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 as seen in figure 1.

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

October 26, 2009
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 scenarios by now to know what to do. Have at it!

October 26, 2009
1.3 Clean Up

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

END OF LAB