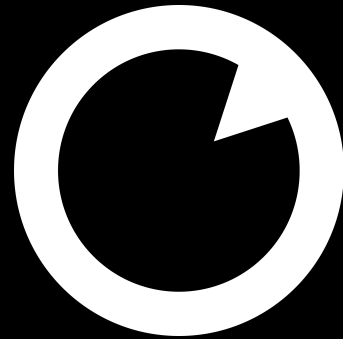# Securing Internet Routing [The Puzzle Pieces]

Tashi Phuntsho
Evangelical Optician (Asia Pacific Lead)
@ Flexoptix

Acknowledgement:

- Slides/ideas from
  - Randy Bush (IIJ Labs/Arrcus)
  - Geoff Huston (APNIC)
  - Aftab Siddiqui (ISOC*)
  - Job Snijders (Fastly)
  - Alexander Azimov (Yandex)
  - Alexander Lyamin (Qrator)
  - Yoshinobu Matsuzaki (IIJ)

Headlines/Incidents

11
September
2024

What the Research & Education Community Learned From Three Impactful Routing Security Incidents in 2024

Incident #1: Commercial Routes Leaked to GREN
Incident #2: GREN Routes Leaked to Commercial Providers   Incident #3: Route Hijack Targeting a U.S. R&E Regional Network

Cloudflare 1.1.1.1 incident on June 27, 2024

2024-07-04

Bryton Herdes   Mingwei Zhang   Tanner Ryan

Radar by Qrator @Qrator_Radar · Jan 24

🇧🇷 AS266518 (LINK) hijacked 1492 IPv4 prefixes (681 prefixes was announced), creating 2703 conflicts with 136 ASNs in 21 countries.

🌐 Max propagation: 47% (mainly in Brazil)
⏳ Start: 2024-01-23 16:48 UTC. Duration: <5 min.

Radar by Qrator @Qrator_Radar · May 25

🚩 BGP Hijack from Unknown

2024-05-25 13:42 UTC:

👤 AS278034 (?) hijacked 2006 IPv6 prefixes, creating 2744 conflicts with 173 ASNs in 12 countries.
230 prefixes was announced via 🇧🇷 AS53102 (Sitel)

🌐 Max propagation: 29%
⏰ Duration: ~5 min

Global BGP Leaks		Global BGP Hijacks
0	APRIL	0
2	MAY	1
4	JUNE	1

https://qrator.net/blog/details/q2-2024-ddos-bots-and-bgp-incidents-statistics-and

3

WHY?

- NO ONE is in charge?
  - No single authority point for the Internet
  - No REFERENCE point for what's RIGHT in routing

WHY?

- Routing works by RUMOUR
  - TELL what you know & LEARN what your neighbours know (tell)
  - Assume everyone is CORRECT & HONEST
    - *Is the originating network the rightful owner?*

WHY?

- Routing works in REVERSE
  - What you TELL others (outbound) affects inbound traffic
  - What you TRUST and ACCEPT (inbound) affects outbound traffic

WHY?

- There is no EVIL (E-bit) bit
  - RFC3514 was a humorous attempt ☺

WHAT DO WE DO?

- Given a bad routing update does not identify itself as BAD
  - *Can we instead, try to identify GOOD updates?*
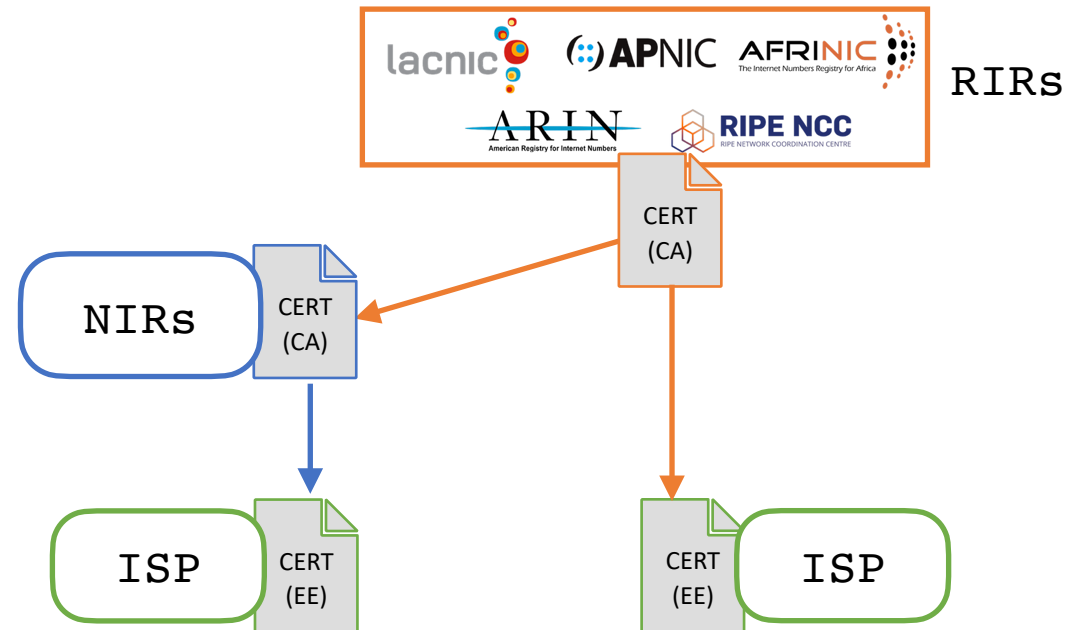 - *How do we identify what is GOOD?*

