

Local Area Networks

LAN Security and local attacks

Overview

- Local network attacks target an internal network
- Some attacks can be launched remotely
- Few ops monitor or guard against local attacks
- Ultimately everything is a physical security problem

Traffic Eavesdropping

- Easy on shared media LANs
- Still possible on switched LANs
 - e.g. flood or trick the bridge address table
- Easy on wireless LANs
- Possible to install physical splitter/tap/hub/bridge
 - Would you see a physical something?
 - Does the link bounce? Would you notice that?

LAN Bridge/Switch Attacks

- Overflow MAC address tables to cause flooding
 - Typical gear can hold a few thousand addresses
 - MAC addresses = 48 bits or >> a few thousand
- Spoof spanning tree BPDU messages
 - Take over as root/designated bridge
 - Cause continuous topology recomputations
- Forge VLAN, priority or aggregation tags
- Spoof PAUSE (flow control) frames (gig only)
- DDoS/floods, broadcast storms

Preventing LAN Bridge Attacks

- Monitor MAC address tables
- Manually set root bridge and monitor
- Use knobs like Cisco's BPDU and Root Guard
- Manually set and prune trunked switch ports
- Use 802.1x port authentication

ARP-based Attacks

- ARP request spoofing
 - Responders to a request cache the sender's info
 - As do others who already have the sender's info
- ARP update spoofing (gratuitous ARP)
- Thinking out loud:
 - Is UNARP widely used? No.
 - Can we poison ARP entries to = group address?

Preventing ARP-based Attacks

- Use LAN switches with one port per end host
- Enable port security to limit source MAC addresses
- Use 802.1x port authentication
- Enable (get) knobs on end hosts to validate ARPs
 - How to best do this?
- Monitor LAN bridge/switch address tables
- Monitor router ARP tables
- Keep history of address/ARP tables
- FYI... vendors must support knobs (at line rate)

Routing Attacks

- Route injection
- Route monitoring
- Route redirection
- Route process DDoS attack
- Note, other types of local attacks may target routers

Preventing Routing Attacks

- Strongly authenticate all routing updates/packets
- Listen/send routing packets where there are routers
- Protect processes and access (ports, IPs, physical)
- Monitor routing
 - Table size (especially changes over time)
 - Checksum values and LSA counts in OSPF
 - Flaps, deaggregation, traffic patterns
- Build baseline network map (ala Ches's netmapper)

DHCP Attacks

- Spoof DHCP requests
- Spoof DHCP replies (or be a rogue DHCP server)
- Thinking out loud:
 - Can we spoof DHCP releases?

Preventing DHCP Attacks

- Monitor DHCP discover/lease activity
- Monitor DHCP discovers, requests and offers
 - Clients broadcast request, contains server IP
 - Can monitor DHCP packets and contents at:
 - DHCP servers
 - Router edges
- Use intra-VLAN knobs (e.g. Cisco's intra-VACL)
- Use anti-spoofing knobs (e.g. Cisco's DHCP Snooping and IP Source Guard)

Multicast Attacks

- Spoof IGMP querier function (does this do much?)
- Spoof IGMP reports (joins)
 - There are 224.0.0.0/4 IP multicast groups
- Spoof or simply generate group traffic
- Thinking out loud:
 - How to better authenticate group participation?
 - Will we see intentional multicast based attacks?

Preventing Multicast Attacks

- Monitor IGMP querier on router edges
- Monitor IP multicast group usage on edges
- Monitor IP multicasted routing state changes
- Heavily filter IP multicast group state, allow just:
 - 224.0.0.0/8
 - 225.0.0.0/8
 - 239.192.0.0/14 (internal only if used)
 - 233.xx.yy.0/8 (GLOP space)
 - Then filter out bogus groups in above ranges

Other Attacks

- HSRP/VRRP - use MD5 auth and/or IPSEC
- Wireless
 - DDoS protection and auth mechanisms needed!
- ICMP redirect, source quench, router advertisement
 - These are easily fixed
- Time sync - who is getting time from who?
- DNS spoofing
- IPv6 - potential problems with discovery/autoconf?