

## Information Assurance: Homework 3 Answers

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.

*The intent of this problem was to get you to think about how adding checks to existing subsystems might cause problems. I was not trying to get you to think about the details of IPSec since we have not looked into that yet.*

*A couple problems that could arise:*

- *How do you make sure that labels on the two systems mean the same thing. For example, one system might have levels of High, Medium, and Low and the other system might have levels of Supreme, Good, Ok, and Poor. Which level on the first system does Good correspond to?*
- *If you apply BLP to network traffic, two way traffic is only possible if the labels are equal assuming you associate writing to the network with a pure write and reading from the network with a read. Much network traffic (like TCP) requires a two way traffic to ensure that the flow control traffic passes between the systems. Without the backchannel the network communication will mysteriously break.*
- *Simply adding a MAC check in the network stack where there was not one before will cause network traffic that had been accepted to no longer work.*
- *Most network implementations try to send ICMP messages to send back error messages. If they do not meet the MAC checks the ICMP messages will not be sent and make it that much harder to figure out what is going on.*
- *Adding labels to the network traffic will increase the packet size and have an effect on network performance.*

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.

*In this question I was trying to get you to focus on what kind of affect mandatory controls have on the security of the system. The LX and MCS systems are very similar except that normal users can select the labels to apply and in LX normal users are more constrained on the placement of labels on files.*

- 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?

*Assume the target user has A, B, and C labels associated with him. These correspond to projects that he is working on. Assume that management has decided that people cleared only for project C should not know about project A. Under the mandatory LX scheme the ISSO (privileged user) could have decided on the file labeling scheme beforehand and made sure that the project A files do not get other labels associated with them.*

*Therefore, a malicious user cannot apply a C label to an project A file. However, the malicious user could copy the contents of a project A file and paste it into a project C file. Or if the system prevents a direct a copy and past, a user cleared for both projects could look at the contents a project A file and retype that information into a project C file.*

*So while the LX system does prevent the direct labeling that would be allowed in MCS, it does not really prevent leaking information between two projects if the user is motivated to do so.*

- 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?

*In this case, the target user wants to comply with the system policy. Again, the user has labels A, B, and C associated with him. Say the user accidentally tries to copy a file labeled A into a C directory? Both LX and MCS would protect the user in this case.*

*Say the user is confused and thinks that a file really should be for project C. In MCS, he could attach a C label. In LX he could not. So the mandatory LX policy would protect the user from himself a little better.*

3. Are the following threats or vulnerabilities? Briefly explain why.
  - a. The system administrator installs a mail delivery system with a buffer overflow bug.

*The overflow bug is a vulnerability. One could also argue that an under trained system administrator that would install a program with a known bug is a threat.*

- b. Leslie accesses the unprotected wireless network of a competing firm.

*Leslie is a threat to the competing firm. The unprotected wireless network is the vulnerability she is exploiting.*

- c. Merlin sets his system password to be the same as his account name.

*Merlin, as a naïve user, is a threat. He is exploiting the vulnerability that the system allows him to set an obvious password.*

- d. Ethel tosses a copy of her credit card statement with associated PIN information in the garbage at the post office lobby.

*Ethel is a threat to herself. The vulnerability is the fact that credit card statement and the PIN are printed together, and the obvious vulnerability of leaving the information in a public place.*

- e. Carl takes home the laptop left at the coffee shop.

*Carl is a threat. He is exploiting the vulnerability of a forgetful coffee shop visitor.*

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.

*Some assets:*

- *The computer hardware*
- *Computer processing power*
- *Access to high speed network*
- *Student and class information*
- *Research results*
- *Homeworks*

- b. Identify two potential threats with their motivations.

*Threats and motivations:*

- *Cleaning staff – Earn money by stealing assets*
- *Cheater – Access information to improve grades*
- *Mafia – Use assets to mount broader attacks*
- *Research competitor – Access unpublished research results*

- c. For each threat source, rank the importance of the assets you identified in the first step.

*The assets I don't list would be of similar low value to the threat and ranked about the same.*

*Cleaning staff would most most value: 1. computer hardware, 2. student and class information, and 3. unpublished research information.*

*Cheater: 1. Homeworks, 2. Student and class information*

*Mafia: 1. Access to high speed network, 2. CPU processing power.*

*Research competitor: 1. Unpublished research results, 2. CPU processing power, 3. access to high speed network.*