BGP Security Level Set

Problem Space and Emerging Solutions

Doug Montgomery (<u>dougm@nist.gov</u>) Manager, Internet Technologies Research Group

The Problem Space

BGP Today

• BGP is no longer simple or static

- RFC4271 A Border Gateway Protocol (BGP-4) 2006
 - ~300 current IETF specifications reference BGP-4
 - https://datatracker.ietf.org/doc/rfc4271/referencedby/?full=True

Foundational glue of the Internet

- Distributed routing protocol that spans the globe.
 - Interconnecting ~74K networks called Autonomous Systems.
 - Exchanging reachability information for ~940K destination IP address prefixes.

BGP design requirements

- Support the prevailing business models of Internet Service Provider interconnection.
 - Policy based routing
 - Selective information hiding
 - Enable inter-domain traffic engineering, DDoS mitigation, VPNs, etc.

Today, ISPs employ complex BGP policies and mechanisms to orchestrate information flow across the Internet.



https://computerhistory.org/blog/the-two-napkin-protocol/



BGP Security Vulnerabilities and Threats

- BGP Security Vulnerabilities Analysis (<u>RFC4272</u>)
 - BGP-4 lacks ...
 - Authentication mechanisms
 - to verify rightful address holders and AS operators.
 - Integrity mechanisms
 - to detect unauthorized manipulation of BGP prefix and path data.
 - Authorization mechanisms
 - of which ASes are allowed to announce what address prefixes.
 - of which AS peerings are in use.
 - Scoping mechanisms
 - to BGP announcements to align with policy conventions.
- Threats
 - Prefix hijacks
 - altering the destination misdelivering data, address squatting
 - Route hijacks
 - altering the paths misdirecting traffic along suboptimal or unintended routes.
 - Route leaks
 - Announces routes in violation of peering policies.







BGP Security Risks

BGP Security "Incidents"

• Vary in intent, scale, range, impact, duration, frequency.

Accidents vs Attacks

- "Never ascribe to malice that which is adequately explained by incompetence."
- "Any act of incompetence can be replicated by a malicious actor."

Observed Ramifications

 Traffic interception / monitoring, data theft, censorship, denial of service, subversion of other network services or security mechanisms.









Emerging Solution Space

BGP Security Solutions

- Long history of solution designs
 - IRR filters, S-BGP, soBGP, psBGP, PF-BGP, IRV, Peerlock, PHAS, ARTEMIS



- There are no silver bullets!
- Viable solutions are beginning to emerge for subsets of the problem space.

Attributes of solutions

- Threats addressed
 - prefix hijacks, path hijacks, route leaks
 - sophistication & location of adversary

Objective of the mechanism

- monitoring, detection, mitigation, prevention
- reactive vs proactive

Implementation scope

- use of existing BGP mechanisms, changes to the protocol
- required out-of-band support systems.

Operational requirements

- additional processing / storage on routers
- configuration / management complexity

Utility in partial deployment

- impact of incremental deployment
- requirements for transitive trust / compliance.

Behavioral impacts

- convergence speed, loads, route stability, failure modes
- feature interactions, introduced new threat vectors.

Adoption incentives / barriers

- does cost / complexity align with benefits,
- maturity of commercial products & services

State of Standardization & Commercialization

- IETF Secure Inter Domain Routing & SIDR Operations Working Groups
 - 2006 current



- Resource Public Key Infrastructure (RPKI)
 - Global public key infrastructure and protocol elements to assign and validate certificates to number resource holders and to publish digitally signed routing data signed with them.

• BGP Route Origin Validation (ROV)

 BGP protocol extensions and support protocols to enable routers to use RPKI Route Origin Authorization (ROA) data to perform Route Origin Validation (ROV) on BGP messages.

BGP Path Validation (BGPsec)

Leverages the same PKI to enable each AS to digitally sign a BGP update, proving that each AS in the PATH authorized the
route announcement to its next hop.

BGP Route Leak Detection / Mitigation (OTC, ASPA)

• RPKI extensions for Autonomous System Provider Authorization (ASPA) objects and BGP extensions to allow networks to detect that a BGP routed path violates typical customer-provider-peer policies for route redistribution.

BGP Source Address Validation (SAV)

• DDoS mitigation techniques that leverage RPKI ROA and ASPA information to construct more robust address spoofing filters.

Resource Public Key Infrastructure (RPKI)

Resource Public Key Infrastructure (RPKI)

- Special purpose X.509 Public Key Infrastructure
- Issue resource certificates (ResCerts) to number resource holders
- Publish data objects signed with ResCerts.

