1. CyberCIEGE User Identification

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 *User Identification* scenario explores the need to identify users to computers and the advantages of centralized authentication servers. The scenario also includes the challenge of authenticating remote users on hostile networks and computers. Finally, the scenario introduces the use of identity peripheral devices as a way of identifying authorized strangers and determining their authorizations.

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.

This scenario explores the following concepts:

- Computers require information about the identity of users. This information may be used to control who can access (e.g., login to) a workstation or who can remotely access a server.

- Verification of user identity is necessary to achieve individual accountability.

- Verification of user identity is necessary to provide access control and implementation of least privilege.

- Use of *authentication servers* can simplify the management of multiple users and multiple computers. When deployed, only the authentication server must manage information that is used to identify users. "Client computers" then use the authentication server to establish the identity of users.

- Sometimes circumstances demand that users access enterprise servers from remote computers that may be hostile (e.g., computers in a Hotel's business center). Identifying users from these computers can be risky unless suitable counter measures are deployed.

- Some situations require a means to authenticate "authorized strangers", i.e., people who are authorized to access a system, but are not explicitly known to the system. Examples are facilities that host many authorized visitors where it is not practical to establish individual user accounts for each visitor. Use of smart cards that contain user authorizations enable systems in which the computers are

computers are configured to recognize the authorization (e.g., all members of a specific group) rather than recognizing specific individuals.

In this scenario you can largely ignore Zones and physical security issues. Also, don't worry about hiring or firing support staff or the trustworthiness of your virtual users.

1.1 Preparation

Access CyberCIEGE as described in "CyberCIEGE Information Assurance Training Tool Availability at NPS".

> From the CyberCEIGE folder on the desktop, open the "CyberCIEGE" icon. This will start the "Campaign Player" seen in figure 1-1.
>
> To reach the User Identification scenario, you must either complete the prerequisite scenarios, or unlock all scenarios using the "Advanced / Preferences" menu selection. New players are encouraged to first play the first three "Training" scenarios and the "Introduction" scenario in the "Starting Scenarios" campaign.

To play the User Identification scenario, select the "Identity Management" campaign and the "User Identification" scenario and 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 state at any time and come back to that state later.

1.2 Play

1.2.1 Phase 1, First Identify Users to the Computers

- Press the space bar (or click the play button) to start the scenario. Observe the users are unhappy because they can't login to their workstations. When the ticker at the bottom of the screen suggests it, press F1 to learn how about user identification in CyberCIEGE.
- As per the instructions in the encyclopedia, configure the computers to identify users. Note you can do this either by configuring each individual computer (i.e., using the "LOCAL" button), or by defining an authentication server. If you configure an authentication server, you can also easily assign it client computers as seen in the encyclopedia "Authentication Server" heading. To configure an Authentication server, review the instructions per the encyclopedia – pick a server from the list in the upper left of the COMPONENT screen and then click the "Authentication Server" button on the lower middle of the screen.
- After you provide the computers with user identification information, you will be directed to change a password policy. If you've defined an authentication server, this can be accomplished by changing a configuration setting on that one computer. Password policies are set by selecting the computer from the list in the upper left of the COMPONENT screen and making selections on the upper right of the COMPONENT screen.

- Access to server based resources should include individual accountability, and this requires that the server that contains the asset only permit remote access to authenticated users. This is configured via the "Remote Authentication" checkbox in the computer's "Configuration Settings" (middle of the COMPONENT screen). First select the component in the upper left of that screen, then make the configuration change.
- The Sugar Spinner data needs protection. It is on a server that also includes an outward facing web server – and you don't have the resources to move the web server to a separate computer (e.g., to create a DMZ.) Thus, you need to consider access control mechanisms (e.g., ACLs). Select the Lollipop Server (in the upper left list of computers in the COMPONENT screen) then select the "Sugar Spinner Data" in the asset list (lower right) and click the ACL button. Who should be able to access this data?

Question 1.	*If you were allowed to change the network topology and the allocation of functions to computers, what might you do differently?*

1.2.2 Phase 2, Remote Authentication

- Let the game run until prompted to check your new objectives.
- Configure the system so that the Sugar Spinner Server can identify Fiona as directed by the objectives.
- Let the game run until something bad happens. After three attacks, you will be prompted to press F1 to see how to prevent these attacks.

Question 2.	*What did you do to keep attackers from accessing the enterprise server using Fiona's password?*

3600 Students can stop here if they wish, though they are encouraged to try to complete the final phase below.

1.2.3 Authorized Strangers

- Check your new objectives
- Look at the visitor's workstation and consider the use of peripheral devices that would let you recognize authorized visitors. Note you cannot add user accounts for visitors.
- Configure a validation profile on the visitor's workstation to permit access by the appropriate group of users.

1.3 Clean Up

The "View Log" button lets you view a log of what occurred during the game.

END OF LAB