Sept 2022

Mutually Agreed Norms for Routing Security

MANRS Presentation for the Joint Engineering Team

Andrew Gallo
MANRS Steering Committee Co-Chair

What is MANRS?

Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats. MANRS offers specific actions via four programs for Network Operators, Internet Exchange Points, CDN and Cloud Providers, and Equipment Vendors.

A bit of history

- In 2014, a group gathered to improve the security and resilience of the global routing system
- Produced ***Routing Resilience Manifesto***
- Original contributors
  - David Freedman, *Claranet*
  - Wesley George, *Time Warner Cable*
  - Jason Livingood, *Comcast*
  - Andrei Robachevsky, *Internet Society*
  - Job Snijders, *NTT*
  - Tony Tauber, *Comcast*

MANRS Today

MANRS is a collaborative initiative of Internet operators

The MANRS Participants are the Internet operators that meet the requirements of the (currently) 4 MANRS programmes:

- Network Operators – 713 participants (896 ASNs)
- IXPs – 104 participants
- CDN/Cloud Providers – 20 participants
- Vendors – 6 participants

MANRS Partners are 19 organisations recognised by the MANRS Community as supporting MANRS through promotion, training, resourcing and/or in other ways

MANRS

MANRS Steering Committee

The Internet Society has developed and supported the MANRS initiative, which has grown quickly and also gained credibility outside of the operator community

MANRS has become bigger than what ISOC staff can support alone

Increasing number of decisions also need to be made :

- Auditing questions as they arise
- How to strengthen the existing MANRS Actions
- Development of ongoing MANRS conformance criteria
- How to handle participants failing to meet the necessary criteria for MANRS conformance
- Development of new programmes

MANRS should be a self-regulating community!

MANRS Steering Committee Membership

Elections were held on 1-3 November 2021, and following persons were elected:

See https://www.manrs.org/about/governance/steering-committee/steering-committee-members/

MANRS For Network Operators

MANRS Actions – Network Operators Programme

There are four actions for Network Operators

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information in relevant RIR database and/or PeeringDB

Global Validation

Facilitate validation of routing information on a global scale

Publish your routing data, so others can validate

Registering number resources in an IRR and/or creating ROAs for them

The Actions in Operation – *Filtering* (Mandatory)

- Description

  Network operator must implement a system whereby they only announce to adjacent networks the AS numbers and IP prefixes they or their customers are legitimately authorized to originate.

  Network operator much check whether the announcements of their customers are correct; specifically, that each customer legitimately holds the AS numbers and IP address space they announce.

- Possible Implementation mechanism
  - Import/Export prefix filters on BGP sessions
  - AS path filter

The Actions in Operation – *Communication & Coordination* (Mandatory)

- Description

  Network operator must ensure that up-to-date contact information is entered and maintained in the appropriate RIR (or NIR) database and/or in PeeringDB. It is strongly recommended that contact information is made publicly available, but at a minimum must be available to other network operators registered with PeeringDB.

- Possible Implementation mechanism
  - Should be pretty obvious!
  - ARIN already bugs us yearly. Just validate and keep your POCs up to date.
  - Use PeeringDB? Keep that up to date as well (including max prefixes!!)←this is a personal gripe

The Actions in Operation – *Global Validation* (Mandatory)

- **Description**

  Network operators must publicly document their intended routing announcements in the appropriate RIR routing registry, RADB or an RADB-mirrored IRR. This includes ASNs and IP prefixes originating on their own networks, as well as the networks for which they provide transit services.

  A network operator may alternatively implement Action 4: Facilitate routing information on a global scale RPKI in lieu of a publicly documented routing policy.

- **Possible Implementation mechanism**
  - IRR
  - RPKI ROAs (but this isn't enough, despite the term "*in lieu*"
- Lots of discussion around this Action

The Actions in Operation – *Anti-Spoofing* (Recommended)

- **Description**

  A network operator should implement a system that enables source address validation for their own infrastructure and end users, and for any Single-Homed Stub Customer Networks. This should include anti-spoofing filtering to prevent packets with an incorrect source IP address from entering or leaving the network.

  A network operator must test whether their network is able to send packets with forged source IP addresses using the CAIDA Spoofer Software. This is to alert the network operator as to whether their network might be used to originate Distributed Denial-of-Service (DDos) attacks, whilst generating publicly accessible information allowing that network to be checked by others.

