Outline for October 1, 2003

Reading: *Robust Programming* handout

Discussion Problem

A vendor informs a company that its system needs a patch installed to fix a security problem. The company obtains a copy of the patch, but does not install immediately. Instead, it puts the patch onto a test system and begins testing the patch

a. Assuming the vendor had thoroughly tested the patch on its systems, why do you think the company does this?
b. How might the company protect itself before the patch is distributed to all its systems?

Outline for the Day

1. Principles of Secure Design (*con't*)
   a. Principle of Separation of Privilege
   b. Principle of Least Common Mechanism
   c. Principle of Psychological Acceptability
2. Robust Programming
   a. Principles
   b. Fragile code's data structure
   c. Fragile code's creation, deletion of queues
   d. Robust code's tickets
   e. Robust code's creation, deletion of queues