International Journal of Social Science and Economic Research

ISSN: 2455-8834

Volume:08, Issue:01 "January 2023"

SOFTWARE SYSTEMS SECURITY IMPLICATION UTILIZING THE BELL-LAPADULA MODEL

Jaden Cutinha

North Creek High School, Bothell, Washington

DOI: 10.46609/IJSSER.2023.v08i01.012 URL: https://doi.org/10.46609/IJSSER.2023.v08i01.012

Received: 3 Jan. 2022 / Accepted: 22 Jan. 2023 / Published: 31 Jan. 2023

ABSTRACT

Due to the multitude of security problems prevailing in society, software and systems security has grown exponentially over the past few years. To combat the issues that arise, there have been a host of approaches that have been attempted to implicate. Current research initiatives through CSS focus on data virtualization security as well as other research including memory forensics. Through this, a relationship has been established that connects them to implications in real-world systems. The main purpose of this remains to implement walls for the prevention of attacks and to remain functional despite extenuating circumstances. The ability to withhold malicious attempts into accessing important data is crucial in the prevention of information loss. In this project I have discussed the model, Bell-LaPadula, that is administered for security. The studies in correlation might align with a potential information security protection that will securely assist in the prevention of the exploitation of a user's privacy.

Software Systems Security through Bella-LaPadula Model

1. Introduction

Due to the exponential growth of data processing in today's society, issues arise from the protection of users' private information. Software system implementations have been created such that the data that the user parses through is encrypted in a way that prevents unauthorized access. The systems created identify certain methods to ensure data privacy: developing security algorithms, utilizing method protocols, and building architecture that protects data to ensure security.

i. Research Focus

There has been an extensive amount of research has been dedicated to searching for innovative solutions to encrypt users' data. Two main research segments stem which include *cryptography*

ISSN: 2455-8834

Volume:08, Issue:01 "January 2023"

and *network &distributed systems security*. **Cryptography** centers around investigating how to secure communications can be established between the user and their data such that their privacy is ensured. While there are many situations that cryptography could encompass, data privacy focuses on specific methods that apply to effectively transmit information from the platform directly to the user, averting any leakage. **Network & Distributed Systems Security** has a specific focus on designing smart systems that can apply to technological devices in a way that they are encrypted from harm. The primary purpose is to shelter the data from unauthorized access to resources that the user stores in systems. To evaluatethese two different research topics, models have been developed and deployed. Archetypes such as the Harrison Ruzzo Ullman Model and the Biba Model have been proposed with the intent of averting the crisis of mishandling users' information. Arguably none of these models have been as essential as the Bell-LaPadula Model.

2. Bell-LaPadula Model

i. Background

The Bell-LaPadula Model is a model with a definitive purpose. It helps to enforce access for applications protecting the data from being compromised. For instance, the government transmits classified information through servers constantly, and protecting their data from unauthorized access is essential. If their data becomes compromised, disaster could result which led to a need for a strong model that could handle the protection of their information from outside networks. The classification of individual subjects and files is organized in such a way that different layers of security are present separating the data. Thus, the Bell-LaPadula Model was established as a means to secure data transfers and storage.

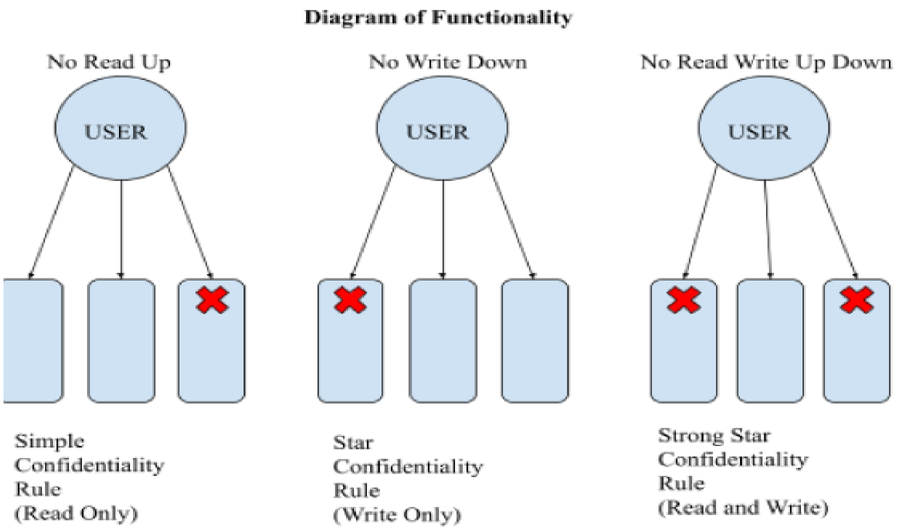
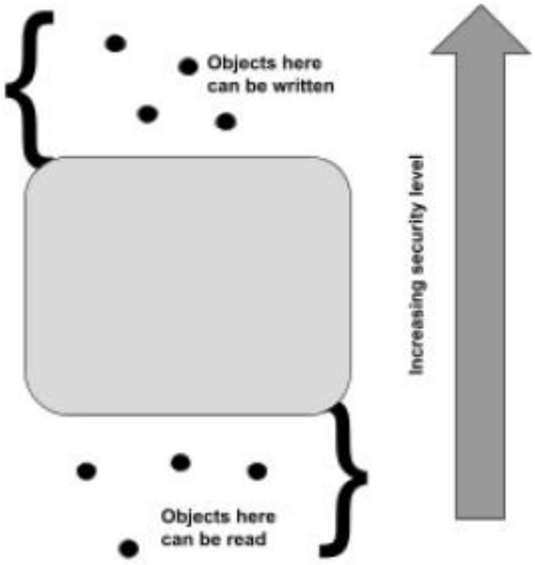


