Answer sheet for CS 136 Final Exam, Spring 2009

1. d
2. a
3. c
4. d
5. a
6. c
7. d
8. c
9. a
10. c
11. b
12. a
13. c
14. a
15. b
16. d
17. b
18. a
19. b
20. a
21. c
22. b
23. d
24. d
25. d
26. a
27. c
28. b
29. b
30. c

Short answer questions

1. One can argue this question either way, and the main point is to do so intelligently. It's like a firewall because it's protective, it frequently relies on what amounts to signature matching, and it typically examines most or all input. It's like a honeypot because it needs fairly deep understanding of what's going on, it doesn't reject attack inputs, and (depending on type) may need to be stateful.
2. A worm with a good random number generator will visit each IP address once before it visits any address twice, allowing the fastest possible spread.
3. Keys used for permanent storage will never (or, at most, rarely) be changed. Keys used for message transit will be used once and discarded. One might argue the permanent storage key must be of higher quality. However, if the message remains critical forever, then, again, the key must never be learned.
4. If malware can infect peripherals, then cleaning a machine requires cleaning all infectable peripherals. One can't simple use a clean boot disk.
5. Error handling is important in writing secure code because attackers will force your error handling code to be exercised, looking for a flaw. Since such code is rarely tested and used, it is more likely to contain such a flaw, so special care is necessary with it.