ECE 435 – Network Engineering
Lecture 23

Vince Weaver

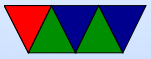
http://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

30 November 2016

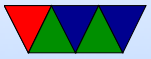
Announcements

- HW#9 was due
- HW#10 will be posted
- Don't forget projects next week



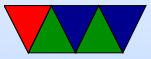
Last Time Questions

- Is RSA symmetric?
- How does git authenticate?

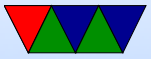


Security

- Physical layer security
- Link-level encryption?
- Application Level?
- Result was 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

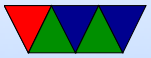


- ESP (encapsulating security protocol)
- Commonly used for site-to-site VPN



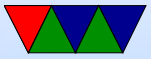
VPN/Tunnel

- 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

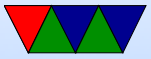


Firewalls

- 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

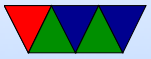


where any servers might be, then an additional more restrictive firewall to internal network. why? if servers compromised don't want free reign over rest of network.

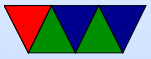


Firewalls

- 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

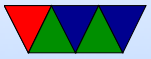


- eBPF



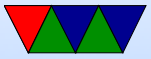
iptables

- 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



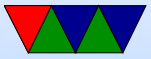
(but not BPF) to speed things up

- Maybe include iptables example from jaguar?



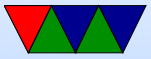
iptables example

```
# 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
```



Security Issues

- 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

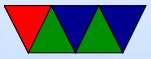


used instead

- 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

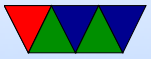


packets that bypass firewall checks

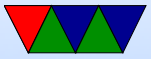
- Amplification
- Mitigations – blackholing/sinkholing. Send all traffic to non-existent server
  firewalls

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

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

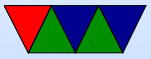


- MiTM
- Ransomware



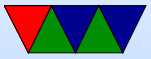
Video Games

cheating, lag, trust client or server, interpolating



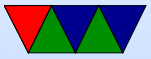
HW#9 Review

- e-mail
  - pop from deater.net via fetchmail
  - LMTP – local mail transport. LHLO. No mail queue, says right away whether deliver mail is possible.
  - encrypted from UFL, but from videotron.ca cablemodem
  - Virus scanned and SPAM scanned
  - pdf attached probably had some sort of exploit
- browser



- Error 404 – not found
- Error 418 – RFC 2324 coffeee protocol (I'm a teapot)
- Error 451 – Unavailable For Legal Reasons / Ray Bradbury

- http header
  - Apache 2.2.2
  - "w3 total cache" – wordpress accelerator? (wordpress is a PHP/mysql content management system)
  - X-pingback – enable pingbacks when linked by wordpress



- Can you connect with telnet? No, way more complex, even discounting encryption