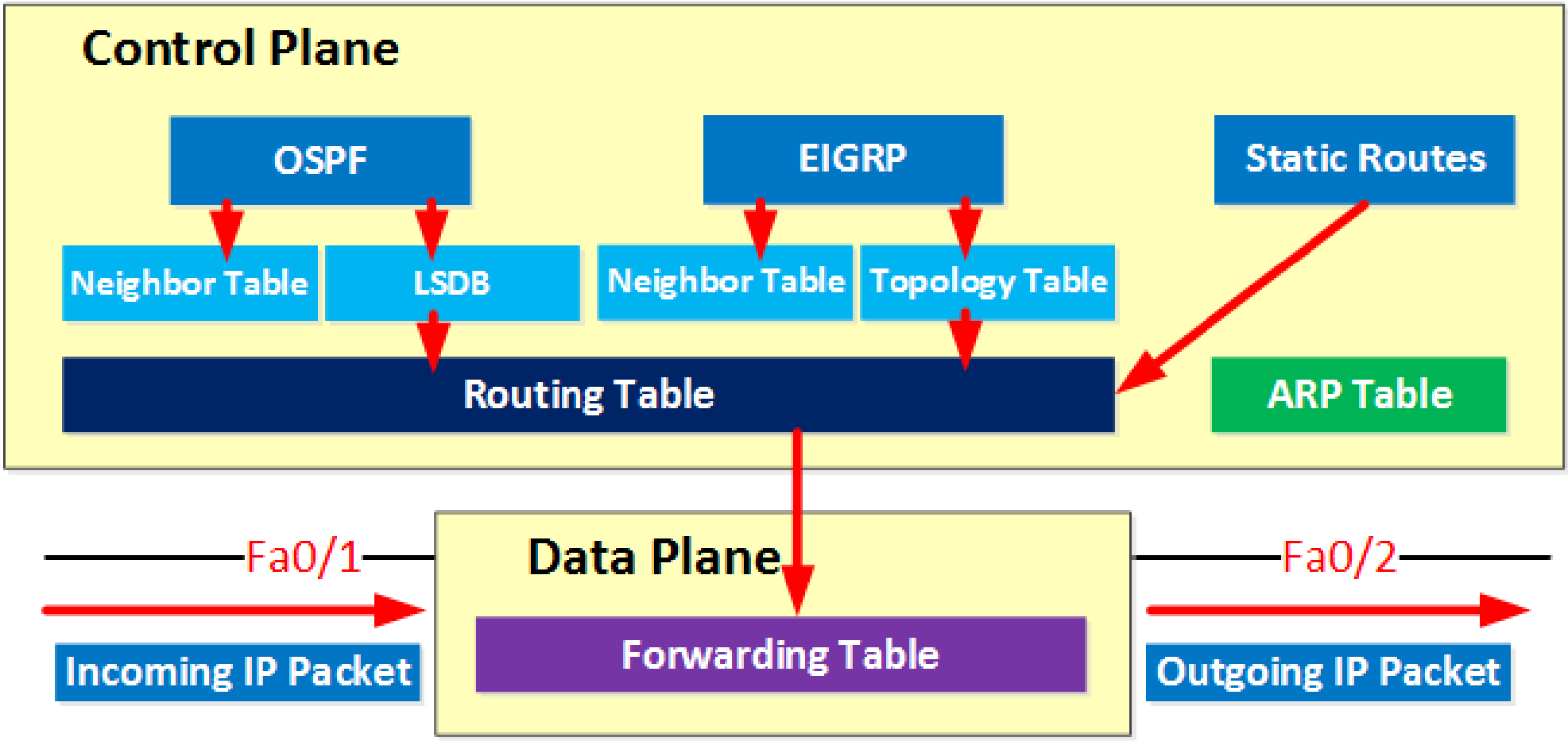
YET ANOTHER DENIAL OF SERVICE VULNERABILITY

Evgeny Uskov

eu@qrator.net

A typical router



Control plane

- Makes decisions about where traffic is sent
- Control plane packets are destined to or locally originated by the router itself
- Control plane packets are processed by the router CPU
- Since the control functions are not performed on each arriving individual packet, they do not have a strict speed constraint and are less time-critical

Data plane

- Also known as Forwarding Plane
- Data plane packets go through the router
- The routers/switches use what the control plane built to dispose of incoming and outgoing frames and packets

Difference

An important difference:

- In data plane packets are handled on hardware level
- In control plane they are processed by the router CPU

Hence, it is usually a **bad** idea to leave control plane open to the Internet

In particular, open TCP port (e.g. BGP) is a vulnerability which can be used for DoS