Identify GOOD

- Back to basics - can we use *Digital Signatures* to convey the Authority to use?
    - Private key to sign the Authority, and
    - Public key to validate the Authority

If the holder of the resource has the private key, it can sign/authorise the use of the resource(s)!

Identify GOOD

- But, how do we establish TRUST in this framework?
  - *Follow the numbered resource allocation hierarchy*

Puzzle Pieces

WHOIS lookup - to verify the holder of a resource(s)

Puzzle Pieces

IRR (Internet Routing Registry) lookup

- Publish routing intent (route origination) and in some cases, inter-AS routing policies

```
~       whois -h whois.radb.net 202.144.128.0
route:          202.144.128.0/23
descr:          DRUKNET-VSNL Route Object
origin:         AS17660
mnt-by:         MAINT-VSNL-IN
changed:        ip.admin@vsnl.co.in 20070102
source:         RADB

route:          202.144.128.0/20
descr:          DRUKNET-BLOCK-A1
country:        BT
notify:         ioc@bt.bt
mnt-by:         MAINT-BT-DRUKNET
origin:         AS18024
last-modified:  2018-09-18T09:37:40Z
source:         APNIC
```

```
~       whois -h whois.radb.net AS17660
aut-num:        AS17660
as-name:        BT-Bhutan
descr:          Divinetworks for BT
admin-c:        DUMY-RIPE
tech-c:         DUMY-RIPE
status:         OTHER
mnt-by:         YP67641-MNT
mnt-by:         ES6436-RIPE
created:        2012-11-29T10:31:33Z
last-modified:  2018-09-04T15:26:24Z
source:         RIPE-NONAUTH
remarks:        ****************************
remarks:        * THIS OBJECT IS MODIFIED
remarks:        * Please note that all data that is generally regarded as personal
remarks:        * data has been removed from this object.
remarks:        * To view the original object, please query the RIPE Database at:
remarks:        * http://www.ripe.net/whois
remarks:        ****************************

aut-num:        AS17660
as-name:        DRUKNET-AS
descr:          DrukNet ISP
descr:          Bhutan Telecom
descr:          Thimphu
country:        BT
import:         from AS6461 action pref=100; accept ANY
export:         to AS6461 announce AS-DRUKNET-TRANSIT
import:         from AS2914 action pref=150; accept ANY
export:         to AS2914 announce AS-DRUKNET-TRANSIT
import:         from AS6453 action pref=100; accept ANY
export:         to AS6453 announce AS-DRUKNET-TRANSIT
import:         from AS42 action pref=250; accept AS42
```

Puzzle Pieces

- <u>IRR</u> entries
  - Used to craft route filters (**prefix/as-path**) with RPSL tools (**rtconfig/bgpq3-4**)