Diagram of Functionality
No Read Up
No Write Down
No Read Write Up Down
USER
USER
USER
Simple Confidentiality Rule (Read Only)
Star Confidentiality Rule (Write Only)
Strong Star Confidentiality Rule (Read and Write)

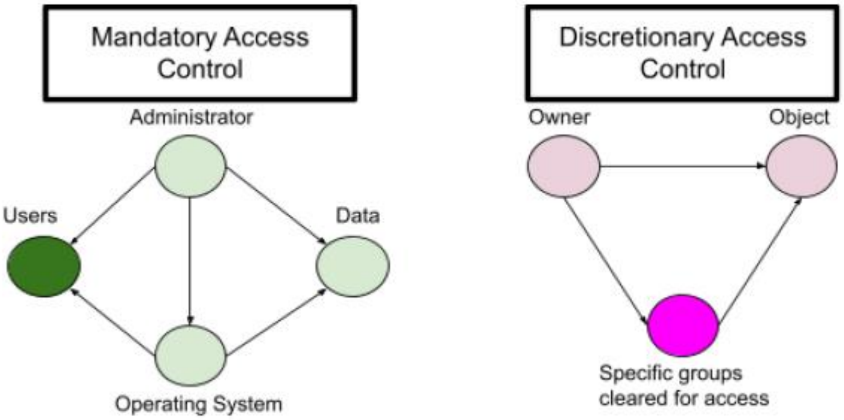
There are three rules that outline the guidelines around the implementation of the Bell-LaPadula Model: the *simple confidentiality rule*, the *star confidentiality rule*, and the *strong star confidentiality rule*. The simple confidentiality rule states that an individual subject can onlyread accessible files that are not included in the upper layers of protection which results in a **no read-up** situation. In the star confidentiality rule, a subject is allowed to access files on their ownlevel of secrecy and above but cannot read files below their own level. This situation results in **no write-down.** Finally, the strong star confidentiality rules state that a subject can only read files on their own individual layer of secrecy but not up or down. This rule is referred to as **no read write up down**.

ii. Model Setup

This model has a structure that defines the backbone of its system. In theory, an individual with a certain level of clearance should not be able to access information that exceeds their security clearance. In ideal situations, users should be on various streams, and accessing other patrons' files would essentially be barred. The main goal for this setup would be to keep theprivate data secure and share the data only when it was necessary.



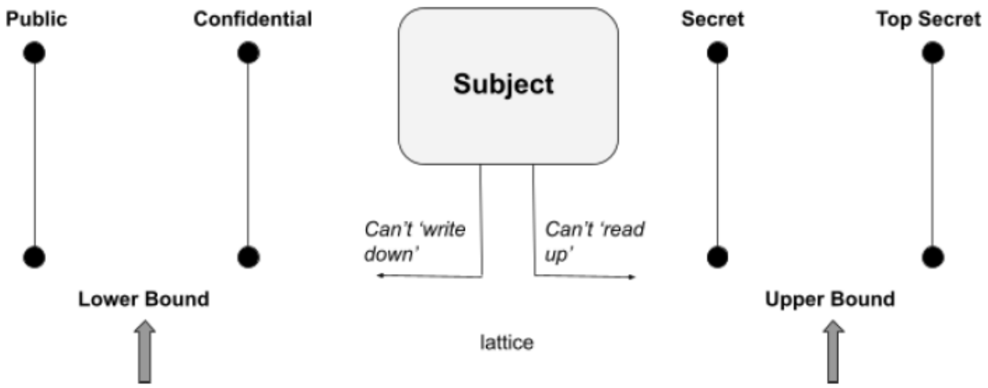
The model illustrates two main concepts which it aims to build off of: *mandatory* and *discretionary access control*. **Mandatory access control** is where a trusted object or individual creates and enforces the guidelines, which are followed for data access. The authorization of MAC is based on permissions and object labels. In contrast, **discretionary access control** is where the individual who is the owner of the particular file or data can change the access control and restrictions based on their input. The authorizations of DAC are based on only permissions. There is no knowledge of the object labels. For instance, if certain access was to be provided for another user, through discretionary access control, the owner of the file would be able to provide the access themselves.