Route Origin Authorizations (ROAs)

- Specifies networks authorized to announce prefixes
- Specifies the maximum length of sub-prefixes
- Signed with ResCerts

RPKI Publication Points

- Repositories of RPKI objects
- Protocols to distribute RPKI objects to network operators.



BGP Origin Validation

RPKI Route Origin Validation (RPKI-ROV)

RPKI Validating Caches

- Download RPKI objects from global publication points.
- Perform X.509 validation on the RPKI objects.
- Distribute distilled RPKI data to BGP routers.

Route Origin Validation (ROV)

- Use RPKI data to validate prefix + origin AS in BGP messages.
 - Valid / Invalid / Not Found
- Set BGP origin validation policy
 - e.g. Ignore Invalid routes.

RPKI-ROV Design Goals

- No crypto or X.509 on router
- BGP protocol unmodified



RIR RPKI Trust Anchor

RPKI-ROV Development Status

Production RPKI Services at all RIRs

- ARIN, RIPE, APNIC, LACNIC, AFRNIC
- <u>https://rpki.readthedocs.io/en/latest/rpki/introduction.html</u>

RPKI Software Infrastructure

- Certificate Authority and Publication Point Software
- Validating cache / relying party software
- RPKI-to-Router software
- <u>https://rpki.readthedocs.io/en/latest/ops/tools.html</u>
- RPKI-ROV Capable Routers
 - Juniper, Cisco, Arista, Nokia, MikroTik, Huawei
 - BIRD, Quagga, OpenBGPD, FRRouting, GoBGP, VyOS
 - <u>https://rpki.readthedocs.io/en/latest/ops/router-support.html</u>









RPKI-ROV Deployment Status

Measurement and Monitoring Tools

- NIST RPKI Monitor
 - https://rpki-monitor.antd.nist.gov/
- MANRS Observatory
 - https://observatory.manrs.org/
- The RPKI Observatory
 - https://nusenu.github.io/RPKI-Observatory/
- Others
 - https://rpki.readthedocs.io/en/latest/ops/resources.html





RPKI Deployment Status

Global Internet

- 45% of announced IPv4 routes are RPKI-ROV Valid
- 39% of announced IPv4 address space is RPKI-ROV Valid
- 49% of announced IPv6 routes are RPKI-ROV Valid
- 56% of announced IPv6 address space is RPKI-ROV Valid





RPKI-ROV Analysis of Address Space (/24s) in Unique Prefix-Origin Pairs (IPv4)

RPKI-ROV Deployment Status

Tough Measurement Problem

- See: <u>Towards a Rigorous Methodology for Measuring</u> <u>Adoption of RPKI Route Validation and Filtering</u>, ACM SIGCOMM CCR, Jan 2018.
- Several projects attempt to track this ... all measure things differently
 - https://rovista.netsecurelab.org/
 - https://observatory.manrs.org/#/overview
 - https://rov.rpki.net/

Status Displaying all operators		- Show fewer - Hide ASN column			
NAME	TYPE	DETAILS	STATUS 🔺	ASN ?	
UPX TECNOLOGIA	transit	signed + filtering	Safe	52863	
Lumen	transit	signed + filtering	safe	3356	
Arelion (Formally Telia)	transit	signed + filtering	safe	1299	
Cogent	transit	signed + filtering	safe	174	
NTT	transit	signed + filtering	safe	291	
Hurricane Electric	transit	signed + filtering	safe	693	
GTT	transit	signed + filtering	safe	325	
TATA	transit	signed + filtering	safe	645	
PCCW	transit	signed + filtering	safe	349	
RETN	transit	partially signed + filtering	safe	900	
Orange	transit	signed + filtering	safe	551	
Telefonica/Telxius	transit	signed + filtering	safe	1295	
Comcast	ISP	signed + filtering	safe	792	
Liberty Global	transit	signed + filtering	safe	683	
T-Mobile	transit	filtering	safe	123	
KPN	transit	signed + filtering	safe	28	
Vocus Communications	transit	signed + filtering	safe	482	
Core-Backbone	transit	signed + filtering	safe	3389	
Swisscom	ISP	signed + filtering	safe	330	
Cox Communications	ISP	signed + filtering	safe	2277	
G8	transit	signed + filtering	safe	2832	
Telstra	transit	signed + filtering	safe	122	
GEANT	ISP	signed + filtering	safe	2096	
Softdados Telecom	transit	signed + filtering	safe	52873	



