1. Multics
    a. Chief architects: Jerome Saltzer & Michael Schroeder
    b. Predecessor to UNIX. UNIX grew out of this
    c. MIT, AT&T, and GE were partners
2. Countermeasure Principles
    a. Least Privilege - Lowest Access
    b. Economy of Mechanism - Each protection small. KISS
    c. Open Design - Little encryption. Does not rely on secrecy
    d. Complete Mediation - Every access attempt is checked
    e. Permission Based - Default condition to deny access. Who can access what
    f. Separation of Privilege - Require multiple methods of diving system into sections for authorization
    g. Least Common Mechanism - limiting sharing of objects. Logical or physical separation. Have different physical network. Logic - VPN
    h. Ease of Use - Protection mechanisms that are easy to use are not avoided
3. CERT's Top 10 Secure Coding Practices
    a. Validate Input
    b. Heed compiler warnings
    c. Architect and design for security policies
    d. Keep it simple
    e. Default to deny
    f. Adhere to principle of least privilege
    g. Sanitize data sent to other systems
    h. Practice defense in depth
    i. Use effective quality-assurance techniques
    j. Adopt a secure coding standard
4. Defensive Design
    a. Anticipate what can go wrong
    b. Plan for malicious attacks
    c. Identify AND withstand an attack
    d. It's the design. Security isn't an add-on
5. Countermeasures that don't work
    a. Penetrate & Patch - Systems built cost to fix high. Systems complex. More likely to introduce more problems.
    b. Security by obscurity
6. Browser Issues
    a. Data fetched from multiple places
    b. Install extensions
    c. Browser can access your system. - Malware
    d. Authentication
7. Attacks
    a. Man-in-the-middle - Extension/addon installed
    b. Keystroke Logger - Records keystrokes you type

    c. Page-in-the-middle -
    d. User-in-the-middle - Captcha!
8. Human Authentication - CAPTCHA
9. Computer Authentication shared secret. Problems - overused
    a. Mother's maiden name
    b. Personal questions
    c. CVV, CVC
10. Communication Authentication
    a. Initial - One Time password ex. multifactor
    b. Ongoing/Continuous - ex. Debit card pin number
11. Misleading web content - graffiti, defacement
12. Malicious web content - Injection attacks, XSS
13. Protecting against web file changes - backups, hash, tripwire tool
14. Web/Bug tracker - 3rd party cookie
15. ClickJacking - object on page. Don't mean to click
16. Drive-by-download - download without permissions, install w/o permission
17. Protecting against malicious content
    a. Validate inputs
    b. Permissions, Access control
    c. Writing secure code
18. Cross-site scripting attack
    a. Reflective - response depends on user input. Malicious link, link contains input
    b. Persistent - Script stored on server
19. SQL Injection - give input to application, make system execute query
20. Directory traversal - adding ../../../../etc/passwd to access information
21. Email SPAM
    a. 68-90% of all email is spam
    b. Sources: China 23%, 19% USA, SKorea 14%
    c. Subjects: 69% Sexual, 17% Pharmaceuticals, 6% Jobs
    d. Why use email attacks? Advertising, build brand recognition, stock pump & dump, malicious data, links, files, free
22. Legal protections against SPAM
    a. CAN-SPAM US
    b. Legitimate vs criminal
    c. Passing laws vs implementing
23. Technical protections against SPAM
    a. Source addresses - screen with AVS
    b. Volume control
    c. postage
24. Phishing - email/web attack that tries to get users to give information
    a. Spear phishing - targeted/personal
25. Network security
    a. Client - requester of information

b. Server - giver of information
c. Node - any system in network that does computation
d. Attacker - any node
e. Victim - any node

