Name: _____ (First name first) **Score:** ____

COSC 6360 QUIZ #2 MARCH 30, 2009

Open book. You can consult **any** document you have **with you**, including those on your laptop.

1. One could envision a version of Kerberos that would assign to its users individual private keys and store on its server their public keys.

a. How would that make it the Kerberos server ***easier to secure***? (20 points)

Storing on the Kerberos server user public keys would make the server much easier to secure as these keys are not secret. We would only have to protect against key tampering and prevent malicious intruders from deleting or modifying user public keys.

b. How would the change ***affect the users*** of the system? (20 points)

Assigning private keys to the users associated with public keys maintained on the server would force the user to keep track of very long non-mnemonic keys.

2. What is the function of Kerberos ***authenticators***? (20 points)

Authenticators let services distinguish between valid request and unauthorized replays of previous requests.

3. How many simultaneous disk failures can a RAID level 5 tolerate without losing any data? (20 points)

A RAID level 5 can tolerate the loss of one of its disks without losing any data.

4. Why do RAID levels 3, 4 and 5 use ***omission correction codes*** instead of ***error correction codes***? (20 points)

RAID levels 3 to 5 use omission correction code because disks either operate correctly or fail to return any data. Hence, we only have to worry about missing data.