CIS 551 / TCOM 401
Computer and Network Security
Spring 2006
Lecture 15
Announcements

• Project 2: Due TODAY

• Midterm II
  – March 21st (One week from today)
  – In class
  – Same format as last time
  – Will cover all material since Midterm I
Recap

• Last time:
  – SSH
  – Human authentication & Passwords
  – Skey authentication

• Today:
  – Ethernet (802.3)
  – Wireless (802.11)
  – TCP/IP
Ethernet (802.3)

- Developed in mid-70’s at Xerox PARC
  - Descendent of Aloha, a U. of Hawaii radio packet network
  - DEC, Intel, and Xerox standard: 1978 for 10Mbps
  - IEEE 802.3 standard grew out of that

- Variants
  - 10Mbps – Multiple Access direct link protocol
  - 100Mbps/1Gbps – designed for point-to-point

- What are these 802.xx things, anyway?
  - IEEE working group number
  - Standardize the protocol
Ethernet Physical links

- Originally used “Thick-net” 10Base5
  - 10 = 10Mbps
  - Base = Baseband (as opposed to Broadband)
  - 5 = maximum of 500 meters segments
  - Up to 4 repeaters between two hosts=2500m max
- 10Base2 “Thin-net”
- More common today: 10BaseT
  - T = Twisted pair (typically Category 5)
  - Much thinner (easier to use)
  - Maximum of 100 meter segments
  - Connected via hubs (still 2500m max)
Ethernet topologies

10Base5 topology

10BaseT topology
Collision Domains

- The Ethernet link is *shared*
- A signal transmitted by one host reaches *all* hosts
- CSMA/CD
  - Carrier Sense, Multiple Access, with Collision Detection
- Hosts competing for the same link are said to be in the same *collision domain*
  - Good news: easy to exchange data
  - Bad news: have to regulate link access
  - MAC: *Media Access Control*
Ethernet Frame Format

- **Preamble** – repeating pattern of 0’s & 1’s
  - Used by receiver to synchronize on signal
- **Dest** and **Src** – Ethernet Addresses
- **Type** – demultiplexing key
  - Identifies higher-level protocol
- **Body** – payload
  - Minimum 46 Bytes
  - Maximum 1500 Bytes
Ethernet Addresses

• Every adapter manufactured has a unique address
  – 6 bytes (48 bits) usually written in Hex.
  – Examples: 00-40-50-B1-39-69 and 8:0:2b:e4:b1:2
  – Each manufacturer is assigned 24bit prefix
  – Manufacturer ensures unique suffixes

• First bit = 0 indicates unicast address
• First bit = 1 indicates multicast address
• All bits = 1 indicates a broadcast address
An Ethernet Adapter Receives:

- Frames addressed to its own address
- Frames addressed to the broadcast address
- Frames sent to a multicast address
  - If it has been programmed to listen to that address
- All frames
  - If the adapter has been put into promiscuous mode
Ethernet Transmitter Algorithm

• If the link is idle transmit the frame immediately
  – Upper bound on frame size means adapter can’t hog the link

• If the link is busy
  – Wait for the line to go idle
  – Wait for 9.6µs after end of last frame (sentinel)
  – Transmit the frame

• Two (or more) frames may collide
  – Simultaneously sent frames interfere
Collision Detection

- When an adapter detects a collision
  - Immediately sends 32 bit *jamming signal*
  - Stops transmitting

- A 10MBps adapter may need to send 512 bits in order to detect a collision
  - Why?
  - 2500m + 4 repeaters gives RTT of 51.2μs
  - 51.2μs at 10Mbps = 512 bits
  - Fortunately, minimum frame (excluding preamble) is 512 bits = 46 bytes data + 14 bytes header + 4 bytes CRC
Ethernet Collision (Worst Case)

T=0

25.6μs

25.6μs

51.2μs
Exponential Backoff

- After it detects 1\textsuperscript{st} collision
  - Adapter waits either 0 or 51.2\,\mu s before retrying
  - Selected randomly
- After 2\textsuperscript{nd} failed transmission attempt
  - Adapter randomly waits 0, 51.2, 102.4, or 153.6\,\mu s
- After n\textsuperscript{th} failed transmission attempt
  - Pick k in 0 \ldots 2^n-1
  - Wait k \times 51.2\,\mu s
  - Give up after 16 retries (but cap n at 10)
Ethernet Security Issues

