RIPE NCC
RIPE NETWORK COORDINATION CENTRE

# Routing security, another elephant in the room

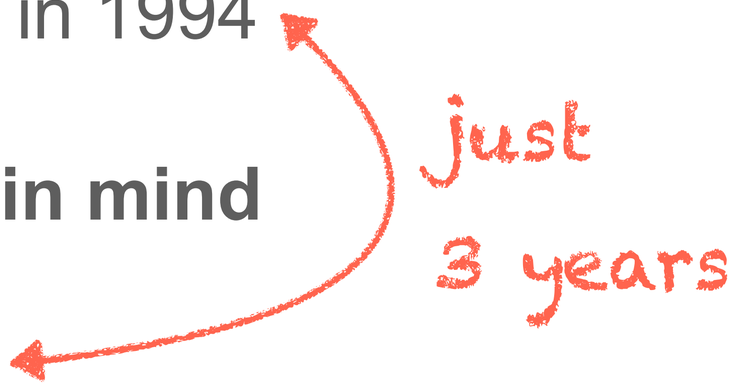
Alex Semenyaka | BHNOG | March 22, 2023

# Border Gateway Protocol

- To reveal routes in the Internet, the Border Gateway Protocol (BGP) was invented
- Created in 1989 (RFC 1105)
- Current BGP version (BGPv4) was released in 1994
- **BGP was never created with the security in mind**
  - The first major incident (AS 7007 incident): April 25, 1997

# Border Gateway Protocol

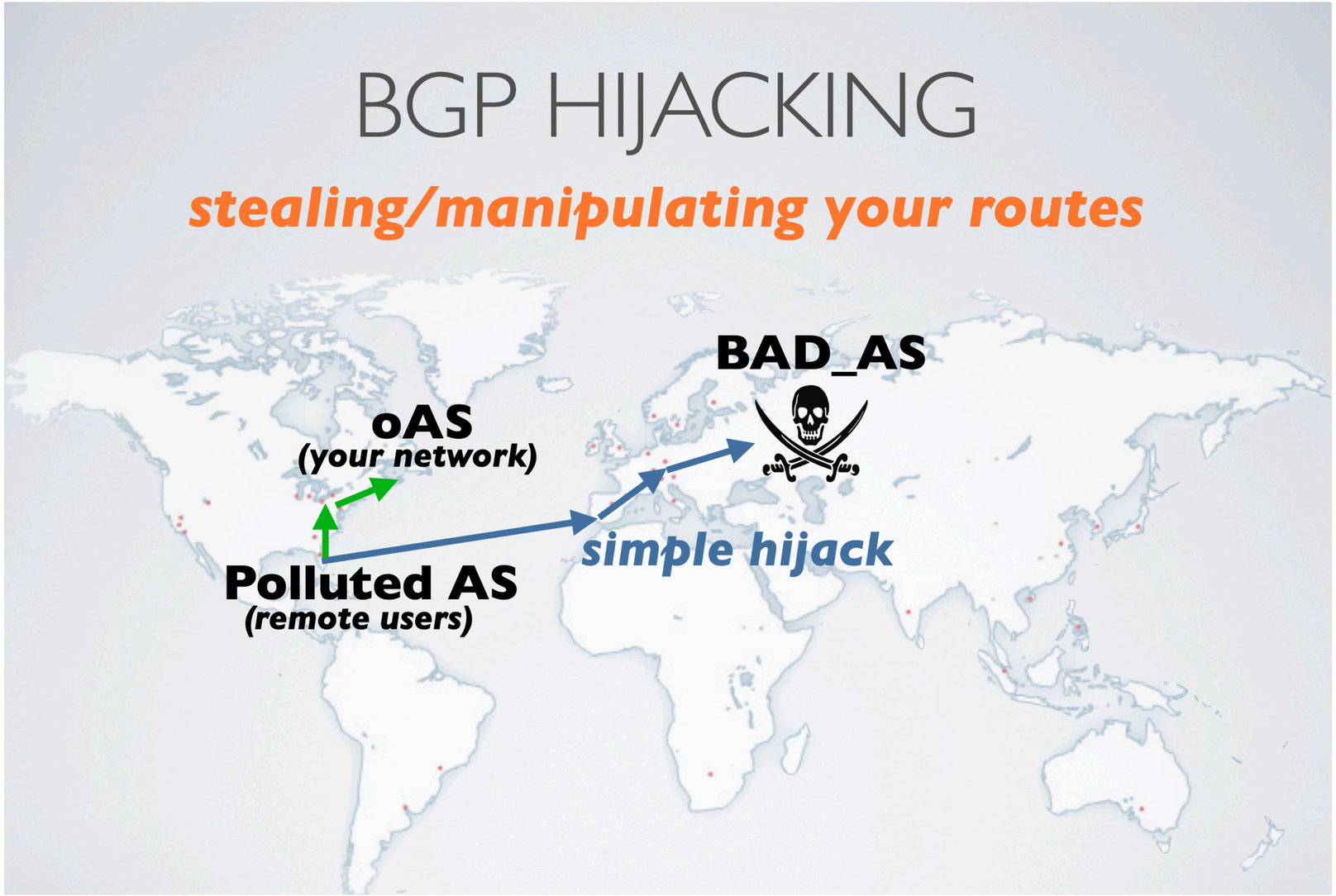
- To reveal routes in the Internet, the Border Gateway Protocol (BGP) was invented
- Created in 1989 (RFC 1105)
- Current BGP version (BGPv4) was released in 1994
- **BGP was never created with the security in mind**
  - The first major incident (AS 7007 incident): April 25, 1997