- Recommended because external validation/measurement is hard

Issues before the Steering Committee

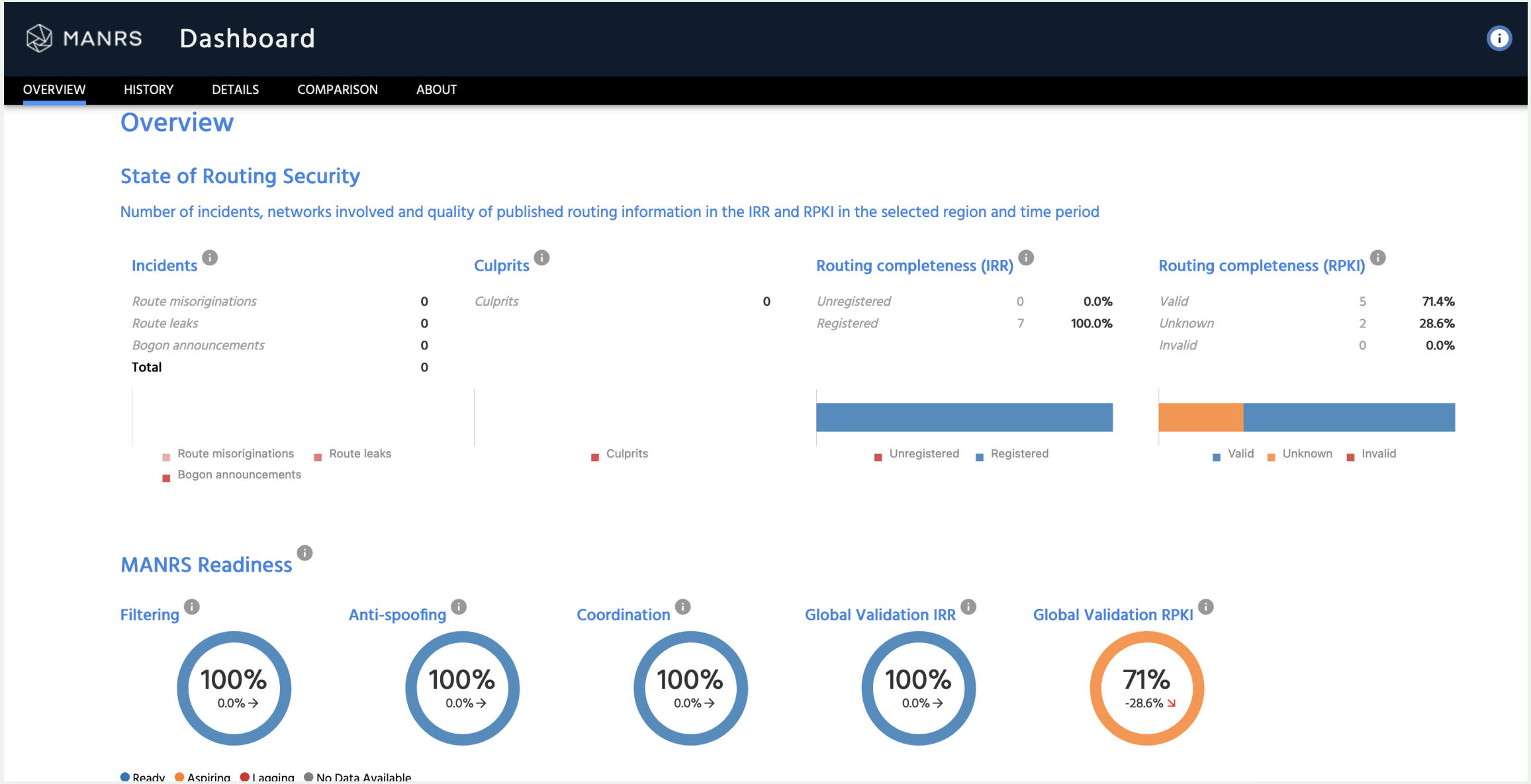
- Organization and governance structure
  - Relationship with ISOC
- Ongoing conformance and strengthening MANRS programmes
  - Improving route incident measurement quality
  - How to address administrative bogons
  - Improving anti-spoofing measurements
  - What is an acceptable level of conformance for sign-up and on an ongoing basis?
  - Regular conformance checks and reporting, including publishing readiness scores
  - Should RPKI become a mandatory action and over what timeframe?
  - Implementing new actions – e.g. ROV?

MANRS Observatory Developments

A lot of work to improve the MANRS Observatory:

- Developing alternative data sources – moving to GRIP (Global Routing Intelligence Platform) to reduce reliance on BGPstream
- Now publishing monthly conformance scores for each participant
- Introducing user management of accounts (updating contacts and details etc…)
- Developing automated application process to improve response times
- Developing improved and more detailed incident analysis

MANRS Observatory



Monthly Reports

Sent to all MANRS Network Operators

Validate incident data -> tune down false positives

Raise awareness of network conformance status

Use as a regular communication channel (e.g. verify Action 3 contacts)

Can be sent to primary + any secondary contacts

MANRS Conformance Report

2022/02/01 - 2022/02/28

ASN

MANRS Readiness Scores

Anti-Spoofing:	**100%**
Coordination:	**100%**
Filtering:	**41%** ↑
Global Validation IRR:	**59%** ↑
Global Validation RPKI:	**3%** ↑

Non-Compliance Incidents

AS Route Misoriginations (BGPStream):	**1**
AS Route Misoriginiations (GRIP):	**2**
Customer Route Hijacks (BGPStream):	**1**
Customer Route Hijacks (GRIP):	**1**

Verify Incidents

MANRS Ambassadors and Fellows Programme

- **Aims to extend outreach and involve the wider Internet community in routing security**
- **Ambassadors** are representatives from current MANRS participants who provide mentorship, guidance, and feedback to others in the routing security community.
- **Fellows** are emerging leaders in their communities, selected after an open call for applications. They're not necessarily representatives of MANRS participant organizations.
- **Tracks:**
  - **Training** – Conduct online tutorials and workshops; help improve existing contents and labs.
  - **Research** – Collect and analyze relevant information on routing incidents; collect feedback from the community.
  - **Policy** – Review documents targeting issues that can be addressed through MANRS actions; help improve existing policy documents for MANRS.

MANRS Ambassadors and Fellows for 2022

See the MANRS website for Ambassadors

See the MANRS website for Fellows

MANRS

MANRS Research

Some new projects:

- **MANRS Conformance Checker** – tool to periodically assess the conformance of MANRS Participants against Action set
- **ROA Historical Explorer** – ability to lookup prefix and provide ROAs covering this within date range, in order to check BGP announcements in the past
- **Blackholing Stats** – allow MANRS Participants to blackhole /25 to /32 of their address space so other participants can null route in order to mitigate DDoS

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov