1. Multics
    a. Chief architects: Jerome Saltzer & Michael Schroeder
    b. UNIX grew out of this
    c. MIT, AT&T, and GE were partners
2. Countermeasure Principles
    a. Least Privilege
    b. Economy of Mechanism
    c. Open Design
    d. Complete Mediation
    e. Permission
    f. Separation of
    g. Least common mechanism
    h. Ease of use
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 problems
    b. Plan for attack
    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
    b. Security by obscurity
6. Browser Issues
7. Attacks
    a. Main-in-the-middle
    b. Keystroke logger
    c. Page-in-the-middle
    d. User-in-the-middle
8. Human Authentication
9. Computer Authentication
10. Communication Authentication
    a. Initial
    b. Ongoing/Continuous

11. Misleading web content
12. Malicious web content
13. Protecting again web file changes
14. Web/Bug tracker
15. ClickJacking
16. Drive-by-download
17. Protecting against malicious web content
    a. Access controls
    b. Webpage owner responsibility
    c. Writing good code
18. Cross-site scripting attack
    a. Reflective
    b. Persistent
19. SQL Injection
20. Directory traversal
21. Email SPAM
22. Legal protections against SPAM
23. Technical protections against SPAM
24. Phishing
25. Network security
26. Network characteristics
    a. Anonymity
    b. Automation
    c. Distance
    d. Opaqueness
    e. Routing diversity
27. Transmission Media
28. Layered communication
29. ISO
30. OSI
31. IOS/OSI
32. OSI Model
    a. 7 layers
    b. Know names
    c. Common protocols at each layer
    d. Purpose of each layer
33. Types of networks
    a. LAN
    b. WAN
    c. Internet and internet
34. Threats in networks
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
37. Reconnaissance
    a. Technical
    b. Non-technical
38. Protocols to know
    a. ARP
    b. TCP
    c. DNS
    d. IP
    e. UDP
39. TCP Handshake
    a. Seq & ACK numbers
40. Attacks
    a. ARP spoofing
    b. TCP hijacking
    c. DNS poisoning
41. Threats
    a. Interception
    b. Modification
    c. Fabrication
    d. Interruption
    e. Reconnaissance
42. Port scanning
43. Famous Attacks
    a. Malformed packets
    b. Ping flood
    c. Ping of Death
    d. Smurf Attack
    e. Land Attack
    f. Syn-flood
44. Botnets
45. Botnet management
46. Botnet market
47. Firewall types
    a. Packet filtering gateway
    b. Stateful inspection
    c. Application Proxy
    d. Guard

    e. Personal firewall
48. Honeypot
49. Intrusion Detection Systems
50. Signature based IDS
51. Heuristic based IDS
52. IDS Issues