# BGP Security

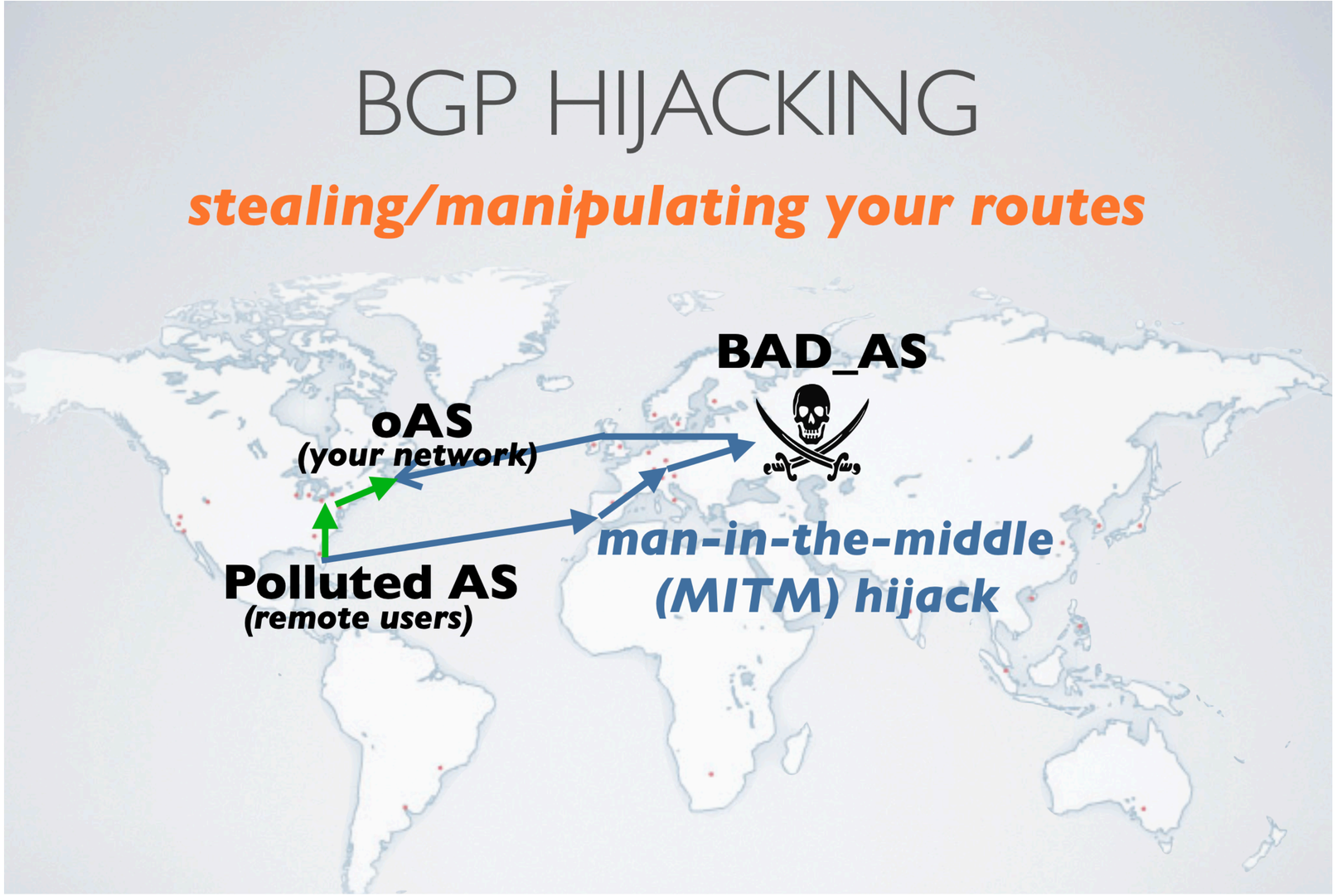
- Alas, BGP was never created with the security in mind
- BGP runs on a huge number of different devices, so it is difficult to quickly implement changes to the protocol
- Improvements to the BGP security model have been going on for a long time
  - …but the legacy design problems are still many