Puzzle Pieces

IRR: using AS-SET

```
~  bgpq4 -l BTv4-IN AS-DRUKNET-TRANSIT
no ip prefix-list BTv4-IN
ip prefix-list BTv4-IN permit 27.123.224.0/19
ip prefix-list BTv4-IN permit 27.123.224.0/22
ip prefix-list BTv4-IN permit 27.124.64.0/20
ip prefix-list BTv4-IN permit 27.124.64.0/22
ip prefix-list BTv4-IN permit 27.124.68.0/22
ip prefix-list BTv4-IN permit 27.124.72.0/22
ip prefix-list BTv4-IN permit 27.124.76.0/22
ip prefix-list BTv4-IN permit 43.230.208.0/24
ip prefix-list BTv4-IN permit 45.64.248.0/22
ip prefix-list BTv4-IN permit 45.64.248.0/23
ip prefix-list BTv4-IN permit 45.64.250.0/24
ip prefix-list BTv4-IN permit 45.64.251.0/24
ip prefix-list BTv4-IN permit 103.7.252.0/22
ip prefix-list BTv4-IN permit 103.10.236.0/22
ip prefix-list BTv4-IN permit 103.10.236.0/22
```

```
~  bgpq4 -6l BTv6-IN AS-DRUKNET-TRANSIT
no ipv6 prefix-list BTv6-IN
ipv6 prefix-list BTv6-IN permit 2001:df3:e180::/48
ipv6 prefix-list BTv6-IN permit 2001:df5:a300::/48
ipv6 prefix-list BTv6-IN permit 2400:1440::/32
ipv6 prefix-list BTv6-IN permit 2400:4e60::/32
ipv6 prefix-list BTv6-IN permit 2400:4e60::/33
ipv6 prefix-list BTv6-IN permit 2400:4e60:8000::/33
ipv6 prefix-list BTv6-IN permit 2403:580::/32
ipv6 prefix-list BTv6-IN permit 2403:580::/33
ipv6 prefix-list BTv6-IN permit 2403:580:8000::/33
ipv6 prefix-list BTv6-IN permit 2403:8700::/32
ipv6 prefix-list BTv6-IN permit 2404:5540::/32
ipv6 prefix-list BTv6-IN permit 2404:5540::/33
ipv6 prefix-list BTv6-IN permit 2404:5540::/34
```

```
~  bgpq3 -3f 17660 -l BT-IN AS-DRUKNET-TRANSIT
no ip as-path access-list BT-IN
ip as-path access-list BT-IN permit ^17660(_17660)*$
ip as-path access-list BT-IN permit ^17660(_[0-9]+)*_(18024|18025|59219|132232)$
ip as-path access-list BT-IN permit ^17660(_[0-9]+)*_(134715|135666|137925|137994)$
ip as-path access-list BT-IN permit ^17660(_[0-9]+)*_(140695)$
```

```
~  bgpq4 -f 17660 -l BT-IN AS-DRUKNET-TRANSIT
no ip as-path access-list BT-IN
ip as-path access-list BT-IN permit ^17660(_17660)*$
ip as-path access-list BT-IN permit ^17660(_[0-9]+)*_(18024|18025|59219|132232)$
ip as-path access-list BT-IN permit ^17660(_[0-9]+)*_(134715|135666|137925|137994)$
ip as-path access-list BT-IN permit ^17660(_[0-9]+)*_(140695)$
```

Puzzle Pieces

Issues with IRR

- No single authority model
  - Is an entry genuine/correct?

- Too many RRs
  - If two RRs contain conflicting data - which one to use/trust?

- Incomplete data
  - If a route is not in a RR : invalid or is the RR just missing data?

Issues with IRR Filters

- ONLY as good as the correctness of the IRR entries!
- USE authoritative sources:
  `-S` in `bgpq3/4`, or `-s` in `rtconfig`

Aside – IRR improvements

prop-151 (Aftab bhai): <u>restricting non-hierarchical as-set</u>

- Helps fix *name collision* issues
- `as-set` can ONLY be created by the maintainer of the ASN in the object

Hierarchical as-set (RFC2622)

