BGP Security

Kevin's Attic for Security Research
kevinkoo001@gmail.com

Table

BGP Operation (1/2)

BGP Concept & Topology

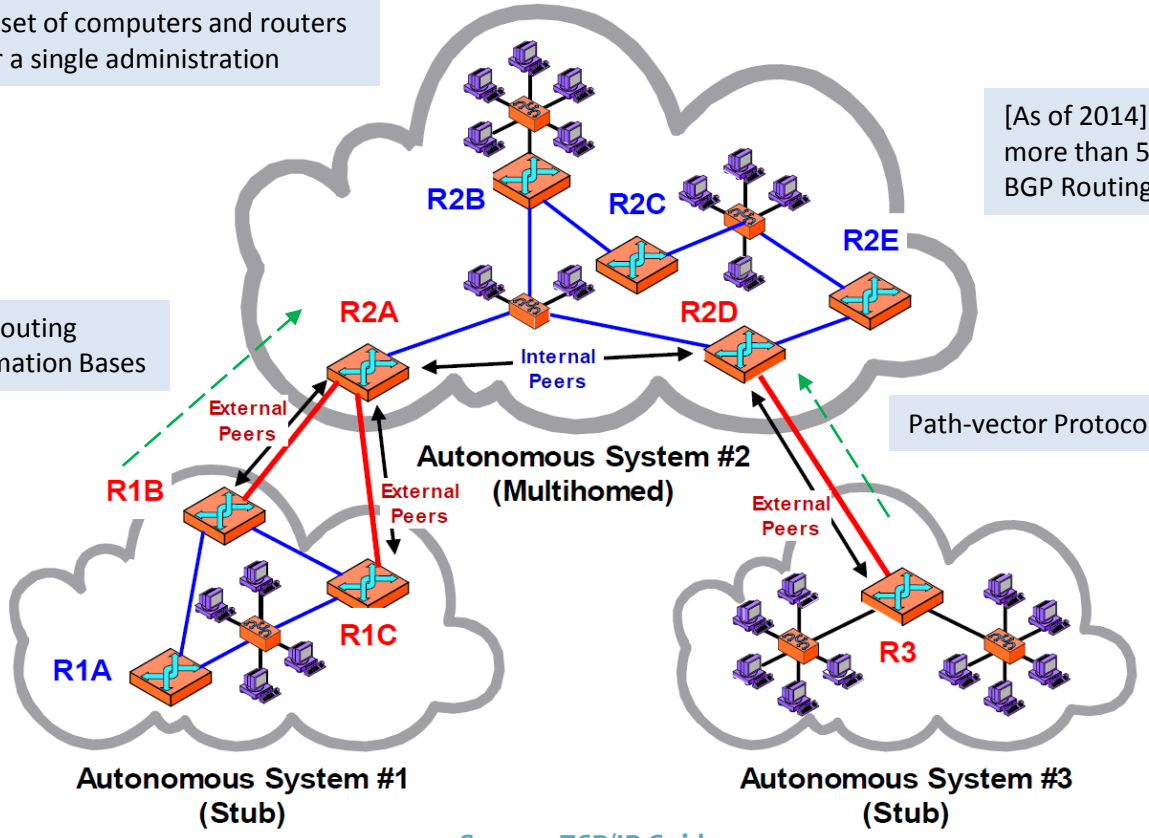
- BGP (Border Gateway Protocol): iBGP(internal peers) and eBGP(external peers) among ASes

AS: A set of computers and routers under a single administration

[As of 2014]
more than 500,000
BGP Routing Tables

RIB: Routing Information Bases

Path-vector Protocol (RFC1322)

