Journal of Defense Management
ISSN: 2167-0374
OPEN ACCESS Freely available online
Opinion

Multi-level Security and Security Policy

Ian Ross*

Durham University, Durham, England, UK

OPINION

Multilevel security is a security Policy that allows data and users to be classified using a hierarchical security level system mixed with a non-hierarchical security category system. There are two basic purposes of a multilevel-secure security policy. In many firms, protecting sensitive or secret data is critical. Businesses may risk legal or financial consequences if such information is made public. At the absolute least, they will lose customer confidence. However, with the right investment or compensation, they may usually recoup from these financial and other losses. The same cannot be said for the defence and related communities, which include military services, intelligence agencies, and some police departments. If sensitive information is released, these firms may not be able to recover quickly, if at all. Security is required at a greater degree in these communities than in businesses and other organisations. The presence of information with varying levels of security on the same computer systems constitutes a serious concern. Even when various users log in using distinct identities, with different permissions and different access levels, it's not easy to separate different information security levels. Some companies go so far as to buy separate systems for each level of protection. However, this is frequently too expensive. A technique is needed to allow users with varying levels of security to access systems at the same time without danger of information contamination.

Labels are used to denote security levels by individuals, computers, and networks in such a system. Data can travel between levels that are similar, such as "Secret" and "Secret," or from one level to another. This indicates that users at the "Secret" level can share data and obtain data from Confidential-level (i.e. lower-level) users. Data, on the other hand, cannot flow from one level to another. This disables processes at the "Secret" level from reading "Top Secret" information. It also prevents operations at a higher level from writing data to a lower one by accident. The "no read up, a write down" model is what it's called.

MLS access rules are always used in conjunction with standard access permissions (file permissions). If a user with a security level of "Secret" uses Discretionary Access Control (DAC) to prevent other users from accessing a file, this also prevents users with a security level of "Top Secret" from accessing the file. A higher security clearance does not immediately grant access to browse a file system at will. On multi-level systems, users with top-level clearances do not immediately have administrative rights. While they may have full access to the computer's contents, this is not the same as having administrative privileges.

The Bell-La Padula BLP model is used by SELinux, with Type Enforcement (TE) for integrity. Simply put, MLS policy ensures that a Subject has the necessary permissions to access an Object of a specific categorization. For example, under MLS, the system needs to know how to handle a request like: Can a process running with a Top Secret/UFO clearance, Rail gun, write to a Top Secret/UFO file? The answer will be determined by the MLS model and the policy that is developed for it. (Take, for example, the issue of information seeping into the file from the Rail gun category.) The way information and employees are managed in strictly controlled environments like the military, MLS fits a very narrow (but crucial) set of security standards.

Access restrictions are applied to various layers of processes, with varying rules for user access at each level. If a user does not have the proper authority to start a process at a given level, they will not be able to access information. MLS implements the Bell–LaPadula (BLP) paradigm for system security in SELinux, which uses labels to govern the flow of information across security levels by applying labels to files, processes, and other system objects. The labels for security levels in a typical implementation could range from the most secure, top secret, through secret and classified, to the least secure, unclassified. For example, in MLS, you might set up a programme called secret to be able to write to a top-secret file but not read from it. Similarly, you'd allow the same application to read and write to a secret file, but only to read classified data.

Correspondence to: Ian Ross, Durham University, Durham, England, UK, E-mail: ian.ross@lshtm.ac.uk

Received: November 09, 2021; **Accepted:** November 23, 2021; **Published:** November 30, 2021

Citation: Ross I (2021) Multi-level Security and Security Policy. J Def Manag. 11: 223.