ECE 435 – Network Engineering
Lecture 25

Vince Weaver

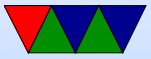
https://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

18 April 2024

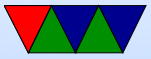
Announcements

- Don't forget projects next week
  Sent out a tentative schedule
- Final project writeup due by May 3rd (last day of classes)
- HW#8 grades were sent out, HW#9 almost done
- Don't forget HW#10 due
- Final is Tuesday April 30th 1:30pm, here (see next slide)



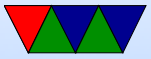
Final Exam Preview

- Final on Tuesday April 30th at 1:30pm, here
- Can have one single-side 8.5x11" piece of paper for notes
- Cumulative, but focusing on things after the first midterm
- Know the 7 OSI layers
- Physical layer: know things like the tradeoffs fiber/copper, satellite, fiber
- Link Layer: Ethernet (why it won over token ring), how collision detection works. Wireless ethernet, how



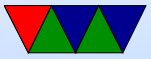
collision detection works.

- IPv4 – addresses. traceroute output
- IPv6 – addresses, why necessary
- TCP/UDP – why use one over the other, three-way handshake
- Probably no socket programming
- Might show packet dumps, not expect you to memorize all the offsets



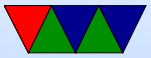
HW#9 Review – Ethernet Frame

- Ethernet header: MAC/MAC/IPv4
  - MAC addresses dest/src. 00:11:22:33:44:55 (they don't look like IP addresses)
  - Note not size, as it's 2048 and size must be smaller than 1500
    0x800 means IPv4
- OUI: Speed Dragon – cheap 2nd ethernet card in my gateway / Pi Foundation
- MAC address is that of router



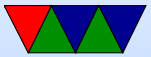
HW#9 Review – ARP

- ARP / maps IP addresses (or other) to MAC.
- Given IP, what's MAC. Not MAC, what's IP (that's reverse-ARP and rarely needed)
- Note ARP is ipv4 only, use neighbor discovery protocol for IPv6



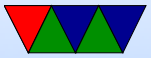
HW#9 Review – Ethernet

- Ethernet was simpler and cheaper than token ring
  - efficient? You'll have to explain that
  - Twisted pair? While twisted pair is cheaper, ethernet was co-ax at the time (and even token ring got twisted-pair eventually)
  - Aside on simplicity, the horrors of NE2000 cards, Donald Becker's rants
- 64 bytes ensured a collision could happen
- Maximum size of 1500 was due to cost of RAM, but also



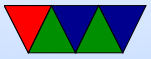
the larger it is the more likely an error can happen

- Ethernet drops things on floor if error



HW#9 Review – Investigation

- Collision count low? Most likely you're connected to a switch (full duplex) so there aren't any collisions.
  - Low traffic or low packet size could also help, but that wasn't necessarily the case here
  - Running in a VM can also have no collisions as in theory your OS is faking up an ethernet card
- Way to tell if switch is notice full-duplex. In theory gigabit usually (but not always) will imply a switch as well

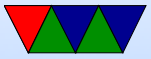


Network Security

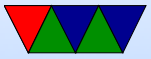
As described by Tannenbaum

- Secrecy – keeping private data from others
- Authentication – being sure person is who they claim
- Nonrepudiation – signed documents, how do you prove a document is an original
- Integrity control – make sure document sent is the one that was received, unmodified

Possibly also include code mistakes/exploits.

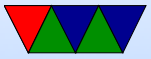


Network Security: Which Layer?



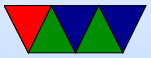
Physical Layer Security – Air Gapping

- Just don't use network
- Move files via USB? Can that have security issues? Stuxnet?
- Separate networks for sensitive info. What is secret?
  - Classified info
  - Credit card info
  - Secret signing keys

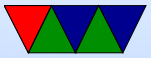


Physical Layer Security – TEMPEST

- Telling what computers are doing based on radiated signals
- Tell what machines are doing by radio interference
- Old CRT monitors could tell by RF, also if have view of room by brightness as screen scanned
- Interference in nearby cables, ground, parallel lines
- Blinking lights on routers
- Lasers bouncing off windows
- Soviet gift of US seal with hidden chambers that would

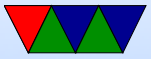


vibrate when people talk, modify a microwave signal shot through the room



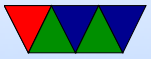
Physical Layer Security – Side Channel Leaks

- Intentionally leaking info via side channel
  - What if paranoid and they epoxied the USB ports shut
  - Keyboard light
  - QR-codes on screen
  - Varying fan speed
  - Sound (ultrasound?)



