BGP Security

By: Andrew Maywapersaud,
Nishat Anjum, Hamza Jalil

Outline

- What is BGP?
- Its vulnerabilities
- Possible Attacks
- Countermeasures

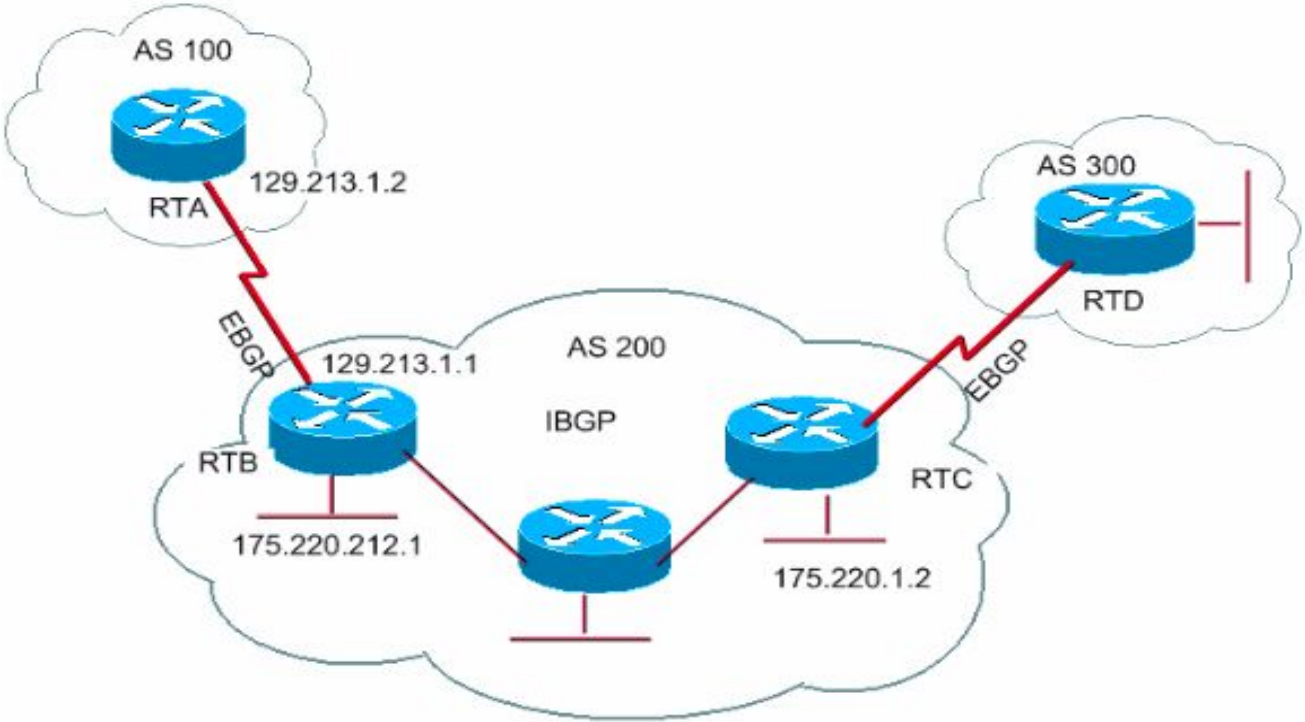
Border Gateway Protocol

- 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

Internal and External BGP Peerings



https://www.goline.ch/it-news/55-internet-autonomous-system-as202032

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)

