Spring 2023 Topics in Internet Security

Final Project - BGP

Team 18

Minji Seo, Suchan Kim

Introduction

- We modify BGP-4 (RFC 4271) implementation to incorporate verification via PKI
  - Append signatures to existing OPEN, UPDATE message formats
  - 3 signatures:
    - A certificate on (ASN, prefix)
    - Signature on default UPDATE message
    - Signature on (ASN, NLRI) of BGP message origin

Message formats

- Common header
  - 16-octet all-one Marker
  - 2-octet unsigned message Length
  - 1-octet Type
    - 1 - OPEN
    - 2 - UPDATE
    - 3 - NOTIFICATION
    - 4 - KEEPALIV

Message formats

- Update
  - 1-octet Version (4)
  - 2-octet My ASN
  - 2-octet Hold Time: used to calculate connection KeepAlive time
  - 4-octet BGP Identifier: IP of sender’s router
  - 1-octet Optional Parameters Length
  - N-octet Optional Parameters
  - 1-octet Allowed Prefixes Length
  - N-octet Allowed Prefixes: List of prefixes the sender can advertise
  - 256-octet Signature (verify with root CA’s public key)

Message Formats

- Update
  - 2-octet Withdrawn Routes Length
  - N-octet Withdrawn Routes
  - 2-octet Total Path Attribute Length
  - N-octet Path Attributes: includes AS_PATH, NEXT_HOP, …
  - 2-octet Network Layer Reachability Information Length
  - N-octet Network Layer Reachability Information
  - 256-octet Signature: signed on preceding bytes except header
  - 2-octet Origin ASN
  - 1-octet Origin NLRI Length
  - N-octet Origin NLRI: NLRI in the first BGP message
  - 256-octet Origin Signature: signed on Origin ASN, Origin NLRI

Appendix

- Demonstration environment
  - BGP client implementation: yabgp (github)
    - Not usable as a BGP server
    - But runs REST API server at port 8801 to send UPDATE requests to peer
  - Ubuntu 20.04
  - 3 docker containers running Ubuntu 20.04
    - `docker run -it --privileged ubuntu:20.04`
  - 2 containers for BGP peers
  - 1 container for relaying TCP traffic (port 179)
    - Runs only `nc -l 179 < fifo | nc -l 179 > fifo`
    - The two containers establish connection to each one of netcat processes
  - The three containers are connect to the default docker bridge network

Appendix

- Local

```
2023-06-17 23:27:04,285.285 8033 INFO yabgp.core.protocol [-] --route_refresh = True
2023-06-17 23:27:04,285.285 8033 INFO yabgp.core.protocol [-] --cisco_route_refresh = True
2023-06-17 23:27:04,286.286 8033 INFO yabgp.core.protocol [-] --enhanced_route_refresh = True
2023-06-17 23:27:04,286.286 8033 INFO yabgp.core.protocol [-] --graceful_restart = True
2023-06-17 23:27:04,286.286 8033 INFO yabgp.core.protocol [-] --cisco_multi_session = True
2023-06-17 23:27:04,286.286 8033 INFO yabgp.core.protocol [-] --add_path = None
2023-06-17 23:27:04,286.286 8033 INFO yabgp.core.protocol [-] --afi_safi = [(1, 1)]
2023-06-17 23:27:04,295.295 8033 INFO yabgp.core.fsm [-] [172.17.0.4]State is now:OPENSENT
2023-06-17 23:27:07,188.188 8033 INFO yabgp.core.protocol [-] [172.17.0.4]A BGP Open message
as received
2023-06-17 23:27:07,189.189 8033 INFO yabgp.core.protocol [-] --version = 4
2023-06-17 23:27:07,189.189 8033 INFO yabgp.core.protocol [-] --ASN = 65002
2023-06-17 23:27:07,189.189 8033 INFO yabgp.core.protocol [-] --hold time = 180
2023-06-17 23:27:07,189.189 8033 INFO yabgp.core.protocol [-] --id = 172.17.0.3
2023-06-17 23:27:07,189.189 8033 INFO yabgp.core.protocol [-] --allowed prefixes = ['172.17.0
0/24']
2023-06-17 23:27:07,190.190 8033 INFO yabgp.core.protocol [-] [172.17.0.4]Neighbor's Capabili
ies:
2023-06-17 23:27:07,190.190 8033 INFO yabgp.core.protocol [-] --afi_safi = [(1, 1)]
2023-06-17 23:27:07,190.190 8033 INFO yabgp.core.protocol [-] --cisco_route_refresh = True
2023-06-17 23:27:07,190.190 8033 INFO yabgp.core.protocol [-] --route_refresh = True
2023-06-17 23:27:07,191.191 8033 INFO yabgp.core.protocol [-] --four_bytes_as = True
2023-06-17 23:27:07,191.191 8033 INFO yabgp.core.protocol [-] --enhanced_route_refresh = True
2023-06-17 23:27:07,191.191 8033 INFO yabgp.core.factory [-] Set BGP peer id 172.17.0.3
2023-06-17 23:27:07,191.191 8033 INFO yabgp.core.protocol [-] [172.17.0.4]Hold time:180,Keepa
ive time:60.0
2023-06-17 23:27:07,192.192 8033 INFO yabgp.core.protocol [-] [172.17.0.4]Send a BGP KeepAliv
 message to the peer.
2023-06-17 23:27:07,192.192 8033 INFO yabgp.core.fsm [-] [172.17.0.4]State is now:OPENCONFIRM
2023-06-17 23:27:07,220.220 8033 INFO yabgp.core.protocol [-] [172.17.0.4]A BGP KeepAlive mes
age was received from peer.
2023-06-17 23:27:07,220.220 8033 INFO yabgp.core.fsm [-] [172.17.0.4]State is now:ESTABLISHED
2023-06-17 23:27:25,063.063 8033 INFO yabgp.api.utils [-] API request url http://172.17.0.2:8
01/v1/peer/172.17.0.4/send/update
2023-06-17 23:27:25,063.063 8033 INFO yabgp.api.utils [-] API request method POST
2023-06-17 23:27:25,064.064 8033 INFO yabgp.api.utils [-] API POST data {'attr': {'1': 1, '2'
 [[2, [65003, 65001]]], '3': '172.17.0.2'}, 'nlri': ['1.1.1.0/24'], 'origin_msg': {'asn': 650
3, 'nlri': ['1.1.1.0/24']}}
2023-06-17 23:28:07,105.105 8033 INFO yabgp.core.protocol [-] [172.17.0.4]A BGP KeepAlive mes
age was received from peer.
```