- AS-DRUKNET-TRANSIT
  - non-hierarchical as-set
- AS4826:AS-VOCUS
  - hierarchical as-set
  - <AS#>:AS-<as_set_name>

```
as-set:    AS-AMAZON
descr:     Amazon ASNs
members:   AS-AMAZON-NA, AS-AMAZON-AP, AS-AMAZON-EU, AS16509:AS-AMAZON
admin-c:   AC6-ORG-ARIN
tech-c:    AC6-ORG-ARIN
notify:    noc@amazon.com
mnt-by:    MAINT-AS16509
changed:   noc@amazon.com 20230420  #17:54:10Z
source:    RADB
```

```
as-set:         AS-AMAZON
tech-c:         DUMY-RIPE
admin-c:        DUMY-RIPE
mnt-by:         KATERINA-MNT
created:        2022-10-23T19:05:59Z
last-modified:  2022-10-23T19:05:59Z
source:         RIPE
```

```
as-set:         AS4826:AS-VOCUS
descr:          Vocus Communications AS4826 AS-SET
members:        AS4826,AS4826:AS-CUSTOMERS
admin-c:        VPL1-AP
tech-c:         VPL1-AP
remarks:        For queries please email the below contacts
remarks:        NOC - ********
remarks:        IRR Data - ********
remarks:        Peering enquiries - ********
mnt-by:         MAINT-AU-VOCUS
last-modified:  2022-05-29T00:28:23Z
source:         APNIC
```

Aside – IRR improvements

RADB & RPKI ~ *adopted from Maz-san's talk*

- RADB migrated to IRRDv4 on 13th November 2023
- New RPKI based features implemented
  - **route/route6** objects inconsistent with a corresponding ROA will be rejected
  - RPKI Invalid objects will no longer be visible in a query
  - *Not Found* or *Valid* will not be affected

```
Route: 1.1.1.0/24
 Origin: AS13335
  Source: RADB
```

```
Prefix: 1.1.1.0/24
   ASN: 13335
```

```
Route: 1.1.1.0/25
 Origin: AS13335
  Source: RADB
```
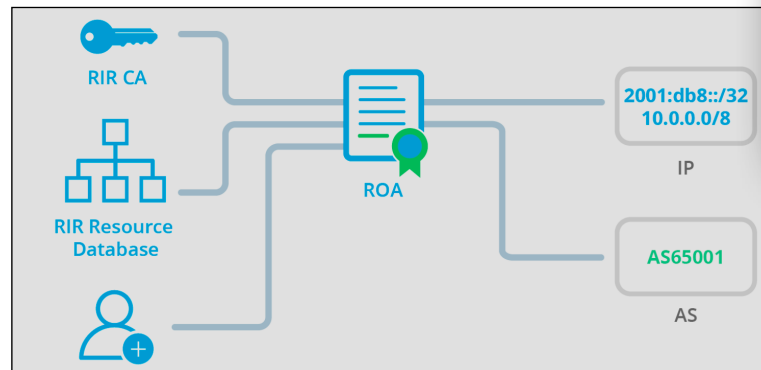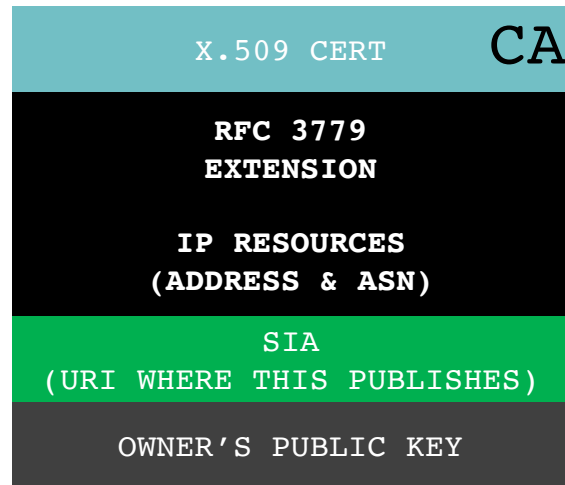
```
Route: 1.1.1.0/24
 Origin: AS12345
  Source: RADB
```

Puzzle Pieces

Route Origin Authorization (ROA)

- Digitally signed object: binding of prefixes & nominated ASN
- Can be verified crypto-magically
- Multiple ROAs can exist for the same prefix