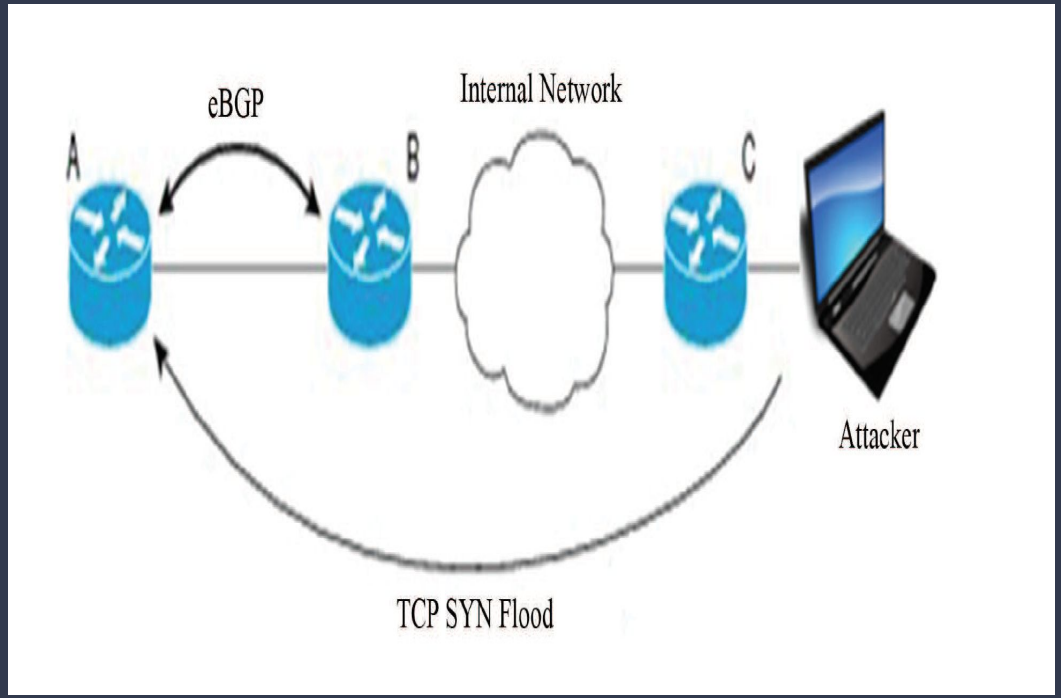
- Destination router learns multiple routes and selects the best one based on:
  - local policies
  - shortest AS_Path
  - closest Next_Hop router
  - pre-defined set of criteria[4]

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

https://smemagazine.asia/en/wp-content/uploads/2019/09/20190917-SME-Website-Byline-Image-Security.jpg

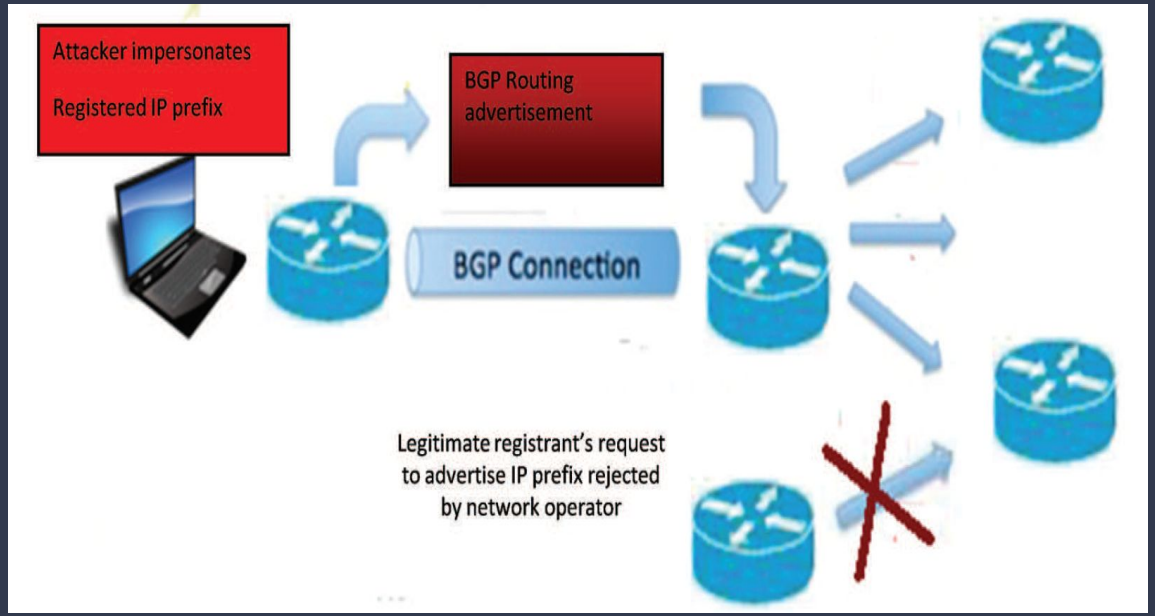
TCP SYN Flood Attack



[1]