Appendix

- Peer

```
2023-06-17 23:27:06,881.881 3075 INFO yabgp.core.protocol [-] [172.17.0.4]TCP Connection esta
lished
2023-06-17 23:27:07,022.022 3075 INFO yabgp.core.protocol [-] [172.17.0.4]Send a BGP Open mes
age to the peer.
2023-06-17 23:27:07,023.023 3075 INFO yabgp.core.protocol [-] [172.17.0.4]Probe's Capabilitie
:
2023-06-17 23:27:07,023.023 3075 INFO yabgp.core.protocol [-] --four_bytes_as = True
2023-06-17 23:27:07,023.023 3075 INFO yabgp.core.protocol [-] --route_refresh = True
2023-06-17 23:27:07,023.023 3075 INFO yabgp.core.protocol [-] --cisco_route_refresh = True
2023-06-17 23:27:07,023.023 3075 INFO yabgp.core.protocol [-] --enhanced_route_refresh = True
2023-06-17 23:27:07,023.023 3075 INFO yabgp.core.protocol [-] --graceful_restart = True
2023-06-17 23:27:07,024.024 3075 INFO yabgp.core.protocol [-] --cisco_multi_session = True
2023-06-17 23:27:07,024.024 3075 INFO yabgp.core.protocol [-] --add_path = None
2023-06-17 23:27:07,024.024 3075 INFO yabgp.core.protocol [-] --afi_safi = [(1, 1)]
2023-06-17 23:27:07,034.034 3075 INFO yabgp.core.fsm [-] [172.17.0.4]State is now:OPENSENT
2023-06-17 23:27:07,094.094 3075 INFO yabgp.core.protocol [-] [172.17.0.4]A BGP Open message
as received
2023-06-17 23:27:07,095.095 3075 INFO yabgp.core.protocol [-] --version = 4
2023-06-17 23:27:07,095.095 3075 INFO yabgp.core.protocol [-] --ASN = 65001
2023-06-17 23:27:07,095.095 3075 INFO yabgp.core.protocol [-] --hold time = 180
2023-06-17 23:27:07,095.095 3075 INFO yabgp.core.protocol [-] --id = 172.17.0.2
2023-06-17 23:27:07,095.095 3075 INFO yabgp.core.protocol [-] --allowed prefixes = ['172.17.0
0/24']
2023-06-17 23:27:07,096.096 3075 INFO yabgp.core.protocol [-] [172.17.0.4]Neighbor's Capabili
ies:
2023-06-17 23:27:07,096.096 3075 INFO yabgp.core.protocol [-] --afi_safi = [(1, 1)]
2023-06-17 23:27:07,097.097 3075 INFO yabgp.core.protocol [-] --cisco_route_refresh = True
2023-06-17 23:27:07,097.097 3075 INFO yabgp.core.protocol [-] --route_refresh = True
2023-06-17 23:27:07,097.097 3075 INFO yabgp.core.protocol [-] --four_bytes_as = True
2023-06-17 23:27:07,098.098 3075 INFO yabgp.core.protocol [-] --enhanced_route_refresh = True
2023-06-17 23:27:07,098.098 3075 INFO yabgp.core.factory [-] Set BGP peer id 172.17.0.2
2023-06-17 23:27:07,098.098 3075 INFO yabgp.core.protocol [-] [172.17.0.4]Hold time:180,Keepa
ive time:60.0
2023-06-17 23:27:07,098.098 3075 INFO yabgp.core.protocol [-] [172.17.0.4]Send a BGP KeepAliv
 message to the peer.
2023-06-17 23:27:07,100.100 3075 INFO yabgp.core.fsm [-] [172.17.0.4]State is now:OPENCONFIRM
2023-06-17 23:27:07,222.222 3075 INFO yabgp.core.protocol [-] [172.17.0.4]A BGP KeepAlive mes
age was received from peer.
2023-06-17 23:27:07,222.222 3075 INFO yabgp.core.fsm [-] [172.17.0.4]State is now:ESTABLISHED
2023-06-17 23:27:25,169.169 3075 INFO yabgp.core.protocol [-] [172.17.0.4]A BGP Update messag
 was received and verified
```

Appendix

- Time to receive and verify UPDATE message: ~100ms
  - Overhead from RSA signature verification (2 times)