1. What is a digital signature?
    Ties data to an individual. Identifies the signer
2. What are four properties of a digital signature?
    a. Cannot be altered
    b. Can't produce a match
    c. Indication of who applied signature
    d. Validation that signature is authentic
    e. A file
3. What is the purpose of a digital certificate?
    Binds an identity to a public key
4. What is the basic structure of a digital certificate?
    Managerial structure - Single Hierarchy Authority.
5. What is a certificate chain?
    Root certificate, intermediate certificate, and end entity. All trusting one another.
6. What is a certificate authority?
    A large group of trusted entities
7. What happens if a certificate is lost or stolen?
    Nothing. Certificates are public
8. What is the real source of computer security problems? (The software/applications)
    Errors, Faults, and Failures
9. IEEE Terminology:
    a. Error - Human Mistake
    b. Fault - Incorrect step, command, process, or data definition in a computer program
    c. Failure - departure from the system's required behavior
10. What are functional requirements of a program?
    Set of inputs, behavior, and outputs
11. What are security requirements of a program?
    CIA - Confidentiality, Integrity, Availability.
    a. Session management - used to maintain state
    b. Error management - Provides errors and traces in correct scope.
    c. Configuration management - Drive features and functionality
12. What does Penetrate and Patch mean?
    Fixing one fault often causes a failure somewhere else. Sony Hack 2005
13. What is the cost of fixing bugs in an application at different stages of development?
    a. 10x-100x more expensive after deployment.
    b. Customer satisfaction
    c. Lost referrals
    d. Lost customers
    e. Lost productivity
14. How does a buffer overflow work?
    Overwriting bounds of a buffer
15. How does the stack work?

Subprocedure calls are handled with a stack. Most recent item inserted is the next removed. Stack Smashing - overwriting stack memory.

16. What is a setuid program?
    A program that is run under a certain user ID
17. What dangers does a setuid program present?
    If i is owned by root and the user smashes the stack, they have root access
18. How can I defend against a buffer overflow attack?
    Stay in bounds. Check lengths. Check procedures that may overrun space. Limit privileges of program.
19. What is incomplete mediation?
    a. Not checking input/authentication
    b. Client can send anything
    c. Can't trust client at all
20. What is a time-of-check-to-time-of-use-error?
    Synchronization of data
21. What is an undocumented access point?
    An easy way of accessing internal of a module. Usually in development.
22. Why should I be concerned with libraries and utilities?
    They can't be trusted
23. How does trust impact computer systems?
    You shouldn't use what can't be trusted.
24. What is a virus?
    Self Replicating Malware
25. What is a worm?
    Spreads through network. Standalone program
26. What is a Trojan Horse?
    Program with benign features. Secondary Malware inside
27. What is a logic bomb/time bomb?
    Waits for a condition or time before executing
28. What is the name of the important security report that was written in the 1970's for the department of defense?
    Ware report. Security report.
29. What was the Morris Worm? What Year?
    1988 Infected 3000 victims
30. What was the Morris worm attempting to do?
    Count number of computers on network
31. Know the following from page 175
    a. Melissa - Virus Spreads through email address book
    b. ILoveYou - Worm propagates by email containing malicious script. Uses address book to expand infection. 50 million computers affected.
    c. Code Red - Attacked whitehouse.gov. Resides only in memory.
    d. Nimda - Spread to 2 million machines in 24 hour period
    e. Stuxnet - Worm attacks SCADA automated processing system. Zero day attack

32. What is a zero-day attack?
    Exploit found before vulnerability is patched
33. Is there evidence that patches really protect against attacks? Why?
    Yes. Over the years fewer zero day attacks
34. What are the three categories of harm from malicious code?
    a. Nondestructive
    b. Destructive
    c. Criminal/Commercial Intent
35. What are examples of
    a. Harm to User - email spoofing, keylogger
    b. Harm to System - hide malware, OS/AVS
    c. Harm to Society - Morris worm, i love you
36. Describe the following types of virus infections
    a. Appended virus - Attaches itself to program. Before executable instruction
    b. Surrounding Virus - Same - has control before and after execution
    c. Integrated Virus - Replaces some of target. Integrates through program
37. What are goals of malware? Page 185
    a. Stealth
    b. Not easily destroyed or deactivated
    c. Spreads Widely
    d. Can reinfect
    e. Easy to create
    f. Machine, OS independent
38. What is a boot sector virus?
    Continuing attack. Control of virus begins at bootup. Many modules. Infect single module
39. What is one-time-execution/implanting?
    This step is to acquire and install the code/ download. Not obvious to the user.
40. What is a memory resident virus?
    Remains in memory. Keylogger, allows reinfection through HD
41. What are application targets for a virus?
    a. OS
    b. Compiler
    c. Antivirus
    d. Interpretive programs (Programs that open/read data. Word, pdf, etc)
42. Why is user vigilance important? What is it personally? What is it for a company?
    Hygiene - not engaging in behaviour that permits malicious code contamination.
    a. Personally - Test on isolated computer
    b. Commercially - Only use commercial software acquired from reliable, well established vendors
43. AVS Techniques
    a. Signature detection - Searches memory watching for signatures of viruses
    b. Byte sequence detection
    c. Execution Patterns - Reverse engineer a binary. IDApro

    d. Storage Patterns - Uses code or checksum to detect changes to a file. Then looks for patterns

44. What is a polymorphic virus?
    Many forms of the virus
45. What is an encrypting virus?
    On the HD. Decrypt sequence = signature
46. What is the signature for an encrypting virus?
    The decrypt sequence
47. What are the following countermeasures to malware? (Developer Perspective)
    a. Modularity
    b. Encapsulation
    c. Information Hiding
    d. Mutual Suspicion
    e. Confinement
    f. Simplicity
    g. Genetic Diversity
48. Testing techniques
    a. Functional Testing
    b. Unit Testing
    c. Performance Testing
    d. Integration Testing
49. What is penetration testing?
    Trying to crack a system being tested. Testing inputs
50. What is the effectiveness of penetration testing?
    Best countermeasure to validate input
51. What are limitations of testing?
    a. Can demonstrate the existence of a problem
    b. Can’t demonstrate the absence of a problem
52. Why is input validation so critical to perform?
    Best countermeasure to prevent vulnerabilities