Bell–LaPadula model of computer security

Sumtsova I., Shcheglov S.A., Shendryk V.V.
Sumy State University, inna_sumtsova@yahoo.com, ShcheglovSA@yandex.ru

The exact description is given of Bell and La Padula security model with use of modern notation. The document is intended serve as a basis for more precise formal and academic discussion model. The Bell-La Padula security model created conceptual tools for the analysis and design of safe computer systems.

INTRODUCTION

The Bell-LaPadula Model was created to formalize the USA Department of Defense multilevel security policy.

The Bell and La Padula model is a formal description admissible way flow of information in a secure system. The main objective of this model is to define the acceptable communications where privacy is important.

The model has been used to identify security requirements for systems concurrently handling data at different levels.

THE MAIN TEXT. SECTION 1

Bell-LaPadula model based on the conception the state machine. This concept defines set allowable states (Ai) in the system. Transition from one state to other upon receipt of entrance (s) (X) is defined features switch (D). The aim of this model to its original state is safe and that transitions always results in a safe condition. Transitions between conditions are shown on image1.

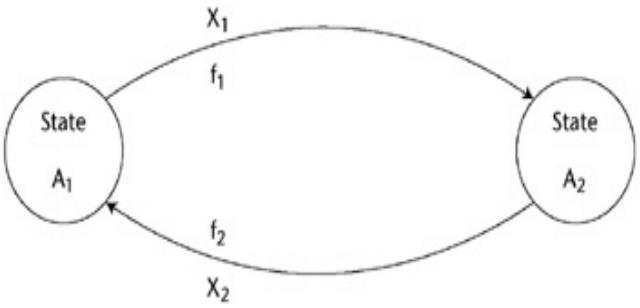

Image 1 – State transitions defined by the function f with an input X.

THE MAIN TEXT. SECTION 2

Bell-LaPadula model specifies a safe state after three multi-properties. The first two properties of mandate access control, and the third enables a discretionary access control. These properties are determined as follows:

1. The simple security feature. State reading the subject at lower level of sensitivity of object at a higher rate of sensitivity not allowed.

Basically, this feature specifies that subject can read an object if class access to subject dominates over access class of the object. So, the subject can read an object just if the object is at a high level of sensitivity than the object.

2. The * (star) Security feature. State showing the information on the subject at a top level of sensitivity to the object at a lowest level of sensitivity is not allowed (without cancellation). Basically, the restrictions of property, the subject can be able to write an object only if the class available the object dominates over access class of the object. Formally, subject to a lowest level of sensitivity can write just object to a higher level of sensitivity.

3. Discretionary security property. Use access matrix to indicate the discrete controlling access.

CONCLUSION

We are aware nearly a third of the century, as creation and the deployment of powerful and secure system. Our total uses of knowledge in a networked world with its EM fazes for fast, secure information exchange. In 21century, we should use our available resources in slim lines between networks.

REFERENCES

[1] IEEE Computer Security Symposiumon Research in Security and Privacy, 4–6 May 1992,Oakland, CA, 286–292.
Security strategy [electronic resource] : : from requirements to reality / London : : Taylor & Francis [distributor], , 2010.
Computer security basics / Deborah Russell and G.T. Gangemi by Russell, Deborah, Gangemi, G. T.O'Reilly, 2009