BGP Security

By: Andrew Maywapersaud, Nishat Anjum, Hamza Jalil
Outline

- What is BGP?
- Its vulnerabilities
- Possible Attacks
- Countermeasures
Border Gateway Protocol

- Inter-domain routing protocol - used for intra-domain routing too
- Makes routing decisions for traffic between two networks
- Path-vector based to prevent looping
- Application-layer protocol but uses transport-layer to exchange information
Autonomous Systems (AS)

- A collection of networks controlled by a single entity i.e. ISPs, universities etc.
- Has a set of address prefixes
- Has designated gateway routers
- Can peer with other ASes via BGP routing
How BGP Operates

(1)

- Runs over TCP port 179 to exchange messages between routers i.e. OPEN, UPDATE, KEEPALIVE etc.

- Routers advertise their possible routes to destination through UPDATE message specifying
  - address prefixes and
  - mandatory attributes i.e. AS_Path, Next_Hop
How BGP operates
(2)

- Destination router learns multiple routes and selects the best one based on:
  - local policies
  - shortest AS_Path
  - closest Next_Hop router
  - pre-defined set of criteria\[4\]
Vulnerabilities

- BGP does not validate routing information
- Trust-based model: Does not authenticate peers
- No authentication of address prefixes
- No verification of BGP attributes in messages i.e. AS_Path
TCP SYN Flood Attack

- BGP uses TCP
- Incomplete 3-way handshakes: DoS
- TCP reset attacks: Guess sequence number, forge a RESET.
  - Target router drops BGP session
  - Peers withdraw all learned routes
Prefix Hijacking

- No origin authentication
- AS falsely claims an IP prefix
  - Routes traffic to attacker for analysis or manipulation
- Notable victims:
  - Youtube (2008)
  - Google (2012)
  - Amazon (2018)
Route Deaggregation

★ BGP gives preference to more specific prefixes: longest subnet mask

○ BGP peer updates routing table with more specific prefix advertised by attacker

★ Updated prefix becomes preferred routing decision

○ Disrupts internet at a larger scale than prefix hijacking
Route Modification of ASPath

- Route injection
- Route deletion
- Black holing
- Path Subversion
- Man-in-the-Middle
- Loops

BGP Security: No Quick Fix
What Can be Done?

INTERNET ENGINEERING TASK FORCE (IETF)

- RPSL
- SIDR
Routing Policy Specification Language (RPSL)\textsuperscript{[8]}

- Registration
- Authentication
- Adoption

- Policy Registrations
- Hardware Configuration
Secure Inter-Domain Routing Working Group (SIDR)

- Resource Public Key Infrastructure (RPKI)\textsuperscript{[6]}
- BGP Origin Validation\textsuperscript{[6]}
- BGP Path Validation (BGPSec)\textsuperscript{[6]}

Internet Providers ★ Routing security becomes a priority in the aftermath of an incident
Secure Inter-Domain Routing Working Group (SIDR)

- In-band Credential Check
- Heavy Cryptography
- Protection
- RPSL adoption\textsuperscript{[8]}
Future

Inter- Domain Trust System? [5]

Will MD5 & RPKI be enough? [7]

1. Securing the BGP session
   - Vulnerability of TCP [5]

2. Verifying BGP Identity
   - Local AS transmission [5]

3. Verifying BGP Information
   - prefix hijacking [5]
The Basic BGP Security Requirements?
Why is route deaggregation more harmful than prefix hijacking?

How do TCP’s security vulnerabilities affect BGP security?

What technology model discussed earlier can be used to eliminate BGP treat model substantially?
References