RPKI-ROA / ROV System Dynamics

Monitoring & Analysis of System Dynamics

- Stability and responsiveness of RPKI infrastructure
- Rate and reason for changes in RPKI-ROV
- Routing impact of filtering INVALID origins



https://www.kentik.com/blog/exploring-the-latest-rpki-rov-adoption-numbers/

1.0

User guery to BGP withdraw delay - All peers



NANOG88: Bush - RPKI Ecosystem Measurement

https://www.nist.gov/services-resources/software/nist-rpki-deployment-monitor

FCC BGP Security Workshop

BGP Path Validation

BGPsec PATH Validation

- Adds hop-by-hop digital signatures to BGP PATH
- Addresses authentication and integrity vulnerabilities in BGP prefix and path data.
 - "BGPsec Protocol Specification", IETF RFC 8205.
 - "BGPsec Algorithms, Key Formats, and Signature Formats", IETF RFC 8608.
- Leverages existing RPKI infrastructure to store and distribute router public keys.
- Significant changes to BGP protocol
 - Crypto on the router!

Concerns about operational impact of wide scale deployment.

- Emerging interest in limit use scenarios (direct peering).
- <u>Reference implementations and test tools exist</u>
 - Commercial implementations lagging.



BGP Route Leak Mitigation

Route Leaks

Network direct interconnections are the result of business relationships and service agreements.

"Valley Free Routes" – routes that cross P2C or P2P links can only be further shared with customers (e.g., down).



FCC BGP Security Workshop

BGP Open & Only to Customer (OTC)

AS3

Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages (<u>RFC9234</u>)

- Routers must configure their "role" relationship to each AS that they peer with.
 - Provider, Customer, Peer, Route Server, Route Server Client.

AS1

- Peers exchange roles during BGP session establishment
- If roles do not agree BGP session is closed.
- A route received on P2C or RSC session with OTC attribute, or a P2P with OTC.
 set to AS# other than the peer AS
 - Route leak detected!
 - Route must be ignored.

OTC - optional transitive attribute added to BGP update sent/received from provider, route server, peer indicating that route can subsequently only propagated "down".

AS6

AS7

P20

AS8

OTC=9

AS2

AS4

AS5

OTC=9

AS9

AS10

10.1.*.*/16

OTC=9

. . .

•••

10.1.6.54

ASPA Route Leak Mitigation

Autonomous System Provider Authorization (ASPA)

- Adds new object type to RPKI system
 - A Profile for Autonomous System Provider Authorization
 - ASPA object created and signed by AS owner containing:
 - Customer ASN (singer)
 - List of ALL provider ASNs for the customer.
- ASPA objects gathered and validated by validating cache.
 - Validate ASPA payloads are distributed to routers.
- Routers use validated ASPA data to filter routes.
 - BGP AS PATH Verification Based on Autonomous System
 Provider Authorization (ASPA) Objects
 - Verification results
 - Valid route is feasible and not a leak
 - Invalid route is either infeasible or a leak
 - Unknown route cannot be validated with existing ASPA objects.
- Can be combined with BGP Open & OTC.



10.1.6.54

Questions? More Information

• "Toward the mutual routing security in wide area networks: A scoping review of current threats and countermeasures," Computer Networks, vol. 230, p. 109778, Jul. 2023,

- https://www.sciencedirect.com/science/article/pii/S1389128623002232
- "A survey on securing inter-domain routing: Part 1," APNIC Blog, Jul. 08, 2021.
 - https://blog.apnic.net/2021/07/08/a-survey-on-securing-inter-domain-routing-part-1/
- "A survey on securing inter-domain routing: Part 2," APNIC Blog, Jul. 09, 2021.
 - https://blog.apnic.net/2021/07/09/a-survey-on-securing-inter-domain-routing-part-2/
- "Security of the Internet's Routing Infrastructure,", BITAG Nov. 2022.
 - <u>https://www.bitag.org/Routing_Security.php</u>
- "Routing security: BGP incidents, mitigation techniques and policy actions.," OECD, 330, Oct. 2022.
 - https://www.oecd.org/publications/routing-security-40be69c8-en.htm
- "Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation," National Institute of Standards and Technology, NIST Special Publication (SP) 800-189, Dec. 2019.
 - https://csrc.nist.gov/publications/detail/sp/800-189/final
- NIST Robust Inter-Domain Routing Project
 - https://www.nist.gov/programs-projects/robust-inter-domain-routing

DISCLAIMER Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.