3. Implications

i. Functionality

The Bell-LaPadula Model mainly centers around the task of ensuring data privacy for government and military purposes, being utilized as a means to protect data. The model utilizes a method of set rules which a patron must follow. Data can only be accessed if the individual has access to the data enforcing strict regulations for the prevention of data mishandling. The data is set into objects and each object is associated with its own security level. In addition, each subject is associated with various dynamic security levels. The set of classifications is individually ordered through the a < relationship.



ii. Illustration

We can look at an example to further understand the Bell-LaPadula Model.

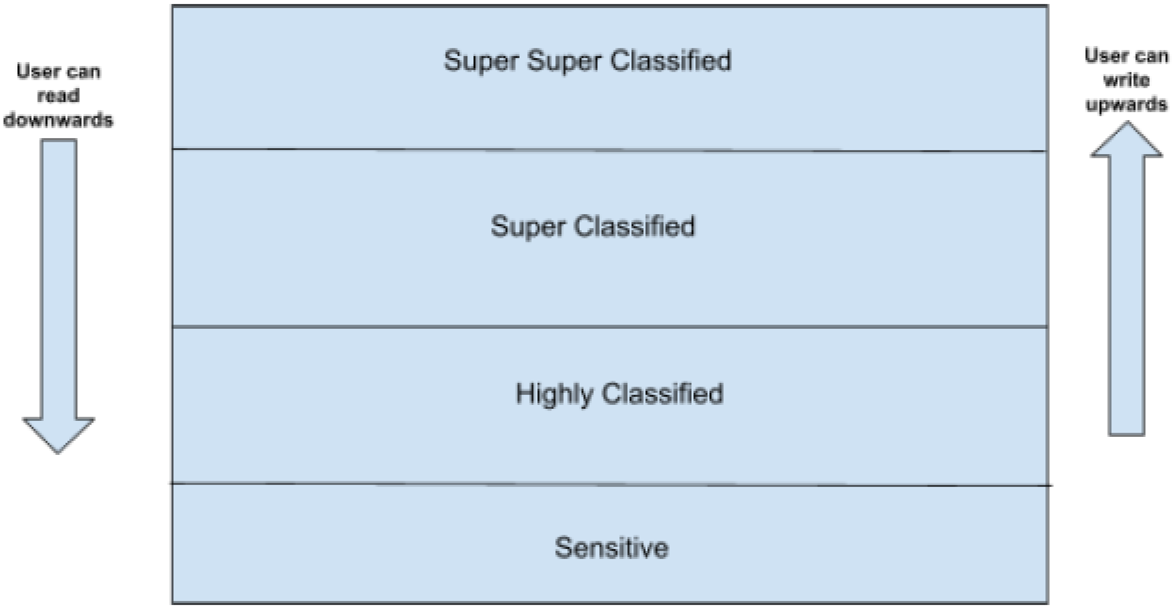
Let's say for instance that we have the set *super-strong, strong, average,* and *weak.*

We know that *weak $<$ average $<$ strong $<$ super-strong.*

A category can be labeled as such: *boss* and *worker* .

The Bell-LaPadula system enforces the idea that the security level A can be given greateraccess than B only if A has a classification that is greater than or at least equal to B's classification level **and** A's set of data is a superset of B's. Using the information that we labeledpreviously we can see this being put into action.

super-strong, {boss, worker} would dominate over strong, *{worker}* since *super-strong $>$ strong* and the set *{boss, worker}* contains worker within it.



4. Restrictions

Though the implementation of the Bell-LaPadula Model is an effective means to storeand access one's personal data, drawbacks are present that limit the construction of the model.

One main limitation is that the model only addresses the concept of confidentiality and the covert channels are not deeply set. This means that access control as a subject is not addressed. In addition, the model as a whole can become inadvertently worthless if state transitions occur. These transitions change the access rights of individuals rendering the model incapable of implementation.

References

- "Introduction To Classic Security Models." *Geeks for Geeks*, 11 July 2022, www.geeksforgeeks.org/introduction-to-classic-security-models/. Accessed 2 Jan. 2023.
- "Protecting Your System: Software Security." *NCES*, nces.ed.gov/pubs98/safetech/chapter7.asp. Accessed 2 Jan. 2023.
- Shen, HongHai. "Bell LaPadula Model." *The University of North Carolina at Chapel Hill*, www.cs.unc.edu/~dewan/242/f97/notes/prot/node13.html. Accessed 2 Jan. 2023.