Telecommunications and Network Security

Mike Smith

26/04/10 - Rev.33

Wireless

- Spread spectrum - distributed across frequency range
- Frequency Hopping Spread Spectrum - FHSS - portion
- Direct Sequence Spread Spectrum - DSSS - all
- Need an Access Point - AP
- Hosts in group must use Service Set ID - SSID
- Authentication
  - Open System Authentication - OSA - in clear
  - Shared Key Authentication - SKA = WEP
  - Wired Equivalent Privacy - WEP - weak
  - Wi-Fi Protected Access - WPA, WPA2 - uses TKIP
- Best Practice
  - Enable 802.11i e.g. WPA
  - Change default SSID
  - Disable broadcast SSID
  - Add RADIUS or Kerberos
  - Put AP at centre of building and in DMZ
  - Implement VPN for wireless devices
  - Configure AP to allow only known MAC addresses
  - Disable DHCP
- Mobile Phones
  - WAP
  - i-Mode - Japan, Asia, Europe
  - Bluetooth - 802.15

OSI Model

- Australia Post Sucks It Never Delivers Parcels
- Application - FTP, TFTP, SNMP, SMTP, Telnet, HTTP
- Presentation - ASCII, EBCDIC, TIFF, JPEG, MPEG, MIDI
- Session - NFS, NetBIOS, SQL, RPC
- Transport - TCP, UDP, SSL/TLS, SPX
- Network - IP, ICMP, IGMP, RIP, OSPF, IPX
- Data Link - ARP, RARP, PPP, SLIP
- Physical - HSSI, X.21, EIA/TIA-232, EIA/TIA-449
- List of Protocols

TCP/IP

- Australian Trains Never Late
- Application
  - TCP - Stream
  - UDP - Message
- Transport
  - TCP - Segment
  - UDP - Packet
- Network - TCP and UDP Datagram
- Data Link - TCP and UDP Frame

WAN Technologies

- Channel Service Unit/Data Service Unit - CSU/DSU
- Switching
  - ISDN
    - BRI ISDN = 2 x B + 1 x D
    - PRI ISDN = 23 x B + 1 B
    - Broadband ISDN
  - Circuit
    - PSTN
  - Packet
    - X.25
    - Frame Relay
    - Cell - ATM
- Switched Multimegabit Data Service - SMDS
- Synchronous Data Link Control - SDLC
- High-level Data Link Control - HDLC
- High-Speed Serial Interface - HSSI
- SS7, VoIP, Session Initiation Protocol - SIP
- Tunneling Protocols
  - IPSec
  - PPP
  - PPTP
  - L2TP
- Authentication Protocols
  - Password Authentication Protocol - PAP - least secure
  - Challenge Handshake Authentication Protocol - CHAP
  - Extensible Authentication Protocol - EAP
  - RADIUS, Diameter, TACACS

Packets and Ports

- Well-known ports 0 - 1023
- TCP: Sequence and Acknowledgement numbers
- UDP: Source, Destination, Length, Checksum, Data
- 23 - Telnet
- 25 - SMTP
- 80 - HTTP
- 161, 162 - SNMP
- 20, 21 - FTP

IP Addressing

- IPv4 - 32 bits, IPv6 - 128 bits
- Class A: 0.0.0.0 - 127.255.255.255
- Class B: 128.0.0.0 - 191.255.255.255
- Class C: 192.0.0.0 - 223.255.255.255
- Class D - Multicast: 224.0.0.0 - 239.255.255.255
- Class E - Reserved: 240.0.0.0 - 255.255.255.255
- Subnetting

Network Devices

- Repeaters
  - Works at Physical Layer
  - Amplify signal
  - Clean up signal
  - Hub = multiport repeater
  - Hub also known as a concentrator
- Bridges
  - Works at Data Link Layer
  - Connect LAN segments
  - Filters based on MAC address
  - Retains same broadcast domain
  - Isolates collision domains
  - Can translate between protocols
- Routers
  - Works at Network Layer
  - Can connect different networks
  - Uses routing protocols: RIP, BGP, OSPF
  - Can filter based on IP address and protocols
- Switches
  - Combine functionality of a repeater and bridge
  - Can work at layer 3 and 4, can use tags = MPLS
  - Used to provide QoS
- Other: VLANs, Gateways, PBXs
- Firewalls
  - Packet Filtering & Dynamic Packet Filtering
  - Stateful
  - Proxy & Kernel Proxy
  - Dual-Homed
  - Screened Host & Screened Subnet

LAN Networking

- Ring, Bus, Star, Mesh Topology
- Ethernet - 10Base2, 10Base5, 10Base-T
- Fast Ethernet
- Token Ring
- FDDI

T- Carriers

- Fractional = 1/24th x T1, 1 voice channel, 0.06Mbps
- T1 = 24 voice channels, 1.544Mbps
- T2 = 4 x T1, 96 voice channels, 6.312Mbps
- T3 = 28 x T1, 672 voice channels, 44,736Mbps
- T4 = 168 x T1, 4032 voice channels, 274,760Mbps