# Basic scenarios: prefix hijack




- “Ideal Denial-of-Service attack”:
  - no victim's resources are exhausted
  - all systems appear to be functioning normally
  - no accessibility from the world.
- Maybe not the victim itself is attacked, but the infrastructure part (e.g., DNS server)

# Basic scenarios: intentional route leak




- Ability to inspect the victim's traffic
- Significant deterioration in the quality of service
- Even harder to detect

# The problem overview

- Any AS can announce any prefix
- Anyone can prepend any ASN to the BGP path
- BGP announcements are accepted without validation
- BGP packets are transmitted without any encryption or authentication mechanisms
- No single authoritative source for who should be doing what

# Sometimes it happens accidentally!

- Typing errors
  - Also known as “fat fingers syndrome”
  - May cause mis-origination
- Configuration errors
  - Faulty BGP filter configuration
  - AS path prepending mistakes
  - Cause routing policy violations and unintentional route leaks/prefix hijacks
- Equipment malfunctioning

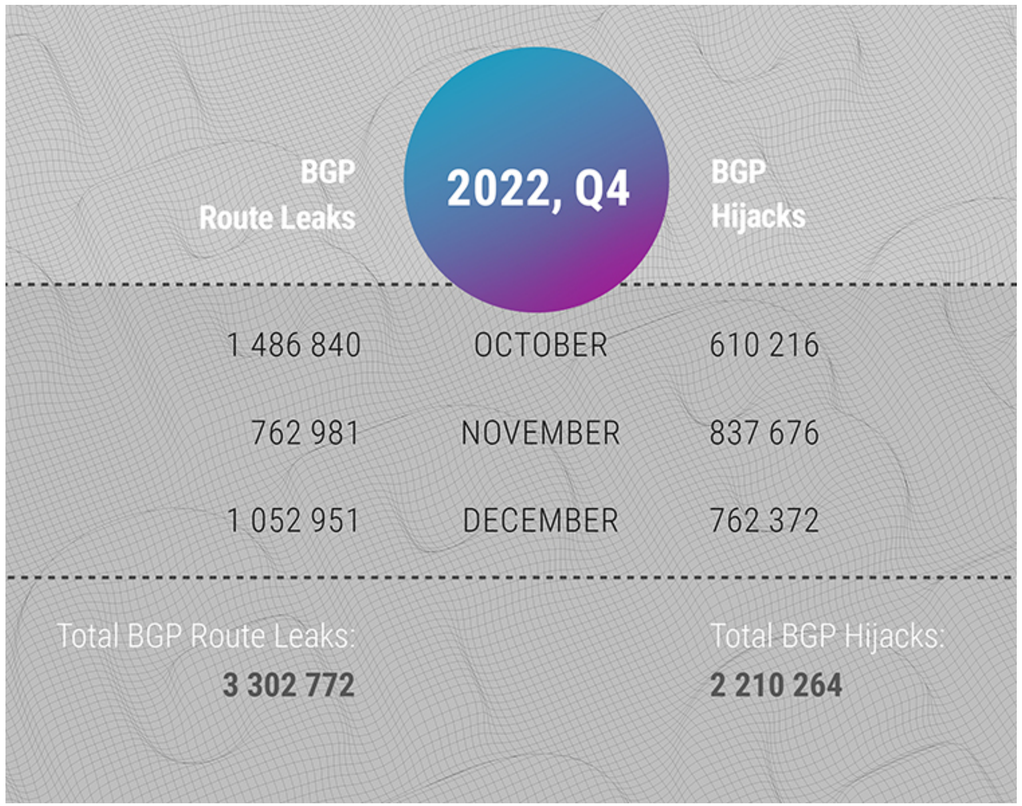
# Malicious opportunities

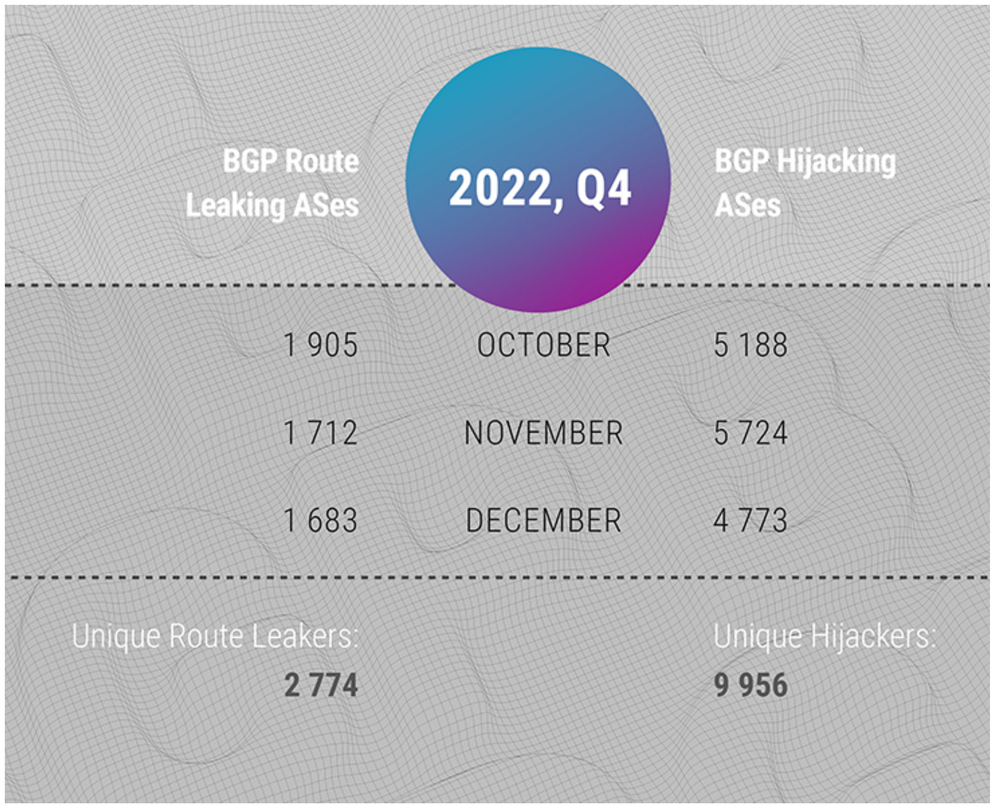
- The perfect DDoS
  - The victim has plenty of resources, but nothing works
- Traffic surveillance