Source: Cloudflare

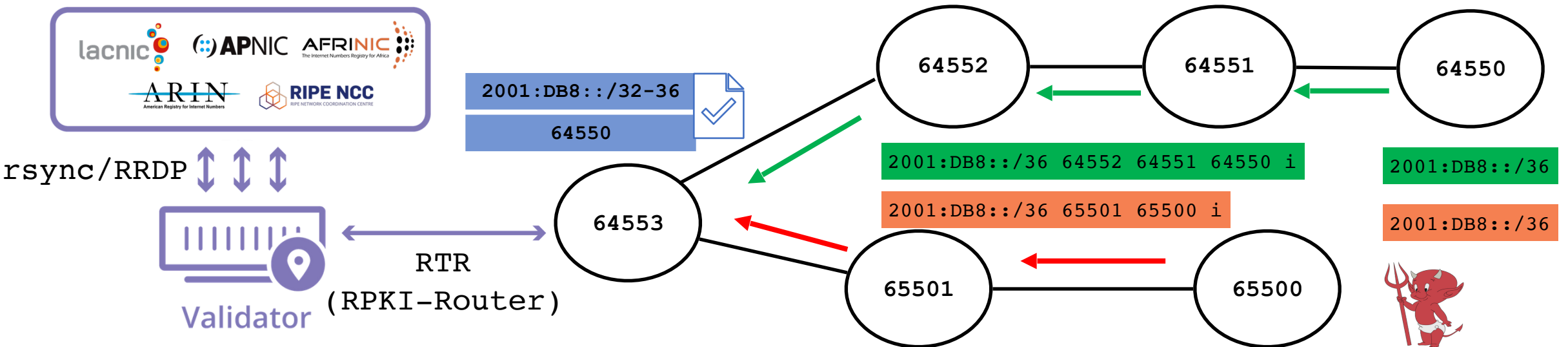| Prefix	202.144.128.0/20
Max-length	/20
Origin ASN	AS18024

Puzzle Pieces

- ## Route Origin Validation (ROV)
  - Validating received routes against validated ROAs
- ## What can it help with?
  - Validate if an ASN is permitted to originate a route
  - Prevent **Origin hijack/fat fingers**

Puzzle Pieces

ROA BCPs

- Use max-length judiciously
  - Only cover those prefixes announced in BGP (`minimal ROA RFC9319`)
- Multi-ASN network?
  - Aggregates/sub-aggs: Transit ASN
  - More specifics: Access ASN
- ROA with **AS0** origin (RFC7607)
 - Not to be confused with undelegated/ unassigned AS0 ROA

ROV BCPs

- Default routes?
- Secure the RTR session
  - `SSH/MD5/TLS/TCP-AO/TLS`
- iBGP propagation – `RFC8097`
- Know your platform:
  - RTR refresh timer → route refresh (`Adj_RIB_In or soft reconfig in`)

https://blog.apnic.net/2020/04/10/rise-of-the-invalids/

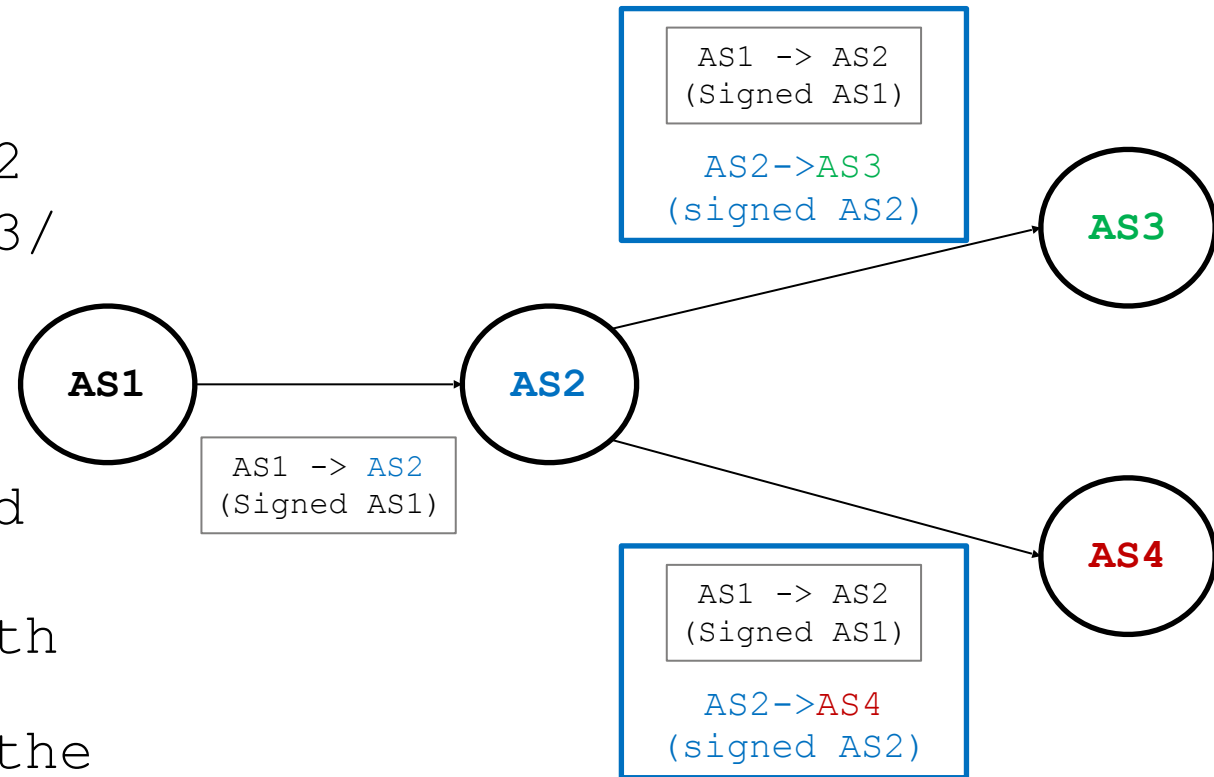https://blog.apnic.net/2022/04/04/rpki-2021-retrospective/

