and 'Top-Secret data cannot be written into files at unclassified levels'. This mandatory access control, which, according to the US Department of Defense's criteria for assessing the computer system, is a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal permission (e.g. authentication) of subjects that access information of such sensitivity. The opposite of mandatory access control is a discretionary access control, defined as 'a means of restricting access to objects based on the identity of the object and/or groups to which they belong. The controls are discretionary in the sense that an issue with a certain access permit is able to pass that permission (perhaps indirectly) to another subject. The Bell-LaPadula model supports mandatory access control by setting associated with items and objects. It also supports discreet access control by checking access rights from an access matrix. In terms of specification, we can consider the multi-level model as adding higher level mechanisms to the matrix model. In addition to supporting arbitrary access specifications to the access matrix, the model protected objects according to different security labels and determines user rights using their approved security authentication levels (It is awkward, but not impossible, to specify this type of access definition using the matrix model.). More formally, each object is associated with a security level in the form (classification level, set of categories). Each item is also associated with a maximum and current level of security, which can be dynamically modified. The set of classification levels is ordered by a $< $ ratio. For example, it may be the set of top-secret, secret, confidential, unclassified, where unclassified < confidential < secret < top-secret A category is a set of names like Nuclear and NATO. Security level A dominates B if and only if A's classification level > B's classification level, and A's category set B's. For example, top secret dominates , {Nuclear, NATO} secret, {NATO}, because top secret > secret and set {Nuclear, NATO} contains {NATO} The model gives an access request (subj, obj, acc) if and only if all the following properties are met: simple security property (no read access): If acc read, level (subj) should dominate level(obj). * property (no write-down): if acc = addd, then level (obj) should dominate level (subj); if acc = write, then level (obj) must be equal to level (subj). safety property: The cell (subj, obj) in the matrix contains acc. Like Multics, this model has problems with hierarchical access control and does not always support the need to know the principle except in rigid military situations. Next: Capability-Based Systems Up: Protection Earlier: Unix Prasun Dewan Man Nov 4 12:08:34 EST 1996 While controlling users' access to protected networks and sensitive data is important in the private sector, it is essential to maintain the security of government and military circles. So much so that a specific protocol was adopted for these uses. Known as multi-level or Bell-LaPadula Model (BLM, or sometimes BLP), this access control system forms the basis of our discussion today. The need for security models It is not enough to establish a security policy to guarantee security. There needs to be enforcement and implementation of what this policy defines – and some means of measuring and assessing how effective it is. A security model formally describes a security policy in such measurable terms. Models are typically used in to ensure that policies meet the needs of (e.g. for compliance with the law). State Machine Models State machines or vending machines are abstract models that are used to detect features such as the security of a computer system, in its current state. The state of each function that is detected may change from time to time, such as when the function is detected. So government machine models can be used in a number of ways, such as the design of programming languages or computer systems, and in the assessment of security. While working at Mitre Corporation, D. E. Bell and L. J. LaPadula developed a state machine model in the 1970s to analyze Multi-Level Security (MLS) operating systems. Their model was constructed using the language of General Systems Theory first proposed by MD Mesarovi'c, and uses a linear non-discretionary approach in the management of control of information flows. It has since become one of the main basis for the methods used to check the security characteristics of real systems. Topics and objects In distribution access control for military or government applications, there are typically multiple levels of security or clearance involved (Eyes Only, Secret, Most Secret, Top Secret, etc.). Bell-LaPadula describes these levels with respect to the items and objects to which they apply. An item (which can be an individual, device, application, computer system, organization, or business unit) is assigned a security clearance and a current level of authentication that cannot exceed the authentication granted. So within a protected system, an item can only be changed down, to a level below the assigned security clearance. Objects (which could be parts of your computer's memory, input/output devices, files, documents, datasets, etc.) are also assigned a security level, a classification based on the sensitivity of the information they contain. An item can only access objects at the levels determined by the item's own security level. Mandatory Access Control The U.S. Department of Defense Trusted Computer System Evaluation Criteria further clarifies this condition by describing mandatory access control as: a means of restricting access to objects based on the sensitivity (as represented by a label) of the information in the objects and the formal permission (e.g. clearance) of subjects to access information of such sensitivity. Discretionary access control As opposed to mandatory access, the discretionary access control restricts access to objects on the basis of the identity of the object attempting to access them and/or relevant groups to which they belong. It's a looser mode, and Bell-LaPadula supports mandatory access controls for most applications based on the security levels associated with different topics and objects. However, the model also supports discreet controls used for an access array. Access Matrix An access control matrix completes the image when used with a set of items and objects. It can be expressed in mathematical terms such as (s,o,a) where s = subject o = object and a = access rights associated with the subject. Topic.