26. Network Characteristics
    a. Anonymity
    b. Automation
    c. Distance
    d. Opaqueness
    e. Routing diversity
27. Transmission Media
    a. Wired cat5/6, coax, fiber
    b. Wireless - radio, microwave, infrared, satellite
    c. No boundaries on wireless communication
28. Layered communication
29. ISO - International Standards Organization
30. OSI - Open Systems Interconnect
31. ISO/OSI - Combined
32. OSI Model - layers to describe network communications
    a. 7. Application
    b. 6. Presentation
    c. 5. Session
    d. 4. Transport
        i. Flow control
        ii. Error detection
        iii. Example - TCP. UDP, SSL, TLS
        iv. addressing - ports
    e. 3. Network
        i. Routing
        ii. Use packets of data
        iii. IP, IPSec, Arp-address
        iv. Addressing - IP address

f. 2. Data Link
    I. Reliable delivery over link
    Ii. MAC - Median Access Control
    Iii. 802.11 - wireless protocol
    Iv. addressing MAC, using frames

E. 1. Physical Layer
    I. Bit transmission

To know-
Layer 5-7 (Application): DNS, FTP, HTTP, IRC, Kerberos
Layer 4 (Transport): Flow control, error detection, TCP, UDP, SSL/TLS, Ports

Layer 3 (Network): Routing, Message blocking, IP, IPSec, ARP, Packets
Layer 2 (Data Link): link to link, MAC, 802.11, MAC Addresses
Layer 1 (Physical Layer): Bit transmission

33. Types of networks
    a. LAN - Local Area Network - Small, <100 users, locally controlled, physically protected, limited scope (dept, floor)
    b. WAN - Wide Area Network - Larger than lan, out of control, CAN (campus area network), MAN (metropolitan area network)
    c. Internet and internet: Internet - world wide web, internet - connected network
34. Threats in networks
    a. Application Vulnerabilities
    b. Network vulnerabilities
35. Non-hardware vulnerabilities
    a. Software
    b. Protocols
    c. Routing
36. Causes of vulnerabilities
    a. Anonymity
    b. Many points of attacks
    c. Sharing of resources/info
    d. Complexity of systems
    e. Unknown perimeter
    f. Reconnaissance - port scanning, dumpster diving, etc
37. Protocols to know
    a. ARP - Address Resolution Protocol: translate IP to MAC address
    b. TCP - Transmission Control Protocol: Performs 3 way handshake. Checks for all packets
    c. DNS - Domain Name System - Domain address -> IP address
    d. IP - Internet protocol
    e. UDP - User Datagram Protocol: Doesn't care about entire set of dat
39. TCP Handshake
    a. Seq & ACK numbers
    b. SYN-ACK syn 1, ack1
    c. ACK# = seq# + 1
40. Attacks
    a. ARP spoofing - fake reply, fake gratuitous ARP
    b. TCP hijacking - Sniff/monitor, inject a valid TCP message, block one side. Man-in-middle
    c. DNS poisoning - DNS Spoofing
41. Threats
    a. Interception
    b. Modification
    c. Fabrication
    d. Interruption
    e. Reconnaissance

42. Port scanning
43. Famous Attacks
    a. Malformed packets
    b. Ping flood -Ddos
    c. Ping of Death - malformed ping. Larger than 65k bytes
    d. Smurf Attack - broadcast message. Spoof sender ip
    e. Land Attack - making host/source address the same.
    f. Syn-flood - Spoof the source of a syn packets
44. Botnets network of compromised computers under control
45. Botnet management - availability, pattern, patching system.
46. Botnet market - spam, child porn
47. Firewall types
    a. Packet filtering gateway - looks at header information. Detects spoofing internal address
    b. Stateful inspection - looks at multiple packets
    c. Application Proxy - simulate the end application
    d. Guard - modify data to pass on
    e. Personal firewall - redirect traffic to AVS, limit download locations
48. Honeypot - all malicious traffic, system has no functional purpose, source for attack into signatures
49. Intrusion Detection Systems (IDS) - firewall, identify active attacks for malware, complementary to firewall
50. Signature based IDS - pattern matching - date, behavior. Complex rule set, large rule set
51. Heuristic based IDS - Identify something out of the ordinary, what is norma? Very difficult
52. IDS Issues - false positives, false negatives, alerts are better than auto response, costs - risk analysis