Puzzle Pieces

- ## Are ROAs and ROV enough?
  - Forged origin ASN: will PASS the ROV test & accepted as GOOD
- ## Ideas?
  - Secure the PATH ~ AS path validation (per prefix) → **BGPsec**
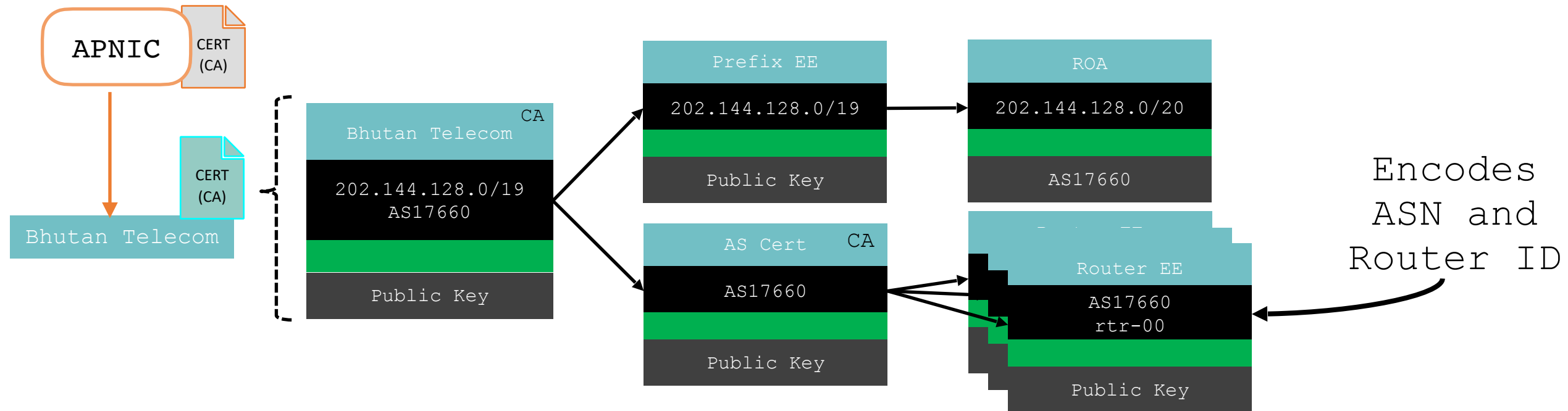
Puzzle Pieces

BGPsec (RFC8205)

- Forward Path Signing
  - AS1 signs the message to AS2
  - AS2 signs the message to AS3/ AS4, encapsulating AS1's message
- Validation
  - ROA check for the prefix and origin AS
  - validate the received AS path against the chain of signatures (for each AS in the AS path) with AS key


```
AS1 -> AS2
(Signed AS1)
```

```
AS2->AS3
(signed AS2)
```

AS3

AS1   **AS2**

```
AS1 -> AS2
(Signed AS1)
```

AS4

```
AS1 -> AS2
(Signed AS1)
```

```
AS2->AS4
(signed AS2)
```

Puzzle Pieces

BGPsec (RFC8205) Challenges

- Cannot jump across non-BGPsec routers/networks
  - `traditional BGP (no BGPsec UPDATE messages)`
- Complex crypto & key distribution mechanism
  - `CPU intensive (`*`validate signatures`*`)`
  - `Memory intensive (`*`per prefix BGPsec UPDATE; new attributes to carry signatures and certs/key IDs for every AS in the AS path`*`)`
- Possible hack
  - *`Routers could generate key pair -> send cert request to RPKI for signing`*
- Lack of clarity
  - `distributing the collection of certs required to validate path signatures`

Puzzle Pieces

Route leak prevention

- We already talked whitelist of customer/peer prefixes under IRR filtering
  - Don't announce routes/prefixes learned from your peers to other peers
  - Apply max prefix limits ~ doesn't help against partial leaks.