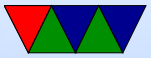
Physical Layer Security – Other

- Using fiber – harder to tap than wired
- Don't use wifi
- Locking wiring closets
- Pressurizing cable lines (notice if someone drills in to tap)
- No cell phones/recording devices in secure areas
  Cell-phone garage
- Evil USB chargers
- CANBUS in cars



Link Layer – Wired

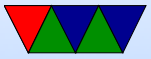
- Switches vs Hubs
  - The move to switches massively increased security on ethernet networks
- Frames can be encrypted
- Usually have to be at least partially decrypted (to expose routing info) to get the next layer
- Attacks
  - ARP spoofing / Port Stealing
  - CAM attacks – overflow the address mapping tables



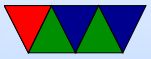
If switch doesn't have room to hold all addresses, falls back to broadcasting the packets and then everyone can see them

- DoS – ARP spoofing, convince switch that the MAC address for actual machine is a non-existent
- DHCP exhaustion
- Spanning Tree Attacks – convince network wrong switch is the root
- VLAN attacks – escape VLAN by messing with headers

- Methods
  - Lock down ports so can't be changed by ARP

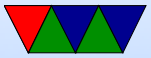


- Switch can notice unknown MAC addresses and not allow connection, or ban port



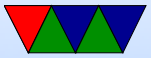
Link Layer Security – Wireless

- Wireless: hidden node, deauth attack
- Eavesdropping
- Masquerading (pretending to be another)
- Traffic Analysis
- Jamming
- Ways to lock things down
  - Encryption
  - Forcing registration/authentication before allowing on network



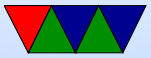
Link Layer – POTS Phone Phreaking

- 2600 Hz, Captain Crunch
  - 2600 Hz tone would cause connection to disconnect, but you could send combinations of tones to re-route
- Blue boxes
- Steve Wozniak



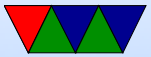
Link Layer – Cellphones

- Stealing phones
- Sim / esim/ isim
- Password reset/guessing
- More Paranoid
  - Tracking
  - Firmware hacked to enable MIC even though phone off
  - Removing battery/Faraday cage shielding?

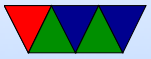


Network Layer Security

- IP security (IPSEC) (RFC 2401, 2402, 2403)
  - Add authentication/encryption at the IP level via extra headers
  - authentication header
  - HAC (hashed message authentication code), mostly made irrelevant by ESP
  - ESP (encapsulating security protocol)
  - Commonly used for site-to-site VPN
- Firewall

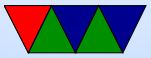


- VPN
- Attacks
  - BGP blackhole
  - Exploits of unpatched router vulnerabilities



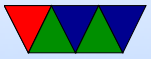
Transport Layer Security

- Encryption, like SSL and ssh
- Attacks
  - See summary later

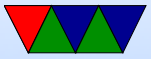


Application Layer Security

- This is where authentication, signing, etc. happens

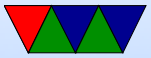


Types of Attacks

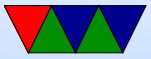


Social Engineering

- People like being helpful
- “Not my Problem”
- Can defeat many of these at all layers
- Physical access
  - Tailgating into businesses
  - Show up with hardhat / high-vis vest
  - Dress like a UPS delivery person with package
- Telephone
  - Call and claim boss demands something

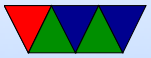


Depending on culture people not want to annoy boss
  - Public directories of company employees and position, can make it sound like you know people
- e-mail
  - Fake invoices
  - Impersonate boss
- Backdoors

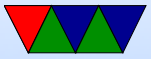


Network Attacks

- DoS – somehow manage to make a service unusable (often by overwhelming network and/or crashing machine)
  - botnets
  - DDoS – distributed, large number of machines contributing
  - smurf attack – send forged ICMP packet with faked source to broadcast address, all on network will reply to the forged IP

