Securing the Internet's Exterior Routing Infrastructure

BGP Vulnerabilities and Security Options

Sandra Murphy

TIS Labs at Network Associates

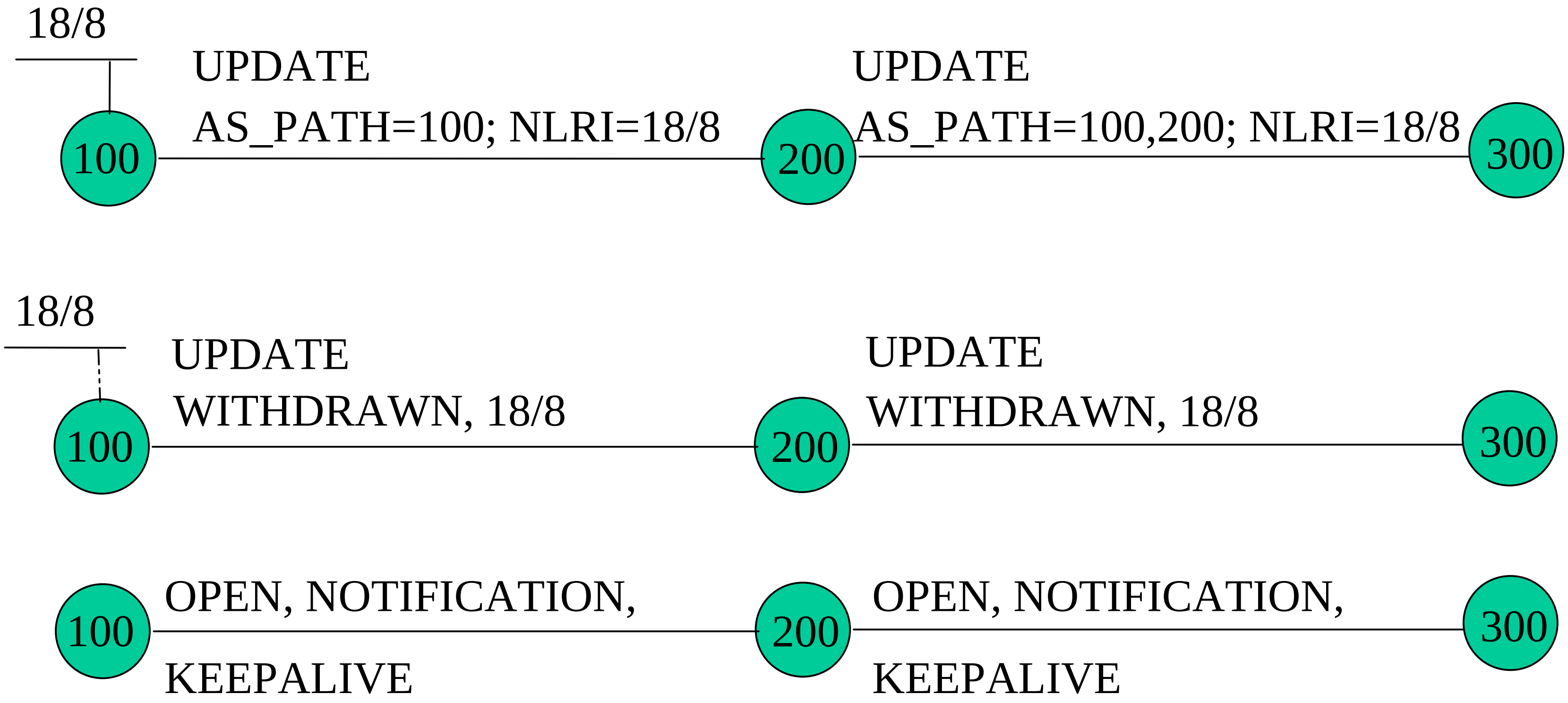
ISOC NDSS '99 2/4/99

TIS Labs at network ASSOCIATES

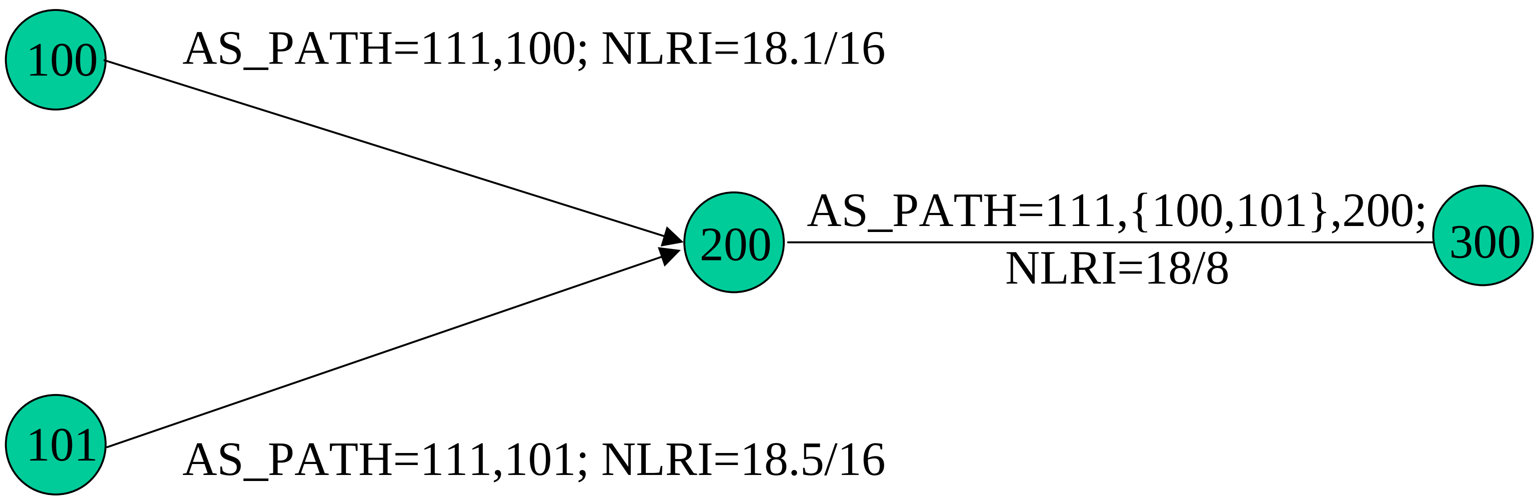
Brief Description of BGP

- BGP belongs to the “distance vector” class of routing protocols (some say “path vector”)
- each Autonomous System receives routes to the network prefixes from its peers
- it computes its best route to each network prefix, based on local policy
- it sends these routes to its peers

Picture of BGP



Picture of BGP aggregation



Vulnerabilities

- weak protection of source authenticity, integrity, or freshness of peer-peer messages
- no authorization of origination of networks
- no protection of authenticity, integrity or freshness of AS path information

Risks

- bogus OPEN/ NOTIFICATION/ KEEPALIVE/ TCP RST
  - disrupt peer-peer communication
  - results in massive changes to routing tables, withdrawn routes, disruption
- bogus UPDATE WITHDRAWAL
  - wherever bogus WITHDRAWAL reaches, network becomes artificially unreachable

Risks (cont'd)

- bogus UPDATE AS_PATH
  - overload routers or AS networks with misdirected traffic
  - misdirected data may follow inefficient path
  - may allow data snooping along bogus route
  - bogus route may actually not forward traffic - network becomes artificially unreachable

Incidents

- Blackholes: all traffic goes to one router/AS
  - a recurring problem from 1970's through today
  - e.g. the AS 7007 problem in spring 1997
- Bogus routes for a particular network
  - constant irritant
- Bogus router/AS
- Peer-peer communication interruption

TIS Labs at network ASSOCIATES

Solutions

- For source authentication, integrity, etc. of peer-peer communication:
  - IPSEC
  - TCP/MD5 (RFC 2385)
  - BGP MD5
- For authorization of network origination
  - need authority

Solutions (cont'd.)

