COSC 6360--Operating Systems
GRADUATE PART OF QUALIFYING EXAMINATION
FINAL EXAMINATION

May 6, 2002

THIS EXAM IS CLOSED BOOK. YOU CAN HAVE TWO SHEETS OF NOTES. YOUR QUALIFYING EXAMINATION SCORE WILL BE BASED ON YOUR SCORE FOR THE TWO FIRST QUESTIONS.

1. ***FILE SYSTEM:***
All computer systems run a risk to be penetrated by an ***intruder*** who may damage the file system by tampering with the contents of some user files and/or deleting others. How could we design a file system that would protect user data against these two mishaps? You should assume that (a) all intrusions will always be detected within at most a couple of days and (b) your disk drives are normally between 40 and 60 percent full. (***Hint:*** your solution should not be encryption-based)
(20 points)

2. ***THIN CLIENTS:***
Back in the 1980s, Sun Microsystems introduced a series of ***diskless*** workstations that had many of the advantages touted for today's ***thin clients***. The idea was that diskless workstation would boot over the network from a central server. They would then remotely mount (using NFS) all file system partitions: read-only for the system partition and read-write for the user and swap partitions. Because there is no per-machine configuration information stored locally, every diskless workstation is essentially the same as any other. This lack of user configurability means fewer system administration headaches, especially with regards to software updates for many machines.

The designers of diskless workstations (or thin clients) and normal "diskful" computers made different basic security assumptions in their systems. For example, diskful computers do not rely on the network; instead, they rely on the authenticity of the operating system on their disks (that is, it is properly installed, etc; no verification is done).

Identify the assumptions and guarantees for the different types of machines, and discuss their practical validity in ***various situations***. (20 points)

3. What does an intruder need to do to convince a Kerberos server to accept a ***replay of an old authenticator*** as a valid authenticator? (5 points) What can the server do to protect itself against this kind of attacks? (5 points)

4. Consider a Totem protocol that would not include ***guaranteed vector messages***. What would be its major drawback? (5 points)

5. Why does Harp ***promote*** its witnesses after it detects a replica failure? (5 points)

6. What is the ***minimum amount of state*** you need to keep to implement the Sprite file consistency protocol? (10 points for a fully justified answer)

7. Why are MEMS using ***magnetic recording*** more complex than MEMS using ***phase-change-media***? (5 points)

8. What is the major motivation to use RAID today? (5 points)

9. Which data structures are used by the Sprite LFS to keep track of the locations of i-nodes? (2×5 points)

10. How does Farsite ensure the security of user files and directories? (2×5 points for an answer fully justifying Farsite solutions)