CyberCIEGE Encryption Key Types

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 Encryption Key Types scenario illustrates some differences between the use of public key cryptography and symmetric keys. It also introduces the risks of transmitting the hash of weak passwords over a network.

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:

- Application based cryptography can provide protection against network sniffing within relatively low motive environments.

- Use of shared secret keys can present challenges when adding additional users, e.g., each pair of users may have to have their own unique shared secrets. This may become hard to manage.

- Public key cryptography generally requires some investment to set up the infrastructure. This includes selecting and installing root certificates and establishing a process for issuing certificates to users (though this scenario hides the mechanics of that). However, once in place, this infrastructure can scale more easily than one based on shared secrets.

- Some authentication implementations transmit the hash of a password over a network. If the hash of a weak password is sniffed off the network, brute force or dictionary attacks can disclose the plain text of the password.

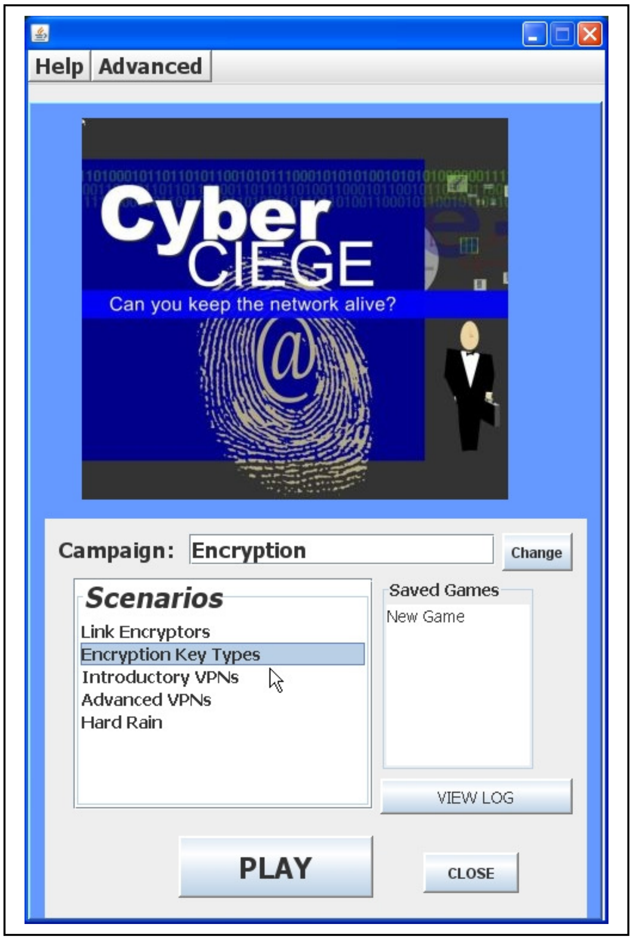
In this scenario you can largely ignore Zones and physical security issues. Also, don't worry about hiring or firing support staff or the trustworthiness of your virtual users.

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

Players are expected to have completed the “Link Encryptors” scenario prior to this lab. Make sure the “Encryption” campaign is selected.



Campaign: Encryption

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

Saved Games
- New Game

Figure 1: Select “Encryption Key Types” and Click Play

Select the “Encryption Key Types” 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 “Symmetric & Public Key Cryptography” movie. 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.

Play

Phase 1: Prevent Network Sniffing

In this phase you must replace the messaging application utilized by your HR users to exchange employee health care information. The initial application sends data over the network unencrypted. After running for a while and observing the attacks, you must replace the messaging application by choosing between an application that uses manually distributed shared keys and an application that uses public key encryption.

- Click the Objectives tab to learn about your first objective.
- Click the ASSET tab to learn about the asset being protected
- Review the network topology via the NETWORK tab
- With the cursor, hover over the individual users to see what they are thinking.
- Press the play button and observe what happens
- After an attack, right click on Joe's computer and view the packet log.
- Purchase replacement messaging applications by right clicking on the user's workstation and then selecting "Applications" / "Add/Remove Software".
- Observe the reaction of the IT support staff to your choice.
- Observe the reaction of Joe to your choice. Check his packet log and observe the new packets.

Provision the Messaging Application for a Third HR User

Check the objectives. You now have a new user in the HR department. You must provide that user with compatible messaging software. When you purchase this software, note the response of the IT support staff, based on you previous choices.

Stop Users from Cracking Each Other's Passwords

User authentication is achieved via a centralized authentication server. Each workstation sends a hash of the user's password to this server in the clear over the network. You cannot change this. However you can keep users from selecting weak passwords that are quickly cracked using brute force or dictionary attacks.

- Run the phase and observe the results of a user cracking another user's password.
- Select the "COMPONENT" tab, select the "Central Server" and adjust it settings to prevent users from selecting weak passwords.

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.

END OF LAB