CS4410 Spring 2009 Solutions to Homework 6

These questions were all true/false and we didn't ask for explanations, but in this answer set Ken is providing a line or two to clarify precisely why the answer was what it was!

1. **True False:** In Java, a **mutex** is identical to a **semaphore** initialized to 1.
   True : A Java mutex is a member of the semaphore class and supports the identical methods.
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.
   *True : With a little luck, when one thread gives up a lock, some other thread will grab it in just a few CPU cycles – just long enough for a zero to be stored into memory and for the next **test-and-set** operation to execute. Can't get lower delays than that!*
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).
   True : the Banker's algorithm is conservative, basically planning for worst-case behavior. For example, suppose a process declares a worst-case need for 10 units of resource X. The Banker's algorithm schedules under the assumption that 10 units will be needed, but perhaps the process will never even request a single unit of X in this particular run. Thus the Banker will have been overcautious, and this typically "maps" to blocking a process when it could have been allowed to execute.
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.
   True. A deadlock can't arise unless the four necessary conditions all hold. Thus by invalidating one, say "hold and wait", we can guarantee that the application won't deadlock. Livelock is a different issue and some of the very changes that eliminate deadlock simply cause a livelock under the original deadlock conditions!
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.
   False (total gibberish). Thrashing is a term related to virtual memory and paging, and has nothing at all to do with threads and critical sections.
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.
   False : Virtual memory often carries a very high cost. And in any case, no computer allows a process to use "unlimited" 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.
   False: The pages in the reclaim pool are used when a place is needed to satisfy a page fault (when the WS Clock algorithm needs to page something in). So yes, if WS Clock gets lucky it

will need some page again before it gets overwritten with something else and in that case, yes, the page won't need to be re-read. But very often by the time that page fault happens, the page in question will have been rewritten to contain some other page.

8. **True False:** When context switching between threads within the same process, the O/S must flush the TLB but not the L2 cache.

   False. When context switching within a single process, neither the TLB nor the L2 cache needs to be flushed, because their contents remain valid.

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.

   True. NFS sends packets in an unencrypted form and anyone watching the network can see the data in them. (The answer changes if you use SUN's secured version of NFS, but as we discussed in class, not many NFS users are able to do so).

10. **True False:** A web browser that supports Javascript and the AJAX environment is in many senses a simple operating system.

    True. AJAX defines a whole collection of system calls and Javascript is a programming language. So this has all the features of a true O/S, albeit a simple one.

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.

    False. Total nonsense. By definition a public key is public – anyone can find it. So anything encrypted with a private key can be decrypted by <u>anyone</u> who wants 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.

    True. With symmetric keys, only the individuals who have a copy of the key can access the record. You would want to be careful how you give out keys, obviously.

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.

    True. TCP's backoff mechanisms are designed under this assumption (linear throughput increase, multiplicative decrease).

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.

    False. TCP has just one mode of operation, namely the one asked about in question 13. TCP doesn't know that it is running on a wireless connection and any packet loss is treated as if it was caused by an overload in a core Internet router.

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.

True: This is a short summary of exactly the way that NAT boxes (often included in your firewall or wireless router) work.

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.

    False: The end-to-end reliability argument actually is exactly the opposite. It says that low level Internet links shouldn't worry about reliability because the endpoints will do so in any case, and worrying about the issue at a low level is (1) pointless, because there are other conditions under which they can get lost anyhow, and (2) expensive.

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.

    False: A TPM has the keys burned in and you can't steal them, period. The reason few operating systems make much use of the TPM is that nobody has figured out what the best way to do so would be.

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.

    True: If a virus virtualizes a computer, the virus scanner might end up running in a clean virtual machine, rather than on the true "raw" operating system…

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.

    True: This is precisely how SSL works.

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.

    True: This is one of the very cool features of the RSA form of public key cryptography. It gets used in some applications, such as electronic voting systems.