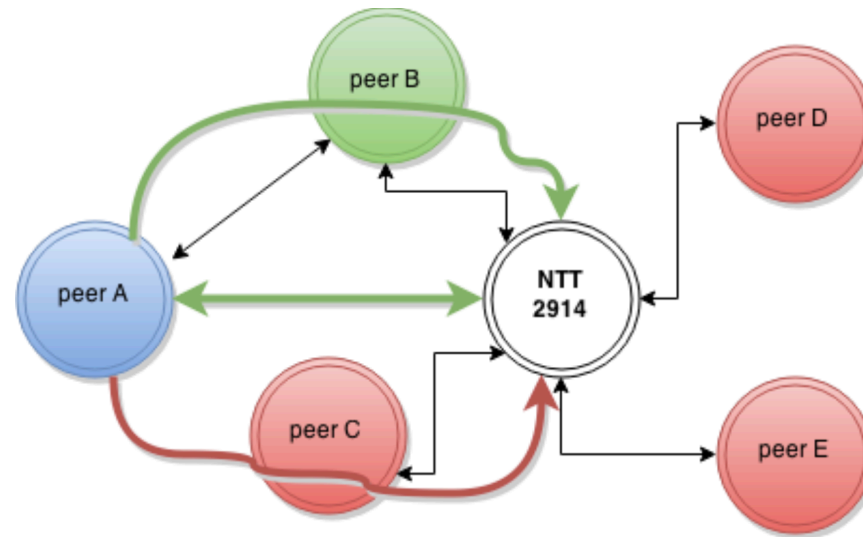# Puzzle Pieces

Peerlock-lite ~ *adapted from Job's NANOG67*

- Wikipedia says [7018, 7922, 3320, 3257, 6830, 3356, 2914, 5511, 3491, 1239, 6453, 6762, 1299, 12956, 701, 6461]
  - https://en.wikipedia.org/wiki/Tier_1_network

- Will you sell transit to these networks?
  - REJECT any prefixes you receive from your customers which contains a big network ASN anywhere in the AS_PATH

```
ip as-path access-list 99 permit \
        _(174|701|1239|1299|2828|2914|3257|3320|3356 \
                |3549|5511|6453|6461|6762|7018|12956)_


route-map ebgp-customer-in deny 1
match as-path 99
```

Puzzle Pieces

<u>Peerlock</u>~ *adapted from Job's NANOG67 talk*

- Given ASNs {A, B, C, D, E} as NTT's peers.
- Peer A subscribes to the peerlock idea (Protected ASN) and indicates that peer B is an "Allowed Upstream"

OK: ^A_
OK: ^B_A_
NOT OK: ^C_A_
NOT OK: ^D_A_
NOT OK: ^E_A_

Job Snijders - Peerlocking - NANOG67

Puzzle Pieces

BGP Roles (RFC9234)

- Update to the BGP OPEN message ~ *BGP Role Capability*
- Must be advertised to and received from a peer
  - If advertised and but not received: SHOULD ignore and establish traditional session
  - Strict mode: if advertised and not received - REJECT
- Roles:
  - Provider | Customer | Peer | RS | RS-client
- Allowed relationship pairs:
  - Provider <-> Customer
  - Customer <-> Provider
  - RS <-> RS-Client
  - RS-Client <-> RS
  - Peer <-> Peer

BIRD

```
protocol bgp {
        local as 65001;
        neighbor 127.20.0.1 as 65000;
        multihop;
        source address 127.20.0.2;
        strict bind on;
        ipv4 {
                import all;
                export all;
        };
        local role customer;
}
```

FRR

```
router bgp 64502
  neighbor 172.16.200.101 remote-as 64501
  neighbor 172.16.200.101 ebgp-multihop
  neighbor 172.16.200.101 passive
  neighbor 172.16.200.101 local-role customer
```

https://blog.qrator.net/en/route-leak-prevention-and-detection-rfc9234_162/

Puzzle Pieces

BGP Roles (RFC9234)

- ## Only to Customer (OTC) attribute
  - Optional non-transitive attribute

- ## Ingress procedure:
  - If a route with the OTC Attribute is received from a Customer or an RS-Client, then it is a route leak and MUST be considered ineligible.