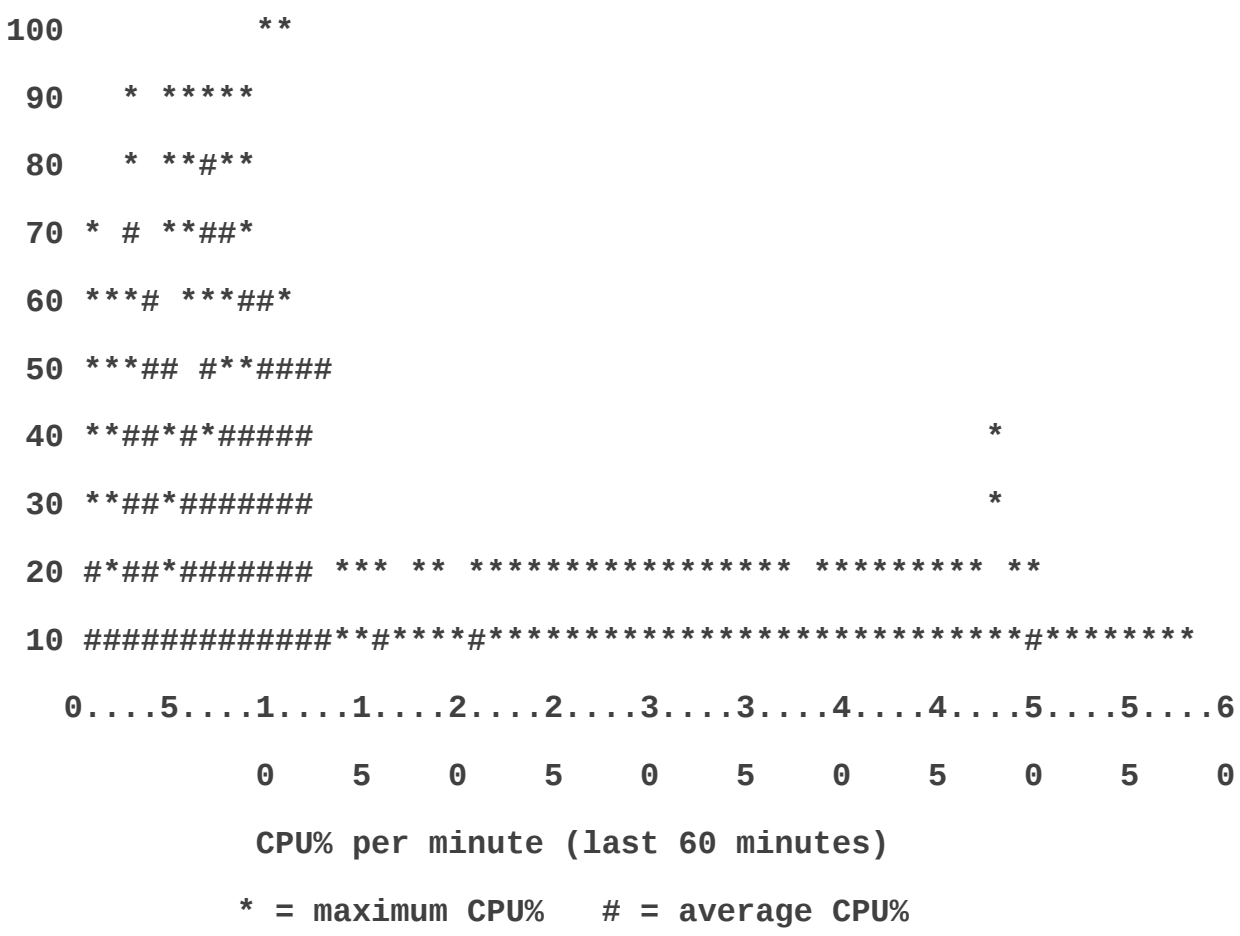
A simple experiment

Victim: Cisco ASR 1002 Router

Attack:

- SYN flood from two machines
- 32 instances of hping --flood on each machine
- about 720 kpps and 0.5 Gbps

A simple experiment: CPU load



A simple experiment: DoS

Apr 27 00:38:27 MSK: %BGP-3-NOTIFICATION: sent to neighbor X.X.X.X 4/0 (hold time expired) 0 bytes

Apr 27 00:38:27 MSK: %BGP-5-NBR_RESET: Neighbor X.X.X.X reset (BGP Notification sent)

Apr 27 00:38:29 MSK: %BGP-5-ADJCHANGE: neighbor X.X.X.X Down BGP Notification sent

Apr 27 00:38:29 MSK: %BGP_SESSION-5-ADJCHANGE: neighbor X.X.X.X IPv4 Unicast topology base removed from session BGP Notification sent

Apr 27 00:38:36 MSK: %BGP-3-NOTIFICATION: sent to neighbor Y:Y:Y:Y:: 4/0 (hold time expired) 0 bytes

Apr 27 00:38:36 MSK: %BGP-5-NBR_RESET: Neighbor Y:Y:Y:Y:: reset (BGP Notification sent)

Apr 27 00:38:37 MSK: %BGP-5-ADJCHANGE: neighbor Y:Y:Y:Y:: Down BGP Notification sent

Apr 27 00:38:37 MSK: %BGP_SESSION-5-ADJCHANGE: neighbor Y:Y:Y:Y:: IPv6 Unicast topology base removed from session BGP Notification sent

Apr 27 00:38:43 MSK: %BGP-5-ADJCHANGE: neighbor X.X.X.X Up

Apr 27 00:38:45 MSK: %BGP-5-ADJCHANGE: neighbor Y:Y:Y:Y:: Up

A simple experiment

Consequences:

- multiple BGP session restarts
- several cases of OSPF reconvergence
- unstable routing table

Evident solution

Do not leave your control plane open to the Internet:

- use ACL
- listen on private addresses

However ...

Common case

Some statistics

Data collecting methodology:

- scan entire IPv4 address space for open BGP ports
- filter hosts that reply with SYN-ACK on all ports
- check that ports behave as BGP (e.g. immediately close the connection)

Some statistics

Hosts with open BGP ports:

- 1230768 unique IPs
- 67841 unique prefixes
- 16450 unique ASes

After establishing the connection:

- 70113 hosts send OPEN message (!)
- 62838 hosts send Notification (connection rejected)
- all other hosts immediately close the connection

Conclusion

There exists a huge number of hosts with open TCP ports that are typically used in control plane

You can check your AS at https://radar.qrator.net

(you need to authorize your AS in order to prevent malicious use of the data)

Please contibute your feedback

(https://radar.qrator.net, Contact Us)