- ★ 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



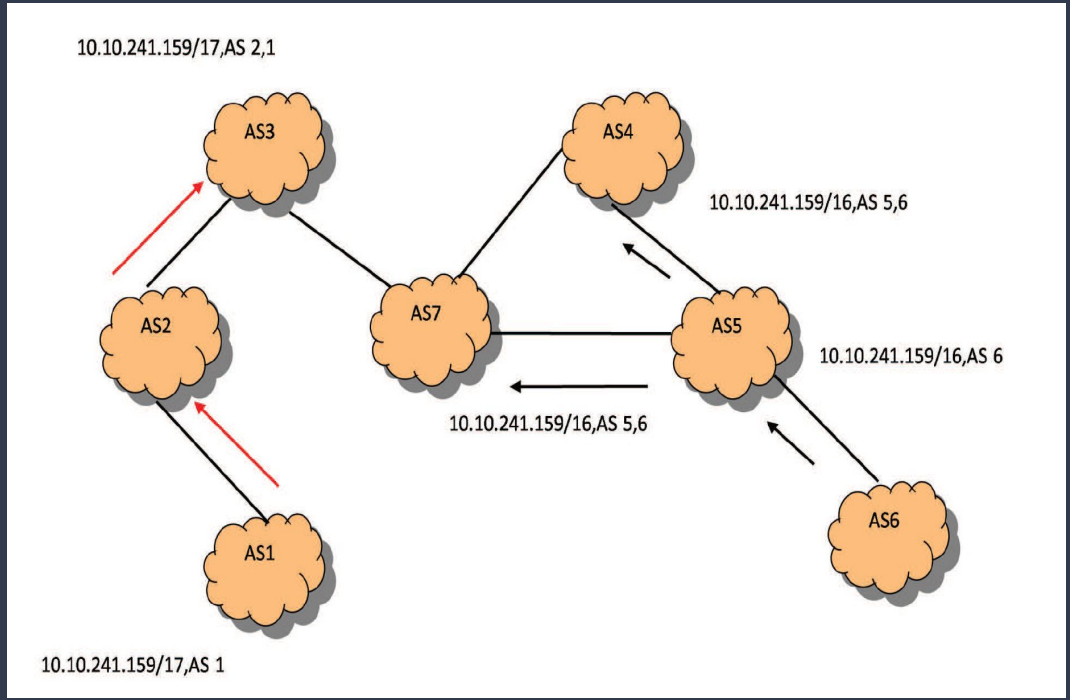
[2]

- ★ 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)

[3]