- ## Egress procedure:
  - If a route contains the OTC Attribute, it MUST NOT be propagated to Providers, Peers, or RSes

Solution	Status	Version
BIRD	+	Appeared in 2.0.11
FRR	+	Appeared in 8.4
OpenBGPD	+	7.5
Mikrotik	Reduced functionality	Appeared before RFC

https://blog.qrator.net/en/route-leak-prevention-and-detection-rfc9234_162/

https://mailman.nanog.org/pipermail/nanog/2024-September/226204.html
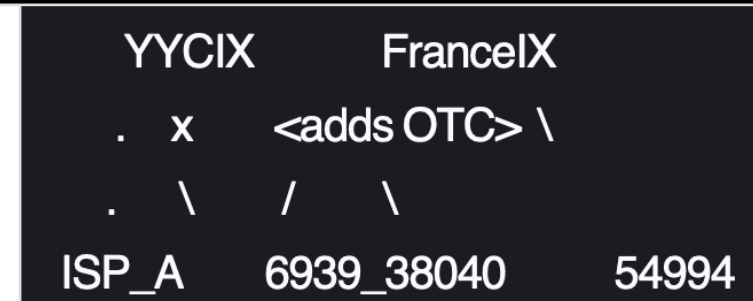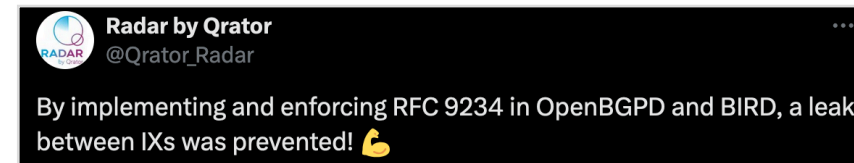
Puzzle Pieces

ASPA (AS Provider Authorization)

Looks at malformed AS_PATHs from customers and peers to detect malicious hijacks and route leaks

- ASPA is a digitally signed object that binds
  - `Set of Provider ASNs (SPAS) to a Customer ASN (CAS) for a specific AFI –` ***signed by the holder of the Customer ASN***

- For Routing, the ASPA is an attestation
  - `that the AS holder (CAS) has authorized the SPAS to propagate its announcements onwards (upstreams/peers)`

Puzzle Pieces

<u>ASPA</u> (AS Provider Authorization) object

```
ASPA := {
        customer_asn (signer)
        providers (authorized to propagate to peers/upstreams)
        AFI (IPv4/IPv6)
}
```

Puzzle Pieces

ASPA in action - 26 January'23

https://www.manrs.org/2023/02/unpacking-the-first-route-leak-prevented-by-aspa/

Puzzle Pieces

ASPA timeline [`BGP, RP, RTR, Signer`]

2023
- OpenBSD rpki-client and OpenBGPD
- Routinator, Krill and RTRTR, StayRTR, rpki-prover, and RIPE NCC have either released ASPA-capable software or are in advanced stages to do so.
- APNIC signer demo - https://github.com/APNIC-net/rpki-aspa-demo

2024
- 6-10 months for IETF to ratify ASPA
- SIDROPS in later stages of specifying the ASPA standard
- Tom Harrison (APNIC RPKI Lead): will start hosted in 2024

2025
- RIRs make Signers available

2026
- COTS BGP Speakers implementations

https://www.manrs.org/2023/05/estimating-the-timeline-for-aspa-deployment/

Puzzle Pieces

AS-Cone [draft expired since Oct'2020]

- *A digitally signed object that binds an ASN and its downstream or transit customer ASNs (and their transit relationship/policies)*

Need Help?

- Want to learn more about:
  - crafting route filters,
  - securing Internet routing best practices/tools
- Refer to NSRC's free training videos at:
  - https://learn.nsrc.org/bgp
- APNIC Academy:
  - https://academy.apnic.net/

شکریہ