1. CyberCIEGE MAC Integrity

CyberCIEGE is an information assurance (IA) training tool that illustrates computer and network security principles through simulation and resource management trade-offs. CyberCIEGE players construct computer networks and make choices affecting the ability of these networks and the virtual users to protect valuable assets from attack by both vandals and well-motivated professionals.

The CyberCIEGE MAC Integrity scenario is a simple example of mandatory access control (MAC) policy enforcement of an integrity policy using security labels and a server that enforces the MAC policy.

As with all CyberCIEGE scenarios, students are encouraged to explore the effects of "wrong" choices as well as trying to select the correct choices. Plan on playing the scenario several times before finally going through it making what you believe are the correct choices.

The MAC Integrity scenario builds on the concepts covered in the MAC scenario, which covered a secrecy policy. This scenario is very similar to that previous MAC scenario, but this scenario includes an integrity policy. This scenario explores the following concepts:

- Real-time sharing of information across integrity levels may require reliance on a computer to enforce a MAC policy. Such computers are sometimes referred to as providing "multilevel integrity".
- Connecting physical networks to a MAC enforcement mechanism requires that you provide the MAC mechanism with a security label for the connection. Some environments may require both secrecy labels and integrity labels.
- Malicious software on a network can corrupt the integrity of information, and thus the integrity label associated with networks should account for the potential for low integrity or malicious software.

1.1 Preparation

Students are expected to have complete the CyberCIEGE Mandatory Access Controls scenario.

From the "Campaign Player", select the "Mandatory Access Controls" campaign

Select the "MAC Integrity" scenario from the scenario list. Then click the "Play" button.

Read the briefing and the objectives screens, and explore the encyclopedia (via the "F1" key). As you play the scenario, remember you can save the game at any time and come back to that state later.

1.2 Play

1.2.1 Phase 1 – Assign Security Labels to Network

- Read the briefing in the GAME tab and check your objectives in the OBJECTIVES tab.
- Look at the labels of the assets via the ASSET tab. Look at the user clearances via the USER tab. Also look at the user goals and notice how they need to share the asset that is on the server.
- In the OFFICE screen, start the simulation and notice how both users are failing a goal because of their inability to share the "Critical Logistics Database" asset.
- Go to the NETWORK tab. Notice Grace's workstation is already connected to the LAN1 network and Sean's workstation is connected to the LAN2 network.
- Connect each network to Server by first selecting the server (click on it) and then click the LAN1 and the LAN2 buttons in the upper right.
- Right click on the server, select Networks and "Label Single Level Network" and then assign labels to each of the two networks.

Question 1.	*What label did you assign to the network connected to Grace's workstation?*
Question 2.	*What would you expect to happen if you assigned the other integrity label to Grace's workstation? After all, she is cleared to "CRITICAL OPERATIONS" integrity. Give it a try.*

- Start the simulation and see if you are successful by winning the scenario.
- Play the scenario again and this time assign the wrong label to Grace's network. Start the simulation. What happens? Click the "Attack Log" button to see a description of the attack. Replay the game, trying to counter each attack while keeping the wrong label on Grace's network. Why do you ultimately fail?

1.3 Clean Up

Exit the scenario by clicking the **Quit** button in the GAME screen.

Collect the game logs into a zipped folder by clicking the "**Advanced**" menu button and selecting "**Collect Logs**". Feel free to provide comments on the game within the provided space. Enter your NPS User ID as the user name in the field. Then click "**OK**" to create the zipped file on the desktop.

If you are running the exercise in the NPS Lab:

- copy the `logCollection.zip` file from the VM's desktop
- Minimize the VM (click on the "_" in the grey bar at the top of the

screen)

- paste it into the workstation host's desktop "CyberCIEGE-Logs" folder.
- if prompted to overwrite the file, click **Yes**.

If you are running the exercise outside of the NPS Lab:

- please email the `logCollection.zip` file to CyberCIEGELogs@nps.edu.

Click on the minimized VMware Workstation session to resume it (and press **<Ctrl>-<Alt>-<Enter>** if it doesn't return to full-screen).

Click the **CLOSE** button to exit CyberCIEGE.

Shutdown or suspend the VM and logoff the workstation if you are finished in the lab.

END OF LAB