Lab 6 CyberCIEGE Link Encryptors

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 link encryptors scenario illustrates the use of encryption to secure communications over networks that are subject to wiretap. Players are encouraged to watch the introductory "Encryption" movie from within the Cryptography tutorial in the CyberCIEGE encyclopedia.

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:

- Unprotected communications are subject to wiretap by attackers with access to the physical communications networks.
- Link encryptors can protect communication over dedicated communications lines.
- Link encryptors have two kinds of connections: unencrypted links and encrypted links. Two link encryptors are connected together via the encrypted link.
- Link encryptors require use of shared keys, otherwise they are unable to decrypt data encrypted by another link encryptor.
- Use of encryption requires some amount of management of encryption keys, which may be expensive and a source of vulnerabilities.
- When protecting high value assets, reliance on software within link encryptors (e.g., to manage keys) requires high assurance software.

In this scenario you can largely ignore Zones and physical security issues. You can also largely ignore configuration settings and procedural settings (e.g., settings on the COMPONENTS screen). Also, don't worry about hiring or firing support staff or the trustworthiness of your virtual users.

6.1 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 **Error! Reference source not found.**.

If you have not yet played the "Introduction" tutorial scenario in the "Starting Scenarios" campaign, you may wish to do that first. You may also want to click the *Help* button and then select Help & *Getting Started*, which will open a browser to a page that will help familiarize you with CyberCIEGE, including a few brief movies.

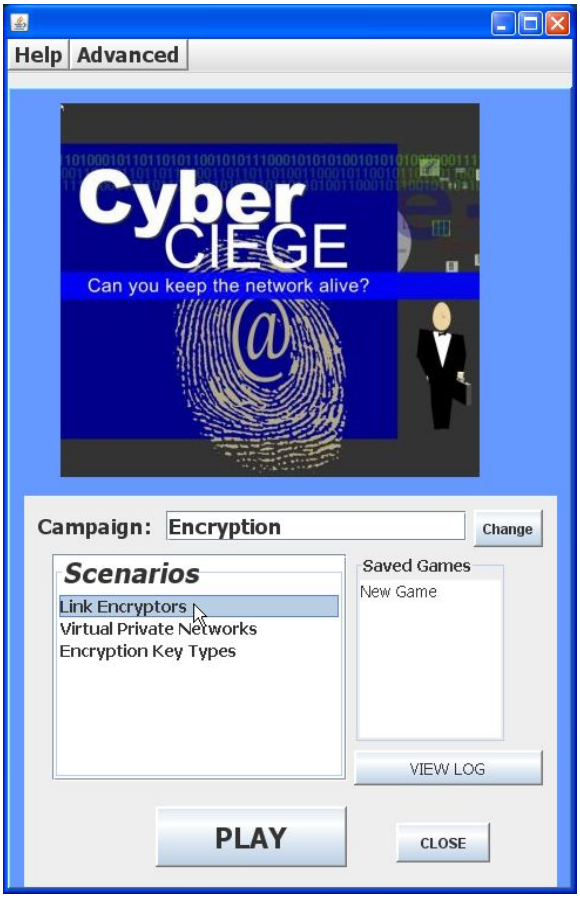

Figure 6-1: Select Link Encrypt Scenario and Click Play

If the "Encryption" campaign is not selected, click the "Change" button and select it. If that selection is grayed out, you can unlock all scenarios via the "Advanced / Preferences" selection in the menu.

Select the "Link Encryptor 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). Select "Cryptography" under "Tutorials and Movies" in the help screen contents, and watch the "Encryption" movie. Then start the scenario. As you play the scenario, remember you can save the state at any time and come back to that state later. Also, the game automatically saves your state at each transition to a new phase.

6.2 Play

6.2.1 Phase 1: Protect the Communications Link

In this phase you must deploy link encryptors to protect valuable assets as they transit a dedicated communications line.

- Click the Objectives button in the OFFICE screen to see how to learn about the value of this asset.
- Review the network topology via the NETWORK tab
- Press F1 to see instruction on how to deploy a link encryptor
- Purchase a link encryptor for each user. Use the "Tab" key to toggle between their desks.
- Configure the link encryptors such that the "encrypted link" is the leased line, and they share a common key.

6.2.2 Phase 2 Stale Keys

Now a year has passed and your encryption keys are stale. You must make a choice between two courses of action. Pause the simulation and consider your choice:

1) Manually change the keys. This choice implies you have instituted a key management procedure that incurs substantial cost. To do this, simply double click on each link encryptor and change the key.
2) Or, replace the link encryptors with more modern devices that have automated key management. Click on the "Buy" button and then click the new link encryptor to view its properties. If you wish to make this choice, buy each user one of these new encryptors. Then got to the NETWORK screen, select each of the old link encryptors and click the "scrap" button. Connect the new link encryptors to the appropriate networks.

After you've made your choice, press the play button to restart the simulation.

6.3 Clean Up

The "View Log" button lets you view a log of what occurred during the game.
Use the "Advanced / Collect Logs" choice in the Campaign Player to collect your logs into a zip folder that can be emailed or dropped into the CyberCIEGE-logs folder if running on a CS-3600 VM.

6.4 Additional Questions

Question 1. *In the Encryption introduction movie, what was the communications problem when the link encryptors were connected via the Internet?*

Question 2. *In the scenario you just played, what was the shortcoming of the "Autocrypt" product?*

END OF LAB