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

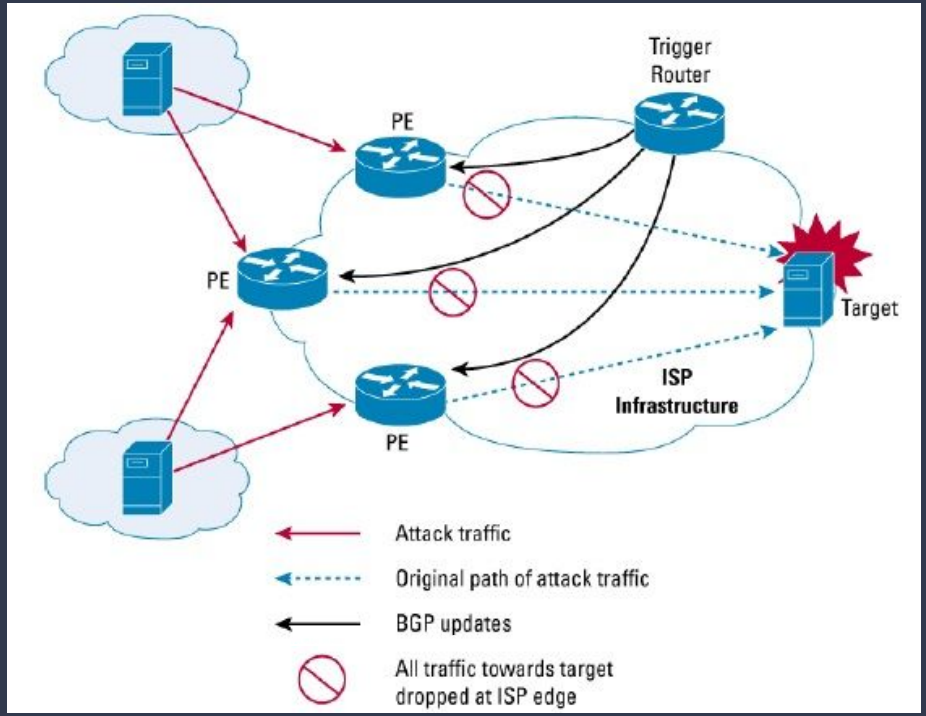


[2]

Route Modification of ASPath

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

[2]



BGP Security: No Quick Fix[8]

What Can be Done ?

INTERNET ENGINEERING TASK FORCE
(IETF)

- **RPSL** [8]
- **SIDR** [8]

Routing Policy Specification Language (RPSL)[8]

- Registration
- Authentication
- Adoption

  - Policy Registrations
  - Hardware Configuration

Secure Inter-Domain Routing Working Group (SIDR)

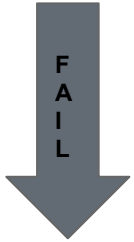
- Resource Public Key Infrastructure **(RPKI)**[6]
- BGP Origin Validation[6]
- BGP Path Validation **(BGPSec)**[6]

