ECE 435 – Network Engineering
Lecture 22

Vince Weaver

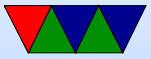
http://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

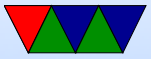
22 April 2021

Announcements

- HW#10 posted
- HW#9 graded
- Attend the new faculty interview talks if you can
- Don't forget projects next week
- Final is Tuesday May 4th 8am, online only
- Rant about IEEESSP ethics / U of Minnesota getting

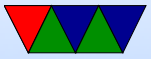


banned from Linux devel

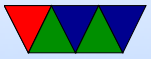


HW#9 Review

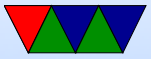
- Ethernet header: MAC/MAC/IPv4
  MAC addresses are 00:11:22:33:44:55 (they don't look like IP addresses)
  Note not size, as it's 2048 and size must be smaller than 1500
  0x800 means IPv4
- Speed Dragon – macbookair with USB-ethernet / Pi Foundation
- MAC address is that of router



- 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)
- Collision count low? Most likely you're connected to a switch so there aren't any collisions. Full duplex I guess is equivalent. Also i running in VM
- Questions
  - Ethernet was cheaper
  - 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

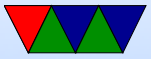


- Ethernet drops things on floor if error

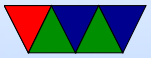


Final Exam Preview

- Final on Tuesday the 4th at 8am, remote
- 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

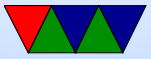


Network Security

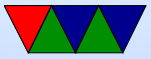
As described by Tannenbaum

- 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.

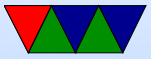


Network Security: Which Layer?



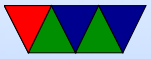
Physical Layer Security

- Air-gap
- Using fiber
- Locking wiring closets
- Pressurizing cable lines (notice if someone drills in to tap)
- TEMPEST
- No cell phones/recording devices in secure areas



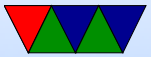
Link Layer Security

- Switches vs Hubs
- Frames can be encrypted
- Usually have to be at least partially decrypted (to expose routing info) to get the next layer
  - CAM attacks – overflow the address mapping tables
  - ARP spoofing
  - DHCP exhaustion
  - Wireless: hidden node, deauth attack

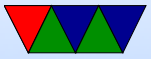


Network Layer Security

- 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

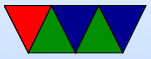


- VPN
- Attacks
  - BGP blackhole



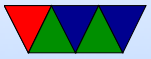
Transport Layer Security

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



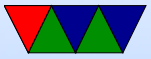
Application Layer Security

- This is where authentication, signing, etc. happens



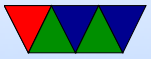
Challenges

- Social Engineering



Network Attacks

- DoS – somehow manage to make a service unusable (often by overwhelming network and/or crashing machine)
  - 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

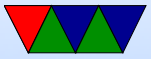


used instead

- 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

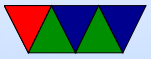


packets that bypass firewall checks

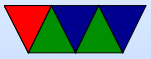
- Amplification
- Mitigations – blackholing/sinkholing. Send all traffic to non-existent server
  firewalls

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

- botnets
- cross-site scripting
- Virus / Worms (morris worm) / Trojan/ Backdoor / Bot

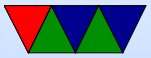


- Phishing
- MiTM
- Ransomware



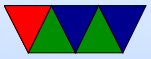
VPN/Tunnel

- 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

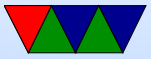


Firewalls

- 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

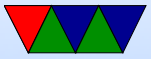


where any servers might be, then an additional more restrictive firewall to internal network. why? if servers compromised don't want free reign over rest of network.

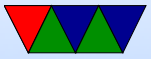


Firewalls

- 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

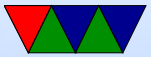


- eBPF
- DMZ



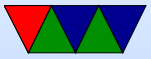
iptables

- 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
```