• Promiscuous mode
  – *Packet sniffer* detects all Ethernet frames

• Less of a problem in *switched* Ethernet
  – Why?
Wireless (802.11)

- Spread spectrum radio
  - 2.4GHz frequency band
- Bandwidth ranges 1, 2, 5.5, 11, 22, ... Mbps

- Like Ethernet, 802.11 has shared medium
  - Need MAC (uses exponential backoff)
- Unlike Ethernet, in 802.11
  - No support for collision detection
  - Not all senders and receivers are directly connected
A and C are hidden with respect to each other

- Frames sent from A to B and C to B simultaneously may collide, but A and C can’t detect the collision.
Exposed nodes

- B is exposed to C
  - Suppose B is sending to A
  - C should still be allowed to transmit to D
  - Even though C—B transmission would collide
  - (Note A to B transmission would cause collision)
Multiple Access Collision Avoidance

- Sender transmits Request To Send (RTS)
  - Includes length of data to be transmitted
  - Timeout leads to exponential backoff (like Ethernet)
- Receiver replies with Clear To Send (CTS)
  - Echoes the length field
- Receiver sends ACK of frame to sender
- Any node that sees CTS cannot transmit for durations specified by length
- Any node that sees RTS but not CTS is not close enough to the receiver to interfere
  - It’s free to transmit
Wireless Access Points

- Distribution System – wired network infrastructure
- Access points – stationary wireless device
- Roaming wireless
Selecting an Access Point

• **Active scanning**
  – Node sends a Probe frame
  – All AP’s within reach reply with a Probe Response frame
  – Node selects an AP and sends Association Request frame
  – AP replies with Association Response frame

• **Passive scanning**
  – AP periodically broadcasts Beacon frame
  – Node sends Association Request
Node Mobility

- B moves from AP1 to AP2
- B sends Probes, eventually prefers AP2 to AP1
- Sends Association Request
802.11 Security Issues

• Packet Sniffing is worse
  – No physical connection needed
  – Long range (6 blocks)
  – Current encryption standards (WEP, WEP2) not that good

• Denial of service
  – Association (and Disassociation) Requests are not authenticated
Wired Equivalent Privacy (WEP)

- Designed to provide same security standards as wired LANs (like Ethernet)
  - WEP uses 40 bit keys
  - WEP2 uses 128 bit keys
- Uses shared key authentication
  - Key is configured manually at the access point
  - Key is configured manually at the wireless device

- WEP frame transmission format:
  \[ 802.11\text{Hdr, IV, } K_{S+IV}\{\text{DATA, ICV}\} \]
  - S = shared key
  - IV = 24 bit "initialization vector"
  - ICV = "integrity checksum" uses the CRC checksum algorithm
  - Encryption algorithm is RC4
Problem with WEP

- RC4 generates a keystream
  - Shared key S plus IV generates a long sequence of pseudorandom bytes $\text{RC4}(\text{IV}, S)$
  - Encryption is: $C = P \oplus \text{RC4}(\text{IV}, S)$  "xor"

- IV's are public -- so it's easy to detect their reuse

- Problem: if IV ever repeats, then we have
  - $C_1 = P_1 \oplus \text{RC4}(\text{IV}, S)$
  - $C_2 = P_2 \oplus \text{RC4}(\text{IV}, S)$
  - So $C_1 \oplus C_2 = P_1 \oplus P_2$
  - Statistical analysis or known plaintext can disentangle $P_1$ and $P_2$
Finding IV Collisions

• How IV is picked is not specified in the standard:
  – Standard "recommends" (but does not require) that IV be changed for every packet
  – Some vendors initialize to 0 on reset and then increment
  – Some vendors generate IV randomly per packet

• Very active links send ~1000 packets/sec
  – Exhaust 24 bit keyspace in < 1/2 day

• If IV is chosen randomly, probability is > 50% that there will be a collision after only 4823 packets
Other WEP problems

• Replay attacks
  – Standard requires the protocol to be stateless
  – Not possible to rule out replay attacks. (The sender and receiver can't keep track of expected sequence numbers)

• Integrity violations
  – Attacker can inject or corrupt WEP encrypted packets
  – CRC (Cyclic Redundancy Check) is an error detection code commonly used in internet protocols
  – CRC is good at detecting random errors (introduced by environmental noise)
  – But, CRC is not a hash function -- it is easy to find collisions
  – Attacker can arbitrarily pass off bogus WEP packets as legitimate ones