Internet Providers

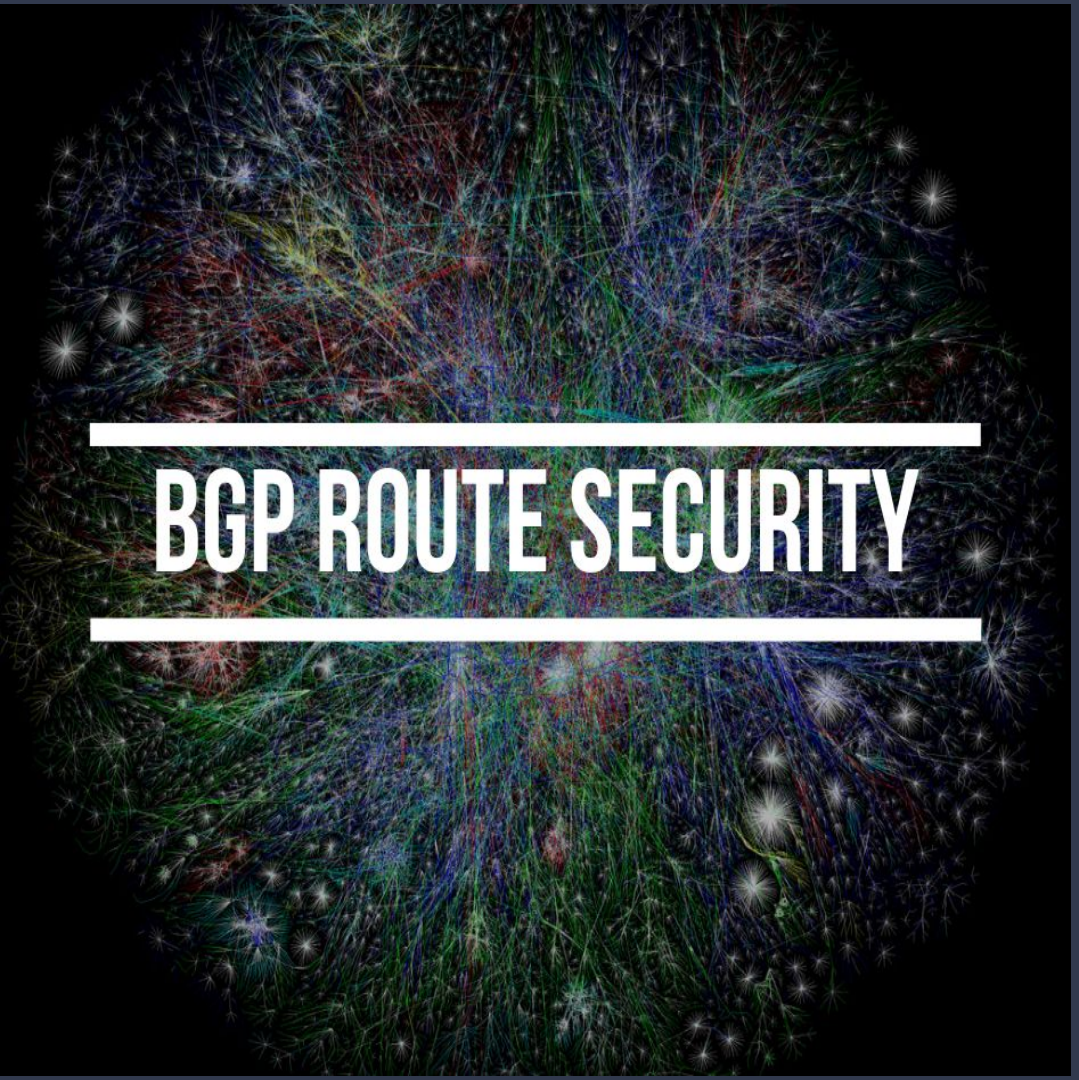
★ **Routing security becomes a priority in the aftermath of an incident**

Secure Inter-Domain Routing Working Group (SIDR)

- In-band Credential Check



- Heavy Cryptography
- Protection
- RPSL adoption[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 ?

QUESTIONS

How do TCP’s security vulnerabilities affect BGP security?

Why is route deaggregation more harmful than prefix hijacking?

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

References

[1] “AS 802 YORKU-AS - York University” [Online] Available: https://db-ip.com/as802

[2] Chakraborty, Suvradip. (2014). Security in Border Gateway Protocol (BGP). 10.4018/978-1-4666-5888-2.ch682.

[3] Hakimi, Rifqy & Saputra, Yuris & Nugraha, Beny. (2016). Case Studies Analysis on BGP : Prefix Hijacking and Transit AS.10.1109/TSSA.2016.7871109.

[4] J.F Kurose and K.W. Ross, “Chapter 5 Network Layer: The Control Plane”, Computer Networking: A Top-Down Approach, 7th Edition, April 2016

[5] Huston, G., Rossi, M., & Armitage, G. (2011). Securing Bgp — A Literature Survey [https://ieeexplore-ieee-org.ezproxy.library.yorku.ca/stamp/stamp.jsp?tp=&arnumber=5473881&tag=1] (2nd ed., Vol. 12).

[6] [Online]Irimia R, Gottschling M (2016) Taxonomic revision of Rochefortia Sw. (Ehretiaceae, Boraginales). Biodiversity Data Journal 4: e7720. https://doi.org/10.3897/BDJ.4.e7720

[7] [Online] Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and protocols for computer communication - SIGCOM Year 2012 Article Title “Towards detecting BGP route hijacking using the RPKI”

[8] Alaettinoglu, Cengiz. “BGP Security: No Quick Fix.” *Www.networkcomputing.com/*, Networkcomputing, 2015, https://www.networkcomputing.com/networking/bgp-security-no-quick-fix.

[9] fig 1 https://www.bleepingcomputer.com/news/technology/new-nist-and-dhs-standards-get-ready-to-tackle-bgp-hijacks/