Experience 8 – Computer Viruses

Student Name: Ben Cendana

Student #:100811212

Contents

1.0: Introduction

This experience is broken into two parts a theory portion and a practical section both are based on the paper written by Fred Cohen titled Computer Viruses: Theory and Experiments. Despite being published in 1987 the paper presents the foundation to modern day sandbox and jailbreaks. The paper advocates isolation as the best method of protection against the spread of viruses and malware, however isolation loses the benefit of communicating between processes. In order to allow some communication while offering a high level of the protection the Bell-Lapadula and Biba models were presented as a way to provide a level of security while allowing data flow control between multiple computers.

For this experience we will explore the concept of flow control and access thought the Biba and Bell-LaPadula models which where highlighted in the article. Next we will apply the concept in a practical application in section 3.0.

2.0: Theory - Lattice Access Control Models

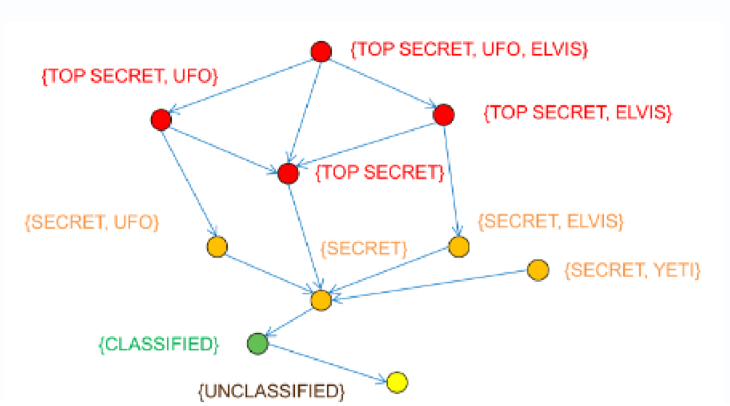


Figure 1: Lattice Access Control Model

The Bell- Lapadula model was developed as a confidential lattice access control models were the node and the security classification level would dictate the subjects read access.

Figure 1 demonstrates how a lattice access control model works, the top level classification is {Secret, UFO, Elvis}. This implies that anyone with this classification can read the layer below it, which is {Top Secret, UFO} and {Top Secret, Elvis}. However anyone with {Top Secret, UFO} or {Top Secret, Elvis} classification is unable to access {Top Secret, UFO, Elvis} as they lack the security classification.

Thus the higher the level in the lattice structure the more read access is available for that user, the user may read the layer below it but can not access the layer above it.

The Bell-Lapadula and Biba models were based on this lattice access control method, both models differ as the emphasis in the Bell-Lapadula is data security while emphasis in the Biba model is in data integrity.

Both models share similar properties and levels of Tranquility. Tranquility is available in two levels these are strong tranquility or weak tranquility.

Strong Tranquility means the file can never be changed while *weak tranquility* means the file can be changed if it doesn't compromise security.

The properties are:

1) Simple Security Property.
2) Star Property.
3) Strong Star Properties.

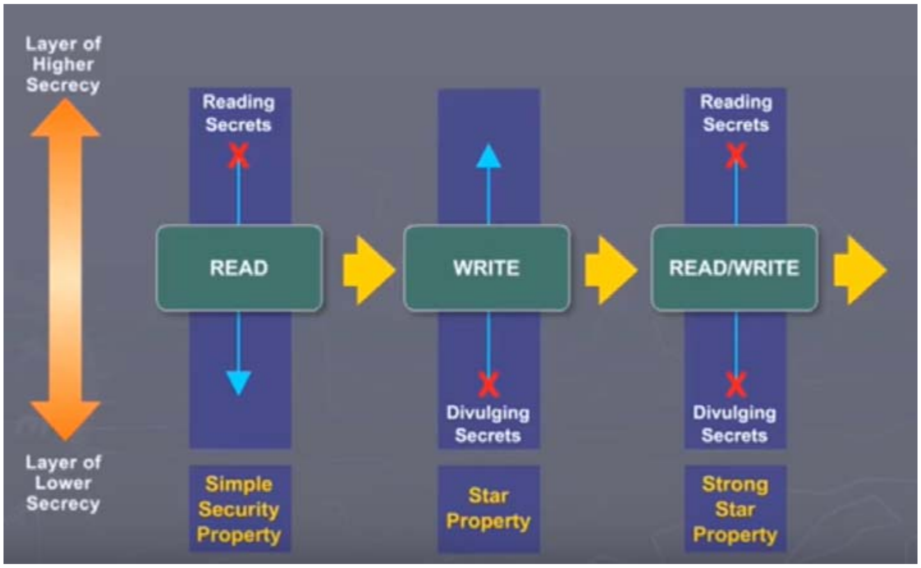


Figure 2: The Properties

2.0.1: Lattice Access Control Models - The Simple Property

The Simple Property states that each layer in the lattice should be unable to read or access the layer above it. A higher layer can still read a lower layer but the lower layer is denied access from reading a higher layer.

2.0.2: Lattice Access Control Models - The Star Property

The star property is similar to the simple star property the only difference is a lower level layer should not be able to write to a higher layer.

2.0.3: Lattice Access Control Models - The Strong Star Property

The strong star property states that each layer should not be able to read then write to the layer above or below it. This is because other layers may influence lower layers which would jeopardize the layers confidentiality.

When the properties and tranquility is applied in a lattice structure we end up maintaining a system of access control that allows security while allowing a good flow of communication.