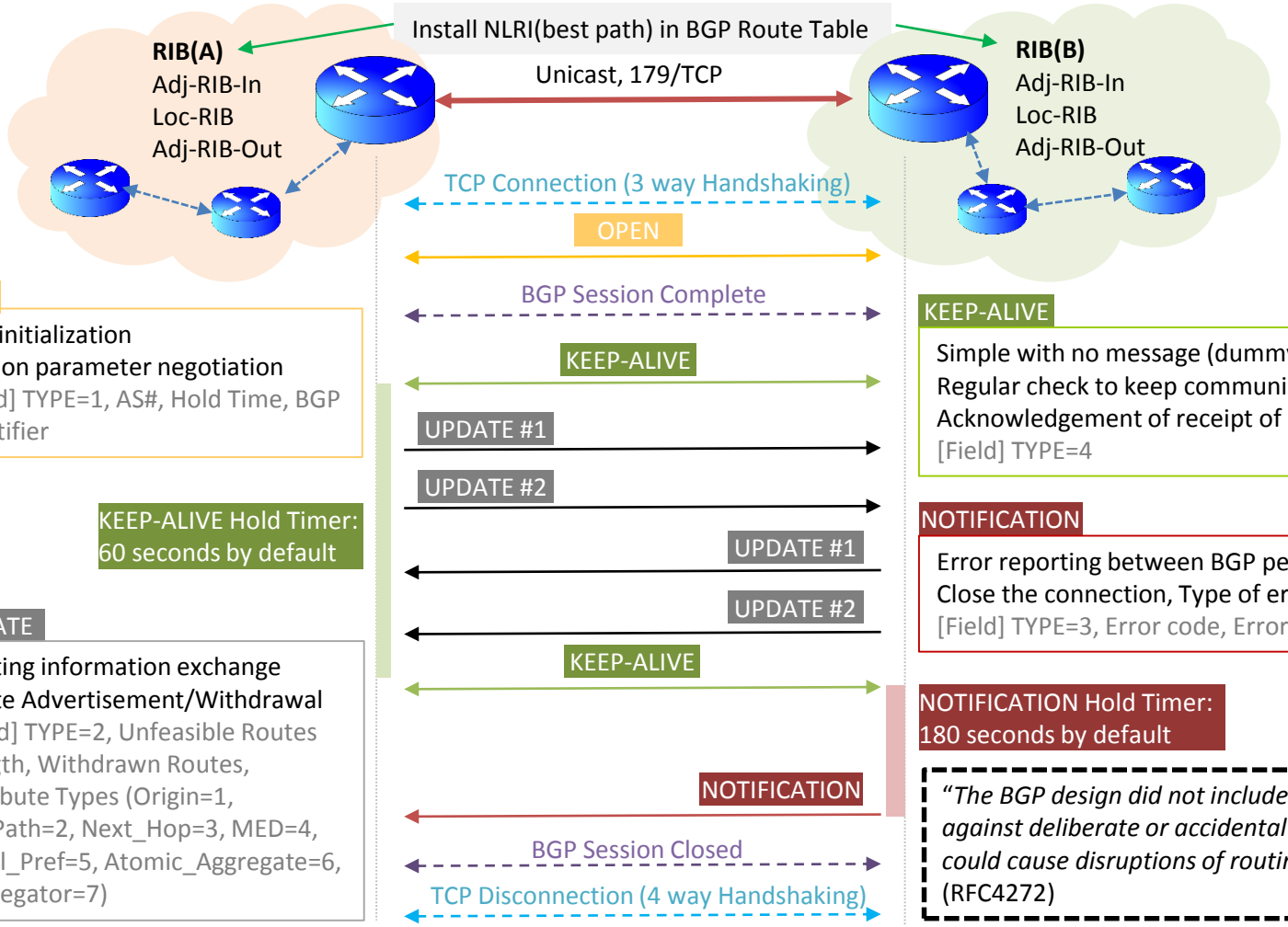


Source: TCP/IP Guide

BGP Operation (2/2)

BGP Message Exchange, Format and Path Vector(Decision) Algorithm

(BGP Attributes for Path Decision) Height weight → Highest LOCAL-PREF → Originated Source → Shortest AS-PATH → Lowest Origin (IBGP < EBGP < incomplete) → Lowest MED → EBGP over IBGP → Lowest IGP Metric → Lowest Route ID → Lowest Originator ID



OPEN

Link initialization
Session parameter negotiation
[Field] TYPE=1, AS#, Hold Time, BGP Identifier

KEEP-ALIVE Hold Timer: 60 seconds by default

UPDATE

Routing information exchange
Route Advertisement/Withdrawal
[Field] TYPE=2, Unfeasible Routes Length, Withdrawn Routes, Attribute Types (Origin=1, AS_Path=2, Next_Hop=3, MED=4, Local_Pref=5, Atomic_Aggregate=6, Aggregator=7)

KEEP-ALIVE

Simple with no message (dummy, size=19)
Regular check to keep communication
Acknowledgement of receipt of a valid *Open*
[Field] TYPE=4

NOTIFICATION

Error reporting between BGP peers
Close the connection, Type of error indication
[Field] TYPE=3, Error code, Error sub-code

