NAME: _____ (FIRST NAME FIRST) **SCORE**: _____

COSC 6360 SECOND MIDTERM OCTOBER 26, 2006

THIS EXAM IS **CLOSED BOOK**. YOU CAN HAVE ONE SHEET (I.E., TWO PAGES) OF NOTES..

1. Explain why Spin is (a) more *extensible* than Unix, (b) more *efficient* than Mach and (c) s*afer* than Windows? **(**3×5 points)

a) Spin is more extensible than Unix because _ you can add extensions to the Spin kernel

b) Spin is more efficient than Mach because _ extensions reside in the kernel address space

c) Spin is safer than Windows because _ extensions cannot trash the kernel _____

2. Consider a RAID-5 system with four data blocks per stripe (b_0, b_1, b_2, b_3) and one parity block p.

a) How much of the total disk space is used by the parity blocks? (5 points)

__ **20** ____ percent

b) What is the most efficient way to update block b_1? (10 points)

Read block(s) _ b_1 and p (assuming we did not have the old value of b_1 in memory)____

Compute _ new p = old b_1 ⊕old p⊕new b_1⊕ _____

Write new block b_1 and _ new block p _____

3. Which conditions should be met before ***Totem*** can deliver ***an agreed delivery*** message**?** (2×5 points)

a) A processor will not deliver a message before it has delivered all prior messages that have been issued by processors in the current configuration. _____

b) The previous messages to consider messages all have time-stamps within the duration of that configuration. _____

(Note: Should I rewrite the question today I would not have used this unnatural decomposition of the answer.)

4. A Totem system has three rings A, B and C. Which messages will a processor *X* be able to deliver assuming that it has received but not yet delivered messages with the following timestamps? (10 points)

From ring A: 4:50 PM

From ring B: 4:55 PM and 5:00 PM

From ring C: 4:45 PM and 5:05 PM,

Process *X* will deliver the messages that arrived at _ 4:45 PM and 4:50 PM _____

5. How could a malicious extension bypass the protection offered by Nooks ***lightweight protection domains*****?** (2×5 points)

a) It can remove the restrictions on its page map._____

b) It can use direct memory access (DMA) to bypass these restrictions _____

6. A system of physical clocks consists of two clocks, one that is slow and loses five minute every hour and another that is fast and advances by five minute every hour. Assuming that the clocks are managed by Lamport's physical clock protocol , what will be the time marked by each clock at two PM given that

a) both clocks indicated the correct time at noon;

b) the processor on which the ***slow clock*** resides sent at one PM one message to the other processor;

c) the message transmission delay was negligible;

d) no other messages were exchanged in the system. (2×5 points)

The fast clock will indicate __2__ hours __10__ minutes plus or minus a few seconds.

The slow clock will indicate __1__ hours __50__ minutes plus or minus a few seconds.

(Explanation: the message did not change anything.)

7. When will the following guarded command ***fail***? (2×5 points)

[value > 0; producer?P() → value:=value -1]

When either _ value becomes ≤ 0 _____

Or _ producer process terminates _____

8. Give ***one*** example of a ***covert channel***? (5 points)

_ Encoding some .information in the price billed for the service _____

9. What is a *replay?* (5 points) What does Kerberos to allow servers to distinguish relays from authentic messages? (10 points)

A replay is a retransmission of a legitimate message transmitted by an intruder that does not understand its contents. Kerberos detects replays by asking clients to include authenticators in their messages. These authenticators contain among other things a timestamp and are encrypted with a session key shared between the service and the user. Since the intruder does not know this session key, it cannot create new authenticators and can only resent them.

Kerberos detects previously sent authenticators by keeping track of the timestamps of recent authenticators and rejecting older ones.