Instructor Notes for the MAC Integrity Scenario
August 2010

Students are expected to have completed the MAC Scenario

The scenario is intended to illustrate the use of a multilevel server to enforce a MAC integrity policy. The scenario includes two LANs, two workstations and a multilevel server that contains a shared high integrity asset. One user must modify the asset, while the other user must read the asset while also using low integrity software and an internet connection. Students must assign secrecy and integrity labels to the multilevel server's two LAN connections. The high integrity asset is unclassified, so both networks should have secrecy labels of unclassified, otherwise old secret data will be compromised.

The scenario a single phase and students are encouraged to play it multiple times.

- The first play, students assign the correct labels to the multilevel server's networks and observe that the users achieve their goals and the asset is not compromised.
- Students are encouraged to play again, this time assigning a high integrity to the low integrity network. An attacker breaks in the weakly protected area where the low integrity workstation sits and compromises the high integrity data.
- If students strengthen the physical security, the asset will still be compromised via the Internet.
- If students disconnect the Internet, one user will fail a goal and the asset will still be compromised due to malicious software on a workstation.