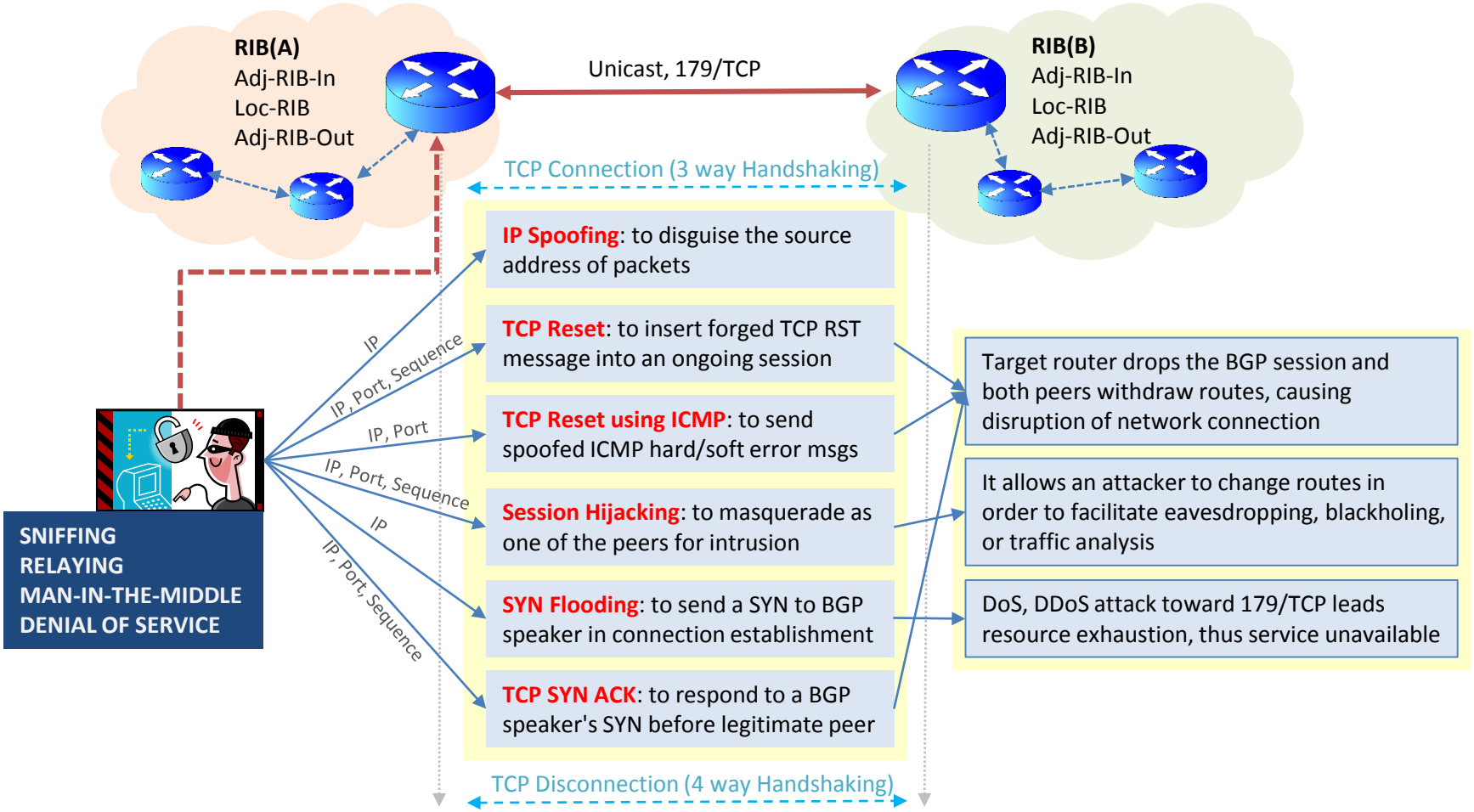
NOTIFICATION Hold Timer: 180 seconds by default

> *"The BGP design did not include protections against deliberate or accidental errors that could cause disruptions of routing behavior."* (RFC4272)

Potential Attacks on BGP (1/2)

