

How Routing Works?

- Internet is organized into Administrative Systems (AS) for routing purposes
 - Network segments under a single administrative control
- Routing means learning how to get to various destinations
 - Because we have packet-switched network we only need to learn next hop
- Routing protocols used inside AS are OSPF or RIP
- Routing protocol used between AS-es is Border Gateway Protocol (BGP)

"Secure Border Gateway Protocol "S-BGP", S. Kent, C. Lynn, K. Seo, IEEE Journal on Selected Areas in Communications, Vol. 18, No. 4, April 2000, pp. 582-592

1

BGP

- BGP plays crucial role in the Internet
 - If it were attacked Internet would literally grind to a halt
- Unlike OSPF and RIP where route is chosen based on distance, BGP routes are chosen based on both the distance and the policy
 - Since policies are kept private, we cannot infer routing even if we knew physical topology and could gather all the messages exchanged between routers
- BGP routers form *peering relationship* with routers in the neighboring domain
 - TCP connection with periodic *hello* messages
- They exchange *BGP updates* to build routing tables

2

BGP Update

- Contains
 - List of prefixes that are not reachable anymore
 - List of prefixes that are reachable
 - AS_PATH, list of AS-es to cross to reach those prefixes
- One router can advertise different information to different peers
- BGP router keeps all advertised routes from its neighbors, it chooses subset of these for itself, and another (same or different) subset to advertise
- Backbone routers know how to reach any address on the Internet

3

Route Changes

- There are no periodic updates sent
 - Update is sent only when a change occurs
 - When a BGP router reboots it receives all the information from its neighbors' tables
- Since updates propagate through the Internet, there is generally a lot of BGP traffic
 - 50% of update traffic is for transient changes – route "flaps" – when the old route is restored after a short period

4

BGP Security

- Security of BGP is defined through correct operation:
 - Each update is authentic, contains recent information and has not been modified
 - Update was sent by an authorized speaker for a given AS
 - First AS in the path (closest to the destination prefixes) was authorized by their owners to advertise them
 - If the update advertises withdrawn prefixes, they were previously advertised as reachable by the same peer
 - Both sending and receiving BGP router correctly apply their policies

5

Threat Model: What Can Go Wrong

- Someone can hijack TCP connection between peers
- Someone can modify updates, delay them, replay them or suppress them
- Someone can subvert a BGP router
 - And then generate false advertisements, spoofing the prefixes it cannot reach
 - Or misconfigure the router
 - Or generate too frequent updates
 - Or generate updates that do not conform to local policies

6

S-BGP

- Handles all threats except those that pertain to correct policy implementation
- Aims to be scalable and deployable solution
 - There is a careful analysis of expected performance
- Works under partial deployment
 - S-BGP information looks to legacy routers as extra information they do not understand
 - Legacy routers just process updates as they ordinarily would and send them further

7

S-BGP

- Uses two public key infrastructures (PKI) to generate keys for signing updates
 - Address Allocation PKI – whoever gave you the address range is responsible to sign a certificate verifying that you own this address range – this gives a router one public/private key K1
 - Administrative System PKI – certifies ability to be a BGP speaker for given AS – this gives a router another public/private key K2
- Uses *attestations* to establish that an AS is authorized to advertise a path to an address space
 - Address attestation for the origin AS – signed by K1
 - Route attestations for transit AS-es – signed by K2

8

S-BGP Update

- Contains
 - Route attestation for each router on the path – signs the AS_PATH info with K2
- Necessary for verification but distributed offline
 - Address attestation for each advertised prefix – gives the origin AS right to advertise, signed with K1
 - Address certificate for each advertised prefix – confirms that this is not a “made up” prefix but that each organization owns this prefix, verifying K1
 - Certificate for each router on the path – verifies K2
- S-BGP uses IPsec between peers to prevent replays

9

How Does S-BGP Help

- Certificates enable verification of:
 - AS is authorized to advertise a block of addresses
 - Organization owns given AS number
 - BGP router is associated with given AS
- Address attestation protects from advertising fake prefixes
- Route attestation protects from changing AS_PATH data, advertising erroneous updates, or breaking local policies
 - Verify that this router is authorized to advertise prefixes, and that it legitimately got update from the previous AS in the AS_PATH

10

Residual Vulnerabilities

- Withholding advertisements
- Re-asserting previously withdrawn route
- Wrongful application of local policies

11

Performance Issues

- Updates are not that frequent – signing them should not take much time
- Also router could receive up to 1 update every 2 seconds
 - Validation overhead would not be a problem
- On reboot, a router receives a lot of updates at once
 - Verification may be costly
 - Router should save validated route attestations on non-volatile storage, then just compare those in the updates with stored ones
- Update size increases from 63B to 450B – but this is small compared to data traffic
- Memory requirements are reasonable (~10MB+26MB per peer)

12