  - Encryption only protects data, but **metadata** can often be recovered or even surveilled
- Identity theft
  - As an example, an attacker issues new TLS certificates, which can then be used for **MitM attacks with full traffic disclosure**
- Digital Assets Theft
- Etc.

# Some examples

- 2003,2008 - hijacking DoD USA address space to send spam
- 2005 - hijacking the address space of Google blocked their services for 1 hour
- 2007 - use of BGP to create fake root DNS servers
- 2013 - DDoS attack by hosting company Cyberbunker on Spamhaus using BGP
- 2014, 2018 - Theft of mined cryptocurrency through fake BGP announcements
- 2017 - A BGP configuration error on the Google network caused the whole of Japan to lose connectivity with the rest of the world for about 30 minutes
- 2019 - an attack on the national DNS of several countries led to the interception of the traffic of many organizations, obtaining logins and passwords to their systems

# Statistics from Qrator Labs



# Countermeasures

Today and tomorrow

# Existing approaches

- Internet Routing Registries (IRR) Data
- RPKI Framework
  - ROA
  - ASPA
- BGPSEC
- BGP Roles
- Incidents detection

# Can Internet Routing Registries help?

## Concerns with the IRR system

**1**

**Not globally deployed**

Just distributed databases

**2**

**No central authority**

Who will verify the accuracy of the data?