2.1: Theory - Bell- Lapadula

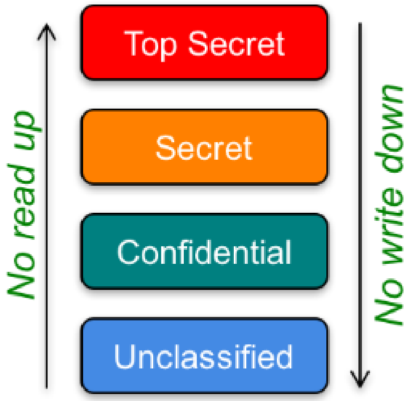


Figure 3: The Bell-Lapadula Model

Figure 3 conceptual demonstrates how the Bell-Lapadula model keeps a system of least privilege with a lattice structure applied. The higher the classification level in the lattice the more read privileges the user has.

2.2: Theory - Biba Model

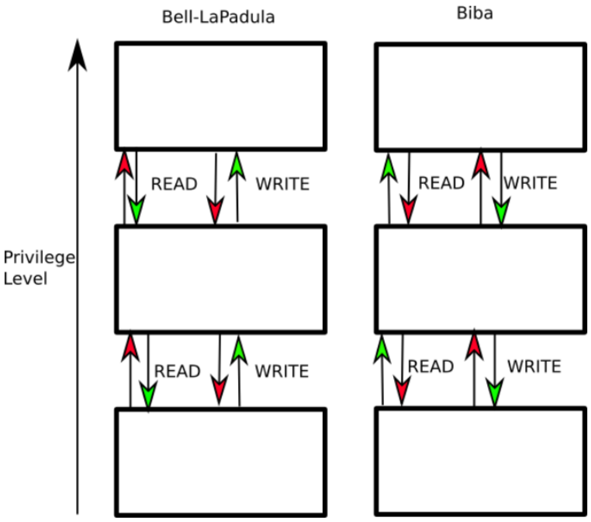


Figure 4: The Bell-LaPadulla vs Biba Model

The Biba Model was introduced to implement data integrity within the Bell-Lapadula model. As can be seen in Figure 4 the only differences are:

1) A lower level user can write or create files to a higher level.
2) A higher level user can not read files to a lower level.

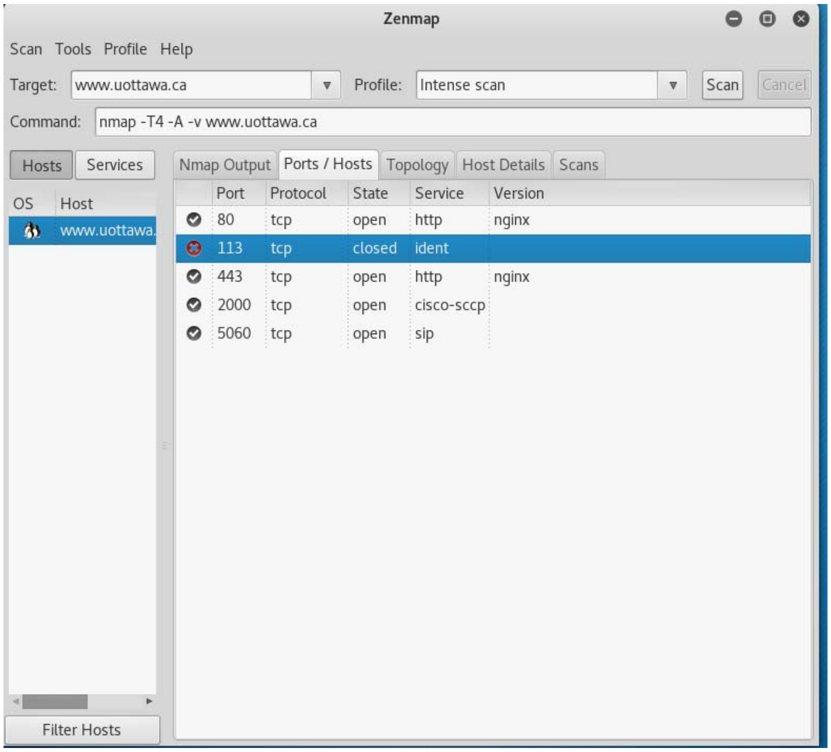
As was observed in the Bell-LaPadulla model each layer is still unable to read and write or modify the layer above or below it.

3.0: Practical

Given that the Bell-LaPadulla and Biba models deal with the flow of data the concept can be applied to network topology with each port and there corresponding application/service(s). The level is the application/service and the category is based on the port, with lower level ports being a layer of higher privilege.

Using the NMap tool we can demonstrate this concept.

3.1: Practical: NMAP – Bell-LaPadulla Model



Target: www.uottawa.ca

Profile: Intense scan

Command: nmap -T4 -A -v www.uottawa.ca

	Port	Protocol	State	Service	Version
✓	80	tcp	open	http	nginx
✗	113	tcp	closed	ident	
✓	443	tcp	open	http	nginx
✓	2000	tcp	open	cisco-sccp	
✓	5060	tcp	open	sip	

Figure 5: The Ports and Services After An NMAP Scan

Applying the lattice access control model to the NMAP scan in Figure 5 we can conclude that the higher level ports represent lower level privileges while the protocol and the services represent the categories.

Since all the ports for the exception of port 113 are open and can be accessed we can say that the Bell-LaPadulla model is being used. The lattice access control works by applying {service, port, protocol} as the classification and level of privilege, thus {ident,113,tcp} is the highest level of privilege while all the others are of a lower level of access.

{http,2000, tcp} and {http,80,tcp} would have a similar level of access but with {http,80,tcp} being a higher level of privilege given the port number. In conclusion we can see that the lattice access control model can be applied to networks in a practical setting.