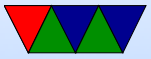


- fraggle attack – like smurf but chargen or echo ports used instead
- Syn Floods/ping flood
- ping of death
- nuke attack – send out-of-band data (with URG set?) to netbios port on windows machine, crash it
- HTTP POST attacks – make valid http post request but only very slowly send data, tying up the server
- IP fragmentation
  too small or too large (confuse router)
  fragment overlap (teardrop), send overlapping



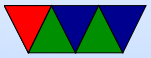
fragments, can confuse OS or allow constructing final packets that bypass firewall checks

- Amplification attacks
- backscatter – due to spoofed addresses, can get reflections from attack in progress elsewhere



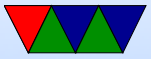
Vulnerabilities

- Buffer overflows
- Untrusted/Unsanitized input
- Backdoors



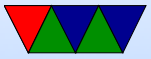
Other Issues

- cross-site scripting/XSS
- Malware
- Virus / Worms (morris worm) / Trojan
- Phishing
- MiTM
- Ransomware
- Fuzzing



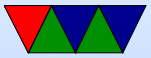
Fuzzing

- Searching for issues by sending random (or almost random) inputs and see what happens



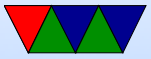
Mitigations

- blackholing/sinkholing. Send all traffic to non-existent server
- firewalls



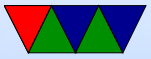
VPN/Tunnel

- Create a tunnel, TCP/IP inside of TCP/IP directly from your machine into remote network (past firewall) or network-network.
- Link layer tunnel – all Ethernet packets go through as if were local
- IPSEC – IP level tunnel, IP in certain range (or all) go through the secure IP tunnel to other side

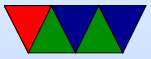


Firewalls

- Runs on machine, intercepts all incoming packets before allowing them through.
- packet-filter based – looks at layer3/layer4
  fast because addr/port fixed locations
- application-gateway – looks into protocol
  may be a proxy server (so can do things like filter http requests to certain websites)
- Organization – firewall to outside, extra DMZ layer where any servers might be, then an additional more

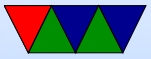


restrictive firewall to internal network. why? if servers compromised don't want free reign over rest of network.

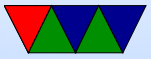


Firewalls

- 1st generation – packet filtering. Check for port number or IP destination and drop if not OK
- 2nd generation – stateful firewall. Keep a packet history so it can make decisions based on state of connection (new connection, existing connection, etc)
- 3rd generation – application level. Can understand protocols like ftp, http, etc, and make decisions
- Deep packet inspection – can be used to block viruses and such, but also censorship

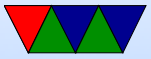


- eBPF
- DMZ



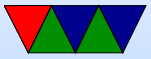
iptables

- Linux changes up firewall interface all the time
- ipfwadm (linux 1.2 - 2.2)
- ipchains (linux 2.2 - 2.4) stateless
- netfilter/iptables (2.4) – stateful firewall
  can filter on lots of things. BPF filters
  NAT is done via this
  port forwarding
  had 4 separate engines (ipv4, ipv6, ethernet, arp)
- nftables (linux 3.13) – merges things, virtual machine



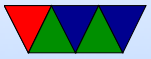
(but not BPF) to speed things up

- Separate ip6tables utility for setting IPv6 rules
- Also arptables/ebtables for filtering ethernet



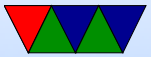
iptables example

```
# Flush all rules

iptables -F
iptables -t nat -F
iptables -t mangle -F

iptables -A FORWARD -i eth1 -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -A PREROUTING -p tcp -i eth1 --dport 2131 -j DNAT --to-destination 1
iptables -A FORWARD -p tcp -d 192.168.8.18 --dport 22 -m state --state NEW,ESTABLISH
```



ssh security

- Fail2ban
- Nonstandard port
- Port knocking
- Call asterisk for one-time pin?
- No-password (key only)
- LCD device



encryption problems

- Keys leaked (DVD/game console issues)
- poor random numbers used (Debian problem)
- differential cryptanalysis (start with similar plaintexts and see what patterns occur in output) [DES IBM/NSA story]
- Power/Timing analysis – note power usage or timing/cache/cycles when encryption going on, can leak info on key or algorithm