

Name:

## Information Assurance: Homework 3

Due September 15, 2006

1. Consider network traffic that carries along a sensitivity label between machines. In class we discussed routing problems associated with using IP options to store the label. Assume you are asked to review a solution that uses IPSec to encode the label, and thus avoids the routing problem. Describe two problems that could arise from the introduction of labeled network traffic.
2. In class we discussed two systems that used category-only labels: Pitbull LX and SE Linux MCS. Their operators for comparing labels are slightly different. Pitbull LX requires the subject to have a superset of categories to access an object. MCS only requires intersection. The two systems also differ in that LX is a mandatory system. A normal user does not have the direct ability to add or remove categories from an object. While in SE Linux, a normal user can assign categories that associated with his account assuming he otherwise has access to the object. For the sake of the questions below, assume that both systems used the superset operator to test for access.
  - a. Consider a malicious user. Does the mandatory nature of the LX system better protect the system? How does it or how does it not?
  - b. Consider a careless user. Does the mandatory nature of LX better protect him from accidental data distribution? e.g., accidentally posting notes from an employee review meeting to a very wide audience. Again, why or why not?
3. Are the following threats or vulnerabilities? Briefly explain why.
  - a. The system administrator installs a mail delivery system with a buffer overflow bug.
  - b. Leslie accesses the unprotected wireless network of a competing firm.
  - c. Merlin sets his system password to be the same as his account name.
  - d. Ethel tosses a copy of her credit card statement with associated PIN information in the garbage at the post office lobby.
  - e. Carl takes home the laptop left at the coffee shop.

(Question 4 on next page)

Name:

4. Consider the following scenario. The university is worried about risk to one of its student computer labs. The lab contains 50 pentium-based work stations with flat screen monitors. All the computers can access the University's high speed internet connection. The computers also have access to department computers that have access to a range of information from student grades and future exams to professor's research results both public and private.
  - a. Identify at least 3 assets.
  - b. Identify two potential threats with their motivations.
  - c. For each threat source, rank the importance of the assets you identified in the first step.