**3**

**No verification of holdership**

Anyone can input anything

**4**

**Not updated properly**

Information is missing, outdated or incorrect

*(From RPKI RIPE Training Course)*

# Can Internet Routing Registries help?


*(From RPKI RIPE Training Course)*

# Can Internet Routing Registries help?

- However, IRR data are important for other purposes
- And in any case, the defense must be echeloned.

**Please, do use IRR!**

*(From RPKI RIPE Training Course)*

# That’s why RPKI was invented

- RPKI is…
  - A resource certification (well familiar X.509 PKI certificates)
  - A security framework (extendable and flexible)
- The currently implemented part of the RPKI is ROA
  - ROA = Route Origin Authorisation
  - verifying the right of an autonomous system to announce that it has a certain prefix
- Next step: ASPA
  - verifying the sequence of ASes along the path

# How does ROA work?

Ties IP addresses and ASNs to public keys

Follow the RIR hierarchy, forming chains of trust (think HTTPS)

Authorised statements from resource holders

- “ASN X” is authorised to announce my prefix Y
- Signed, holder of Y

# How does ROA help with routing security?

- Used to validate the origin of BGP announcements
  - Is the originating ASN authorised to originate this particular prefix?
- Has two parts:
  - Signing own prefixes
  - Verification of others' announcements
- Not a silver bullet
  - Helps address a limited set of violation scenarios

# ASPA (AS Path Authorization)

- Still a draft (current state: draft-ietf-sidrops-aspa-verification-05)
- New element of the RPKI Framework
- Uses the same technique to tie adjacencies in the AS PATH using security certificates
  - Holders of autonomous systems describe links with their neighbors and sign this information with their keys
  - Thus, it is possible to validate the AS PATH attribute (fully or partially)
- Being combined with ROA and BGP roles covers the vast majority of the violation scenarios
  - 925 sterling silver bullet 🙂

# BGPSEC

- RFC Since 2017: RFC8205
- Uses RPKI certificates but is not a part of the RPKI framework
- Uses a new, signed PATH attribute and verifies the signatures in each UPDATE message
- There is a fallback to plain BGP if a peer along the way does not support BGPSEC
- However, the real effect could be achieved only if all BGP speakers support BGPSEC

# BGPSEC issues

- It is a silver bullet, but at the moment, it is a really, really slow bullet
- Today it takes many hours to establish a BGP session
  - The double fault probability is too high now
  - The risk is unacceptable, and had to be mitigated

More uplinks => extra $$

While one session is being re-established, the second session is switched to plain BGP

Incorrect routing information can now be injected without checks

Implementation: volumetric DDoS to the first interface + later injecting malicious routes through the second one

# BGPSEC issues

- It is a silver bullet, but at the moment, it is a really, really slow bullet
- Today it takes many hours to establish a BGP session
  - The double fault probability is too high now
  - The risk is unacceptable and should be mitigated

**In future, it can change**

**When equipment is fast enough, BGPSEC is going to jump in.**

More uplinks = extra protection

While one session is being established, the second session is switched to plain BGP

Incorrect routing information can now be injected without checks

Implementation: volumetric DDoS to the first interface + later injecting malicious routes through the second one

# BGP Roles

- A fresh RFC: RFC 9234
- Defines roles of the BGP session participants:
  - Provider, Customer, RS, RS-Client, Peer
- BGP Only to Customer (OTC) Attribute
- Easy to implement and to deploy
- Also not a silver bullet:
  - Demonstrates the nature of the relationship between companies
    - Their disclosure may be highly undesirable from a commercial point of view
  - Helps address a limited set of violation scenarios

