

Spring 2009 – 22c:086 Networking & Security for Informatics
 Assignment #4 Due by 11:59pm on Thursday, April 16.

Problem 1: Firewalls (Review Question 11.5) [15 points] What is the difference between a packet-filtering router and a stateful inspection firewall?

Problem 2: Reference monitor (Problem 11.5) [20 points] In Figure 11.5 one link of the Trojan horse copy-and-observe-later chain is broken. There are two other possible angles of attack by Drake: Drake logging on and attempting to read the string directly, and Drake assigning a security level of sensitive to the back-pocket file. Does the reference monitor prevent these attacks?

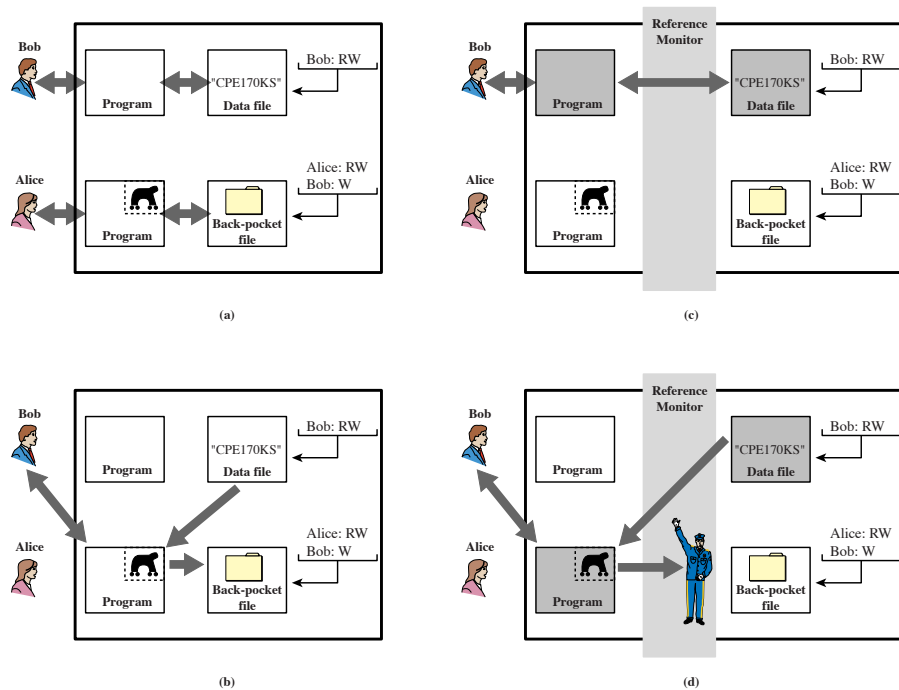


Figure 11.5 Trojan Horse and Secure Operating System

Problem 3: Intrusion detection [15 points] An example of host-based intrusion detection tool is the tripwire program. This is a file integrity checking tool that scans files and directories on the system on a regular basis and notifies the administrator of any changes. It uses a protected database of cryptographic checksums for each file checked and compares this value with that recomputed on each file as it is scanned. It must be configured with a list of files and directories to check, and what changes, if any, are permissible to each. It can allow, for example, log files to have new entries appended, but not for existing entries to be changed. What are the advantages and disadvantages of using such a tool? Consider the problem of determining which files should only change rarely, which files may change more often and how, and which change frequently and hence cannot be checked. Consider the amount of work in both the configuration of the program and on the system administrator monitoring the responses generated.