1. CyberCIEGE ParaZog Email

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 ParaZog scenario builds on concepts learned in the Hard Rain scenario related to use of PKI to manage keys used to protect assets. The ParaZog scenario introduces the potential use of smartcards for key management rather than the "soft certificates" that players were forced to use in the Hard Rain scenario.

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 ParaZog scenario explores the following concepts:

- Some environments require the storage of message on servers whose physical and logical security cannot be ensured. Use of email encryption can reduce the risks to information stored on servers of questionable trust.
- Use of email encryption does not prevent a Trojan horse on either the sender's or the receiver's computer from sending a copy of the plain text message to an attacker.
- Use of "soft certificates" implies that secret keys are stored within a workstation (e.g., by the email client). Loss of physical control over such a workstation could lead to disclosure of secret keys and thus disclosure of sensitive information. PKI-enabled smartcards can avoid this threat because the secret key never leaves the smartcard.
- Protection of email via email client based encryption cannot reasonably be achieved with high assurance, and thus some other protection strategy should be deployed to protect high value assets.
- Smartcards typically have internal storage that can serve as a conduit via which malicious software can move information between systems. In high motive situations, smartcards are no different from a USB memory stick.

1.1 Preparation

From the "Campaign Player", select the "Encryption" campaign.

The player is expected to have first completed the "Hard Rain" scenario prior to playing this scenario.

Select the "ParaZog" 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. Also, the game automatically saves your state at each transition to a new phase.

1.2 Play

You've played enough to know what to do. Watch your objectives and user goals. This scenario requires that you check the Attack Log (whenever that button turns red.

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