**Instructor Notes for the ParaZog email Scenario**

December 2009

Students are expected to have completed the Hard Rain scenario to learn about use of PKI-enabled email clients to protect email.

This scenario is intended to illustrate the use of smartcard-base email encryption to protect email assets from unauthorized disclosure.

The scenario has several phases:

- Phase 1: Email is hosted on the "cloud" and the player can't change that.
  - Contractor that hosts the email has a motive to snoop
  - Player must deploy email encryption
  - Communications networks are protected via VPN and player starts with a CA that issues those certs. Player can choose to use that CA for email certs.
  - If player buys a Smart Card Minter and elects the use of smartcards, one of the users microwaves her smartcard.
- Phase 2: User must perform a remote site survey.
  - New asset and email goals introduced. User goes offsite to an office leased from the contractor who is motivated to snoop on the email. Player must encrypt the email.
  - User returns from site. If player did not use smartcards, and the player did not scrap the offsite computer, the contractor gets access to the offsite office (which they own) and compromises the key.
- Phase 3: High value assets
  - Two new users appear who need to access high value assets.
  - One of the existing users must also access one of these high value assets.
  - Player must buy new email server and workstations and establish an air gap.
  - Player must beef up physical security because one of the users is not cleared (or player can purchase background check).
  - If player deploys smartcard email on the new email server, assets are compromised because malware moves data from sensitive system to the other system.