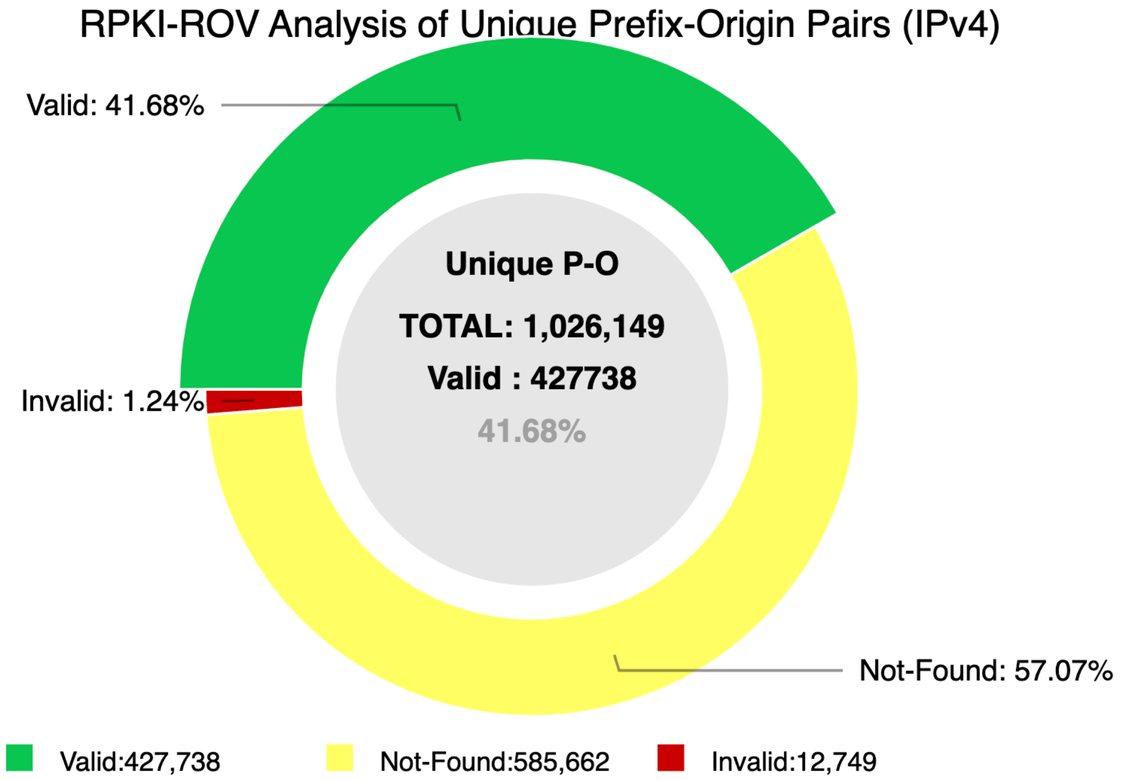
# Incidents detection

- So far, reliable measures to prevent routing incidents are not implemented in the equipment
- Therefore, it is still important to be able to identify such events and work them out manually
- There are different tools to address that, and their usage must be integrated into network operation processes
  - RIPE RIS, RIPEStat
  - A.R.T.E.M.I.S as a stand-alone product
  - Qrator Radar
  - …
- More algorithms to come
  - draft-ietf-grow-route-leak-detection-mitigation-00 as an example