BGP Vulnerability Analysis from TCP Perspective

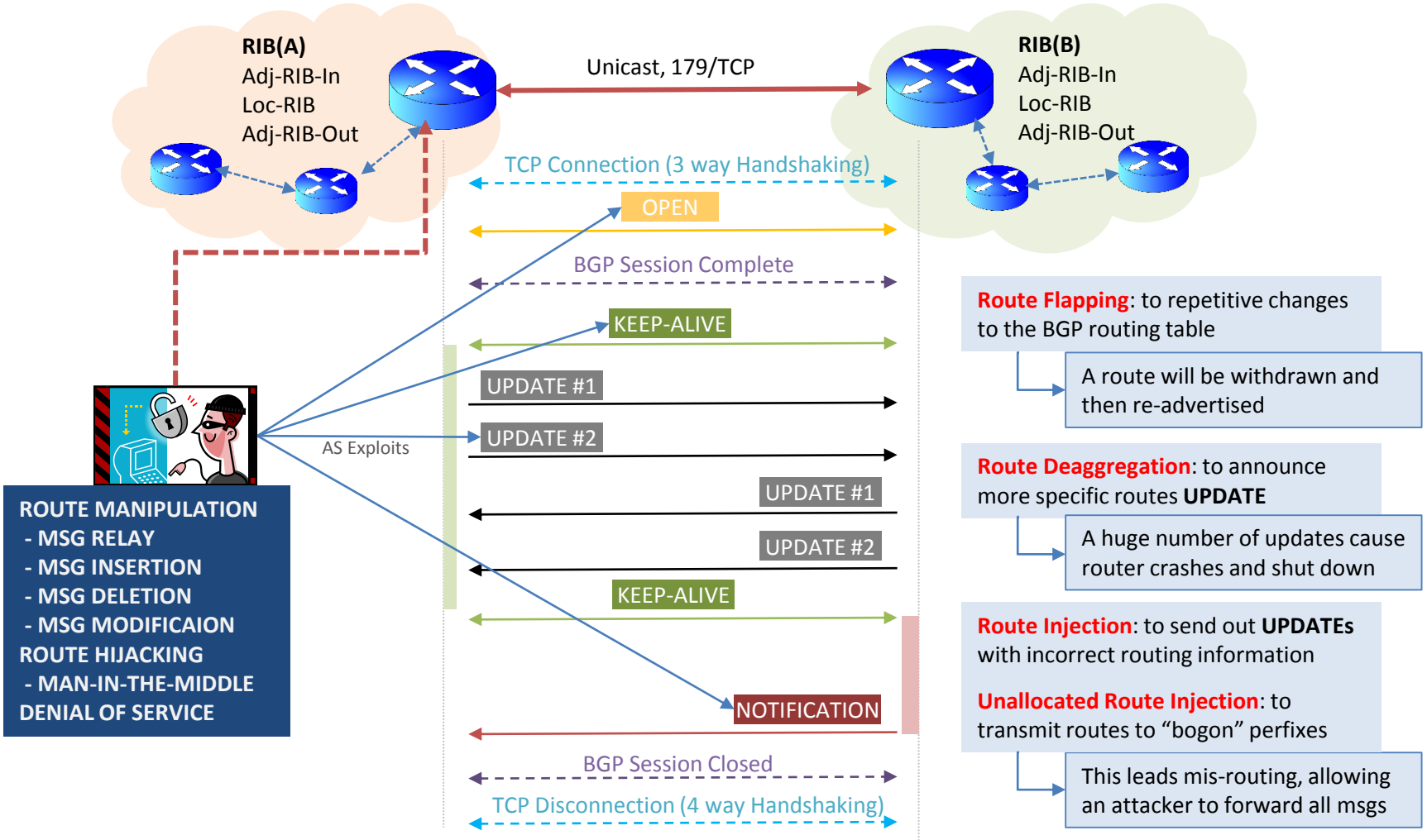
❖ By running over TCP, listening on port 179, BGP is subject to be vulnerable through all kinds of TCP attacks.



Potential Attacks on BGP (2/2)

BGP Vulnerability Analysis from Protocol Perspective

- Fundamental vulnerabilities arise from no mechanism which has specified within BGP in order to (a) validate the authority of an AS and (b) to ensure the authenticity of the path attribute by an AS.



Route Flapping: to repetitive changes to the BGP routing table

- A route will be withdrawn and then re-advertised

Route Deaggregation: to announce more specific routes **UPDATE**

- A huge number of updates cause router crashes and shut down

Route Injection: to send out **UPDATEs** with incorrect routing information

Unallocated Route Injection: to transmit routes to "bogon" perfixes

- This leads mis-routing, allowing an attacker to forward all msgs

BGP Attack Countermeasures

- Use authentication mechanism
  - Use access control list.
  - Use BGP peer authentication: MD5(Routing Advertisement + Shared Key), IPSec if available
  - Configure BGP to allow announcing only designated netblocks
  - Disable BGP version negotiation to provide faster startup
  - Announce only preconfigured list of networks
- Configure route manipulation protection
  - Use BGP graceful restart
  - Use max prefix limits to avoid filling router tables
  - Filter all bogon prefixes with *ingress/egress filtering*
  - Do not allow over-specific prefixes
  - Turn off fast external failover, called route flap damping
  - Record peer changes
- Use secure protocol
  - Only allow peers to connect to port 179 in TCP
  - Randomize sequence number (against spoofing and session hijacking)
  - Consider deploying S-BGP or BGPSec

References

- List of References

- http://www.wired.com/images_blogs/threatlevel/files/nist_on_bgp_security.pdf
- http://www.cidr-report.org/as2.0/
- http://www.tcpipguide.com/free/t_BGPTopologySpeakersBorderRoutersandNeighborRelatio-2.htm
- http://moo.cmcl.cs.cmu.edu/~dwendlan/routing/
- RFC 4271 - A Border Gateway Protocol 4 (BGP-4), which obsoletes RFC 1771, 1772
- RFC 4272 - BGP Security Vulnerabilities Analysis
- RFC 2439 – BGP Route Flap Damping
- http://datatracker.ietf.org/wg/sidr/charter/
- http://www.cisco.com/web/about/security/intelligence/protecting_bgp.html