1. CyberCIEGE 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 Email scenario builds on concepts learned in the Advanced VPN scenario related to use of PKI to manage keys used to protect assets.

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 Email scenario explores the following concepts:

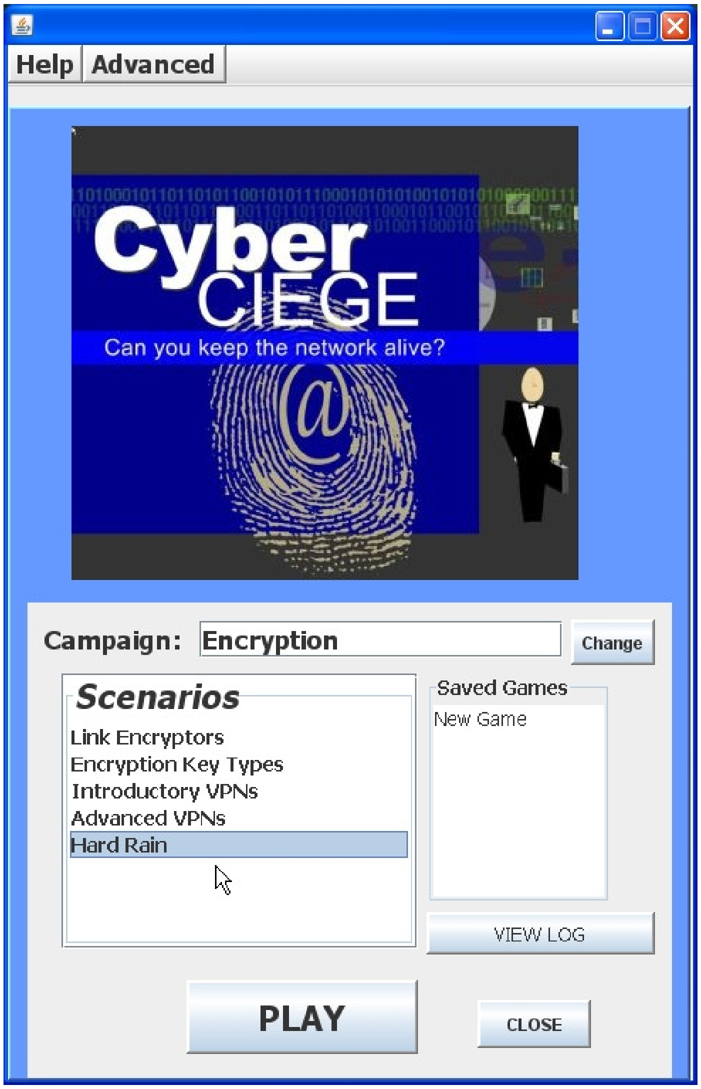
- Some environments don't support traditional access control mechanisms, e.g., all users might, by operational necessity beyond your control, have administrative access to servers.
- Encryption of email can protect the content of email from disclosure even if hostile insiders have access to the email servers that store the email.
- Email clients may include PKI mechanisms to facilitate the management of keys used to protect email.
- There should be some basis for trusting certification authorities that are installed as roots for use by email clients. Consider the potential for an imposter to obtain a misleading certificate from public pay-per-cert CAs and use that certificate to fool a user into thinking some other user has changed their email address.
- Encrypting an email requires the sender to validate the recipient's certificate – which may require installation of some remote party's root certificate. On the other hand, just signing an email does not require the sender to know anything about the recipient and thus does not require installation of any additional roots.

In this scenario you can largely ignore Zones and physical security issues.

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 "Advanced VPNs" scenario prior to playing this scenario. The player should at least view the following tutorial videos:
Public Key Infrastructure: http://www.cisr.us/cyberciege/movies/10CIEGE.html
CyberCIEGE PKI Installed Roots: http://www.cisr.us/cyberciege/movies/12CIEGE.html



Campaign: Encryption

Scenarios
- Link Encryptors
- Encryption Key Types
- Introductory VPNs
- Advanced VPNs
- Hard Rain

Figure 1: Select Hard Rain and Click Play

Select the "Hard Rain" 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). From the Cryptography entry in the "Tutorials and Movies" content page of the online help, view the "Public Key Infrastructure" movie. Also watch the CyberCIEGE PKI Installed Roots video. 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

This scenario includes some multiple choice questions. Some of these are marked as "quizzes" and you should attempt to answer those correctly the first time. Other multiple choice questions are marked as "what is your thinking here?", and are intended to help guide you. Answers to those questions are not recorded as quiz answers, so feel free to experiment with different answers.

1.2.1 Phase 1 – Secure email exchange

- Read the briefing in the GAME tab and check your objectives in the OBJECTIVES tab.
- Find desks for Otto and Debbie, use the Buy button (lower right of the OFFICE screen) to purchase workstations for them, and then drag-and-drop Otto and Debbie to their desks. (Use the <Tab> key to find a user, click on the user and hold down the mouse button and use <Tab> to find a desired location to drop the user.) Then use the NETWORK screen to connect the two new workstations to the LAN.
- Start the simulation by pressing the play button (or the space bar). What happens and why? Follow the instructions to press F1 to learn about email encryption.
- Right-click on Otto and Debbie's computers and select "Applications" / "Configure email application" to configure their email clients. Initially try using the Veriscream CA to issue certificates and add that CA as an "installed root" in the two user's email clients.
- Run the simulation. Note what happens. Buy your own CA and use the <Tab> key to find the computer rack into which to place the CA. Reconfigure the two email clients to use your new CA and remove the Veriscream CA from your installed roots – you no longer trust email certificates coming from that CA!
- Note how you now are short of IT staff? You need people to issue the certificates and manage the installed roots. Use the IT STAFF button in the lower right of the OFFICE screen to hire someone.
- Run until you informed you've reached the next phase.

Question 1.	*Why were the malicious insiders able to access email on the server?*

1.2.2 Phase 2 – New Employee

- Check your objectives.
- What will happen if you just let the simulation run? You might want to try it.
- Configure Miller's email client to protect his secret messages.
- Run until the next phase.

Question 2.	*Why did Miller's email client need to have an installed root certificate?*
Question 3.	*Did Miller's email client need to have a private key and Certification Authority to encrypt the message?*

1.2.3 Phase 3 – Send a Quote

- Check your objectives, and Miller's goals.
- Use the NETWORK tab to view your network. Note how you lack an Internet connection.
- Return to the OFFICE screen and use the BUY button to purchase a router (under the NETWORK DEVICES tab)
- In the NETWORK screen, connect the router to the Internet and the LAN
- Note how Miller is now happy that he can send an email quote to Kevin. But also note why Kevin is not happy.
- Think about the minimal things needed to satisfy Kevin's goal.

Question 4. Why did Kevin's company object to encrypted email?

Question 5. How could this lab be improved?

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