- For AS path protection:
  - digital signature by originating AS
  - digitally signed predecessor information
  - nested signatures of AS-path
  - appeal to registry

Source Authentication Solution

- IPSEC: mature, state-of-the-art, but not everywhere available
- TCP/MD5: widely deployed and used, but not as up-to-date as IPSEC, MD5 strength is suspect
- BGP MD5: has been suggested, but would not protect against TCP RSTs.

Network Origination Solutions

need origination authority that:

- is strongly and everywhere available
- authorizes and authenticates input
- protects data in storage from tampering
- protects communication with queriers
- is compete (or nearly)

AS Path Protection- Signed Origination

- knowing received route is authorized is not sufficient
- also need to know that route was advertised by authorized AS
- originating AS signs original AS Path

TIS Labs at network ASSOCIATES

AS Path Protection - Signed Origination

- advantage: advertisement is not only authorized it is authentic
- disadvantage: the rest of the AS-Path is not protected
- cost: cryptographic management (PKI, keys, Certificates, CRL's, etc.), one signature to verify per AS_PATH

AS Path Protection - Predecessor Signature

- suggested by Smith/Garcia-Luna-Aceves
- originating AS signs and advertises link to neighbor on path (second AS in AS-Path)
- this signed link goes everywhere, similar to link state protocols
- any AS-Path can be compared against the database of received signed links to assure that the adjacencies are valid

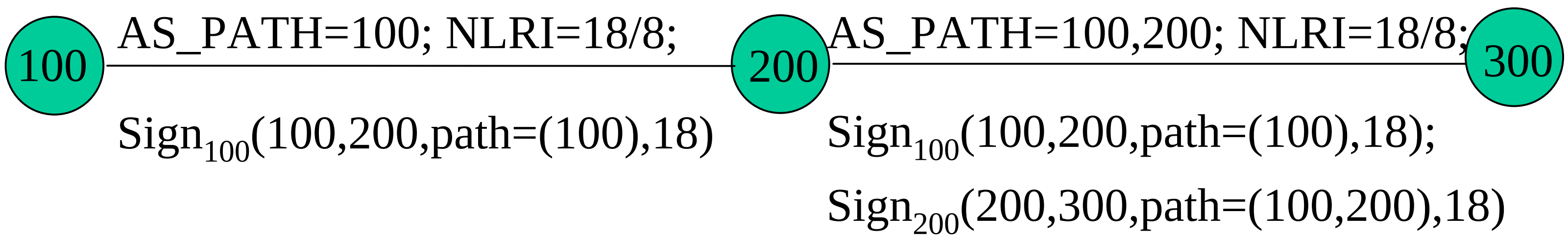
AS Path Protection - Predecessor Signature

- advantages: AS-Path can be verified to be possible, i.e., all adjacencies are valid
- disadvantages: does not assure you that the AS-Path as a whole is valid; difficult to verify AS_PATH for aggregated NLRI
- cost: one signature per link, cryptographic management (PKI, keys, Certificates, CRL's, etc.)

AS Path Protection - Nested Signature

- each router receives routes with signed AS-path (one digital signature per AS on path)
- router computes best route
- router signs new route + AS of peer recipient
- router sends new route, received signatures as proof of validity, and new signature
- recipient checks proof signatures

AS Path Protection - Nested Signature



AS Path Protection - Nested Signature

- advantages: AS-Path verified to be valid
- disadvantage: more complex through aggregation points
- cost:
  - multiple signatures per UPDATE message to carry and validate,
  - one signature generated per UPDATE message,
  - cryptographic management (PKI, etc.)

AS Path Protection - Appeal to Registry

- If AS's register their policy, can validate policy compliance of any received AS-Path
- Advantage: communication with registry is already needed for authorization
- Disadvantage: policy compliance does not assure currently in use; AS's may not wish to disclose details of policy

AS Path Protection - Appeal to Registry

- Cost: protected communication with registry, maintenance of accurate, current, secure registry.

Conclusion

- Source authentication of peer-peer communication: solutions are available. USE THEM.
- Network origination authorization: solutions are proposed (see later talks)
- AS_Path protection: solutions of varying strength are in research stage, but cost increases (with high multiple) with strength