1. Multics

1. Chief architects: Jerome Saltzer & Michael Schroeder
2. Predecessor to UNIX. UNIX grew out of this
3. MIT, AT&T, and GE were partners

2. Countermeasure Principles

1. Least Privilege - Lowest Access
2. Economy of Mechanism - Each protection small. KISS
3. Open Design - Little encryption. Does not rely on secrecy
4. Complete Mediation - Every access attempt is checked
5. Permission Based - Default condition to deny access. Who can access what
6. Separation of Privilege - Require multiple methods of diving system into sections for authorization
7. Least Common Mechanism - limiting sharing of objects. Logical or physical separation. Have different physical network. Logic - VPN
8. Ease of Use - Protection mechanisms that are easy to use are not avoided

3. CERT’s Top 10 Secure Coding Practices

1. Validate Input
2. Heed compiler warnings
3. Architect and design for security policies
4. Keep it simple
5. Default to deny
6. Adhere to principle of least privilege
7. Sanitize data sent to other systems
8. Practice defense in depth
9. Use effective quality-assurance techniques
10. Adopt a secure coding standard

4. Defensive Design

1. Anticipate what can go wrong
2. Plan for malicious attacks
3. Identify AND withstand an attack
4. It’s the design. Security isn’t an add-on

5. Countermeasures that don’t work

1. Penetrate & Patch - Systems built cost to fix high. Systems complex. More likely to introduce more problems.
2. Security by obscurity

6. Browser Issues

1. Data fetched from multiple places
2. Install extensions
3. Browser can access your system. - Malware
4. Authentication

7. Attacks

1. Man-in-the-middle - Extension/addon installed
2. Keystroke Logger - Records keystrokes you type
3. Page-in-the-middle -
4. User-in-the-middle - Captcha!

8. Human Authentication - CAPTCHA

9. Computer Authentication shared secret. Problems - overused

1. Mother’s maiden name
2. Personal questions
3. CVV, CVC

10. Communication Authentication

1. Initial - One Time password ex. multifactor
2. 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

1. Validate inputs
2. Permissions, Access control
3. Writing secure code

18. Cross-site scripting attack

1. Reflective - response depends on user input. Malicious link, link contains input
2. 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

1. 68-90% of all email is spam
2. Sources: China 23%, 19% USA, SKorea 14%
3. Subjects: 69% Sexual, 17% Pharmaceuticals, 6% Jobs
4. Why use email attacks? Advertising, build brand recognition, stock pump & dump, malicious data, links, files, free

22. Legal protections against SPAM

1. CAN-SPAM US
2. Legitimate vs criminal
3. Passing laws vs implementing

23. Technical protections against SPAM

1. Source addresses - screen with AVS
2. Volume control
3. postage

24. Phishing - email/web attack that tries to get users to give information

1. Spear phishing - targeted/personal

25. Network security

1. Client - requester of information
2. Server - giver of information
3. Node - any system in network that does computation
4. Attacker - any node
5. Victim - any node

26. Network Characteristics

1. Anonymity
2. Automation
3. Distance
4. Opaqueness
5. Routing diversity

27. Transmission Media

1. Wired cat5/6, coax, fiber
2. Wireless - radio, microwave, infrared, satellite
3. 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

1. 7. Application
2. 6. Presentation
3. 5. Session
4. 4. Transport
   1. Flow control
   2. Error detection
   3. Example - TCP. UDP, SSL, TLS
   4. addressing - ports
5. 3. Network
   1. Routing
   2. Use packets of data
   3. IP, IPSec, Arp-address
   4. 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

1. LAN - Local Area Network - Small, <100 users, locally controlled, physically protected, limited scope (dept, floor)
2. WAN - Wide Area Network - Larger than lan, out of control, CAN (campus area network), MAN (metropolitan area network)
3. Internet and internet: Internet - world wide web, internet - connected network

34. Threats in networks

1. Application Vulnerabilities
2. Network vulnerabilities

35. Non-hardware vulnerabilities

1. Software
2. Protocols
3. Routing

36. Causes of vulnerabilities

1. Anonymity
2. Many points of attacks
3. Sharing of resources/info
4. Complexity of systems
5. Unknown perimeter
6. Reconnaissance - port scanning, dumpster diving, etc

37. Protocols to know

1. ARP - Address Resolution Protocol: translate IP to MAC address
2. TCP - Transmission Control Protocol: Performs 3 way handshake. Checks for all packets
3. DNS - Domain Name System - Domain address -> IP address
4. IP - Internet protocol
5. UDP - User Datagram Protocol: Doesn’t care about entire set of dat

39. TCP Handshake

1. Seq & ACK numbers
2. SYN-ACK syn 1, ack1
3. ACK# = seq# + 1

40. Attacks

1. ARP spoofing - fake reply, fake gratuitous ARP
2. TCP hijacking - Sniff/monitor, inject a valid TCP message, block one side. Man-in-middle
3. DNS poisoning - DNS Spoofing

41. Threats

1. Interception
2. Modification
3. Fabrication
4. Interruption
5. Reconnaissance

42. Port scanning

43. Famous Attacks

1. Malformed packets
2. Ping flood -Ddos
3. Ping of Death - malformed ping. Larger than 65k bytes
4. Smurf Attack - broadcast message. Spoof sender ip
5. Land Attack - making host/source address the same.
6. 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

1. Packet filtering gateway - looks at header information. Detects spoofing internal address
2. Stateful inspection - looks at multiple packets
3. Application Proxy - simulate the end application
4. Guard - modify data to pass on
5. 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