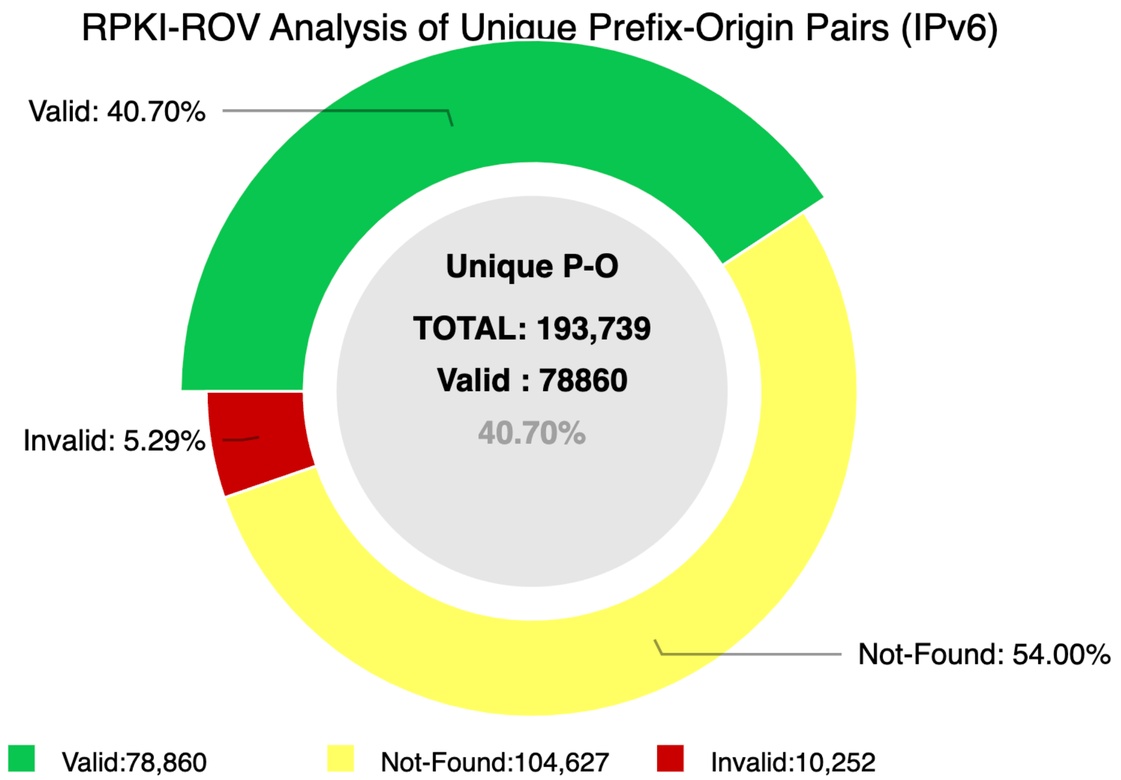
# Intermediate conclusion

- **RPKI is really important now**
- Although it does not currently cover all scenarios, experience is being gained in its operation
- Robust approaches of the future will use RPKI in one way or another

# The global overview (NIST data)

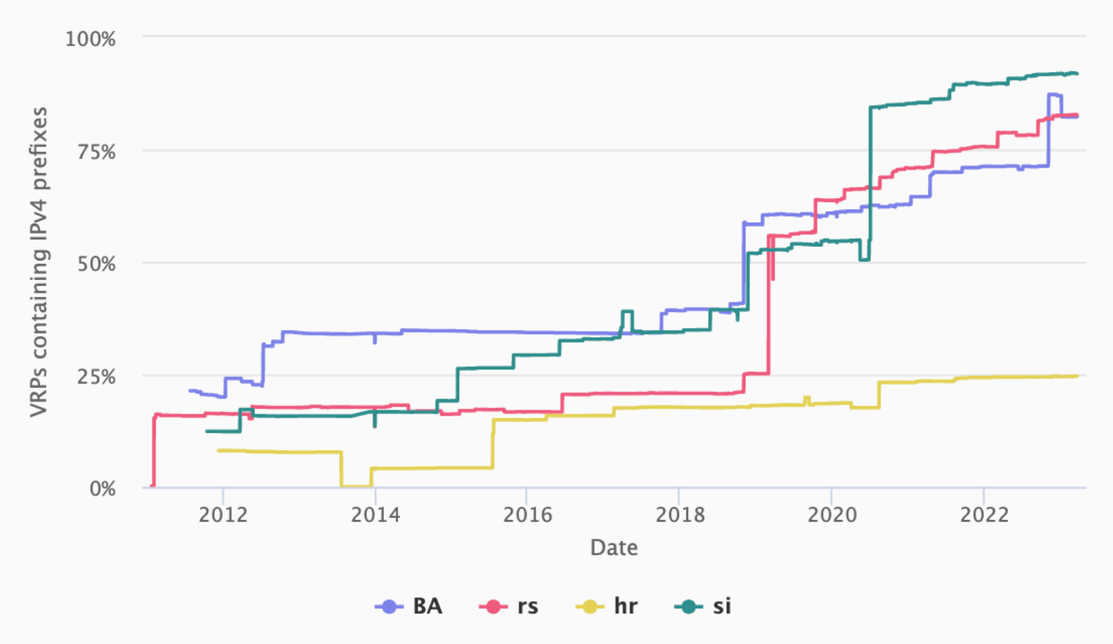



IPv4




IPv6

# ROA Signing in Bosnia i Herzegovina




IPv4


IPv6

# Some observations

- The ratio of signed IPv4 prefixes in Bosnia i Herzegovina is not bad at all!

- However, for IPv6 it is below the world average

  - Do IPv6 enthusiasts and RPKI enthusiasts have little overlap?

  - Signing IPv4 networks is no different from signing IPv6 networks!

# Last but not least

- If you want to know how to deal with routing security, contact us!
- We have our educational programs
  - Face-to-face training courses
    - https://learning.ripe.net/w/courses/cat-16-training-courses/
  - Webinars
    - https://learning.ripe.net/w/webinars/
  - RIPE Academy
    - https://academy.ripe.net/

# Questions

asemenyaka@ripe.net