CS4410 Spring 2009 Homework 6

20 True/False Questions, 5 points each.

(Just hand in a list: 20 question numbers, and True or False for each)

Due: Thursday April 23rd at 9:00am via CMS

1. **True False:** In Java, a **mutex** is identical to a **semaphore** initialized to 1.
2. **True False:** If you have one core (CPU) per thread, and your CPU supports a **test-and-set** instruction, a busy-wait loop would probably have the smallest delays and lowest overheads among ways of implementing critical sections.
3. **True False:** The Banker's Algorithm never allows a deadlock to occur, but may sometimes delay a resource request unnecessarily (that is, may force a process to wait when, in fact, granting its request immediately would not actually have resulted in a deadlock).
4. **True False:** By invalidating one or more of the 4 conditions for deadlock, an application can ensure that it is deadlock-free, but might not ensure that it is *livelock* free.
5. **True False:** The term **thrashing** is used to describe a situation in which some set of threads is able to make unlimited progress, but some other subset of one or more threads never manages to enter the critical section.
6. **True False:** Virtual memory allows a process to use an unlimited amount of memory with the same performance as if all its pages fit into physical memory.
7. **True False:** The WS Clock cleans pages when it evicts them from the working set, but because those pages end up in a reclaim pool, once a page has been paged in once, it will never actually need to be paged in from the disk again – if the page is ever needed, it can just be retrieved from the reclaim pool.
8. **True False:** When context switching between threads within the same process, the O/S must flush the TLB but not the L2 cache.
9. **True False:** When accessing files that are on a remote file server implementing the NFS protocol, any data read or written would be visible to an intruder who is passively wiretapping the network and simply watching the packets travelling back and forth.
10. **True False:** A web browser that supports Javascript and the AJAX environment is in many senses a simple operating system.
11. **True False:** A person's private medical records could be secured by creating an asymmetric key pair and then encrypting the record with the *private* key from the pair. The corresponding public key could then be registered in exactly the same way that Amazon.com publishes its public key for use when we make an HTTPS connection to a secure web site such as Amazon.com's "my account" site. A health care giver would look up the public key and could then unlock the medical record, but third parties who aren't supposed to access the record would be unable to do so.
12. **True False:** A person's private medical records could be secured by encrypting them with a symmetric key and only giving a copy of that key to health providers with a legitimate reason to access the record.

13. **True False:** When using TCP to transfer data over the Internet, if loss occurs TCP will react by slowing down its transmission rate, under the assumption that a router or link has become overloaded.
14. **True False:** When using TCP to transfer data over a wireless connection, if loss occurs TCP will react by retransmitting packets more aggressively, so as to overcome the inherent lossy nature of wireless communication.
15. **True False:** Network address translation, used between the clients of a data center such as Amazon.com and center itself, makes it possible for Amazon.com to have a single IP address (or perhaps two, if Amazon.com has two internet providers). TCP connections combine this IP address with per-connection port-numbers to "represent" a much larger number of connections between specific clients to specific computers with distinct IP addresses within the data center.
16. **True False:** The "end to end" reliability argument says that when one router passes packets to another router, any loss that occurs on the link between them should be corrected by the pair of routers, so that the end point applications can treat the Internet as a reliable, lossless transport mechanism.
17. **True False:** One reason that modern operating systems don't make very much use of the TPM (trusted platform module) is that a virus can so easily steal the secret TPM keys.
18. **True False:** If a virus installs itself as a virtual machine on your computer, even virus scanning products might not be able to detect the problem.
19. **True False:** Protocols such as SSL generally use asymmetric keys as a kind of bootstrapping mechanism with which the endpoints can negotiate symmetric keys that they then use for the data-exchange part of a secured session, because asymmetric cryptography is much slower than symmetric cryptography.
20. **True False:** With a blinded signature protocol, one could create a proof that a particular document existed in a certain form at a certain time, and yet the agent signing the document would not be able to see the data it was signing. The unblinded document and the associated signature could later be shared with the public, so that anyone could read the document, and could also confirm that the signature is valid.