



MANRS

MANRS Participants Meeting @ RIPE 78

Kevin Meynell

Manager, Technical & Operational Engagement / MANRS Community Builder

meynell@isoc.org

Proposed Agenda

- 1) MANRS Observatory Update & Demo
- 2) Improving the MANRS auditing process
- 3) Next steps towards maintaining and improving MANRS conformance
- 4) Documentation of routing security requirements for peering and connectivity procurements
- 5) Development of MANRS Implementation Guide for IXPs



Some MANRS Statistics

64,420 ASes in routing system

(source: CIDR Report)

~10,000 multi-homed ASes

155 network operators are MANRS participants

279 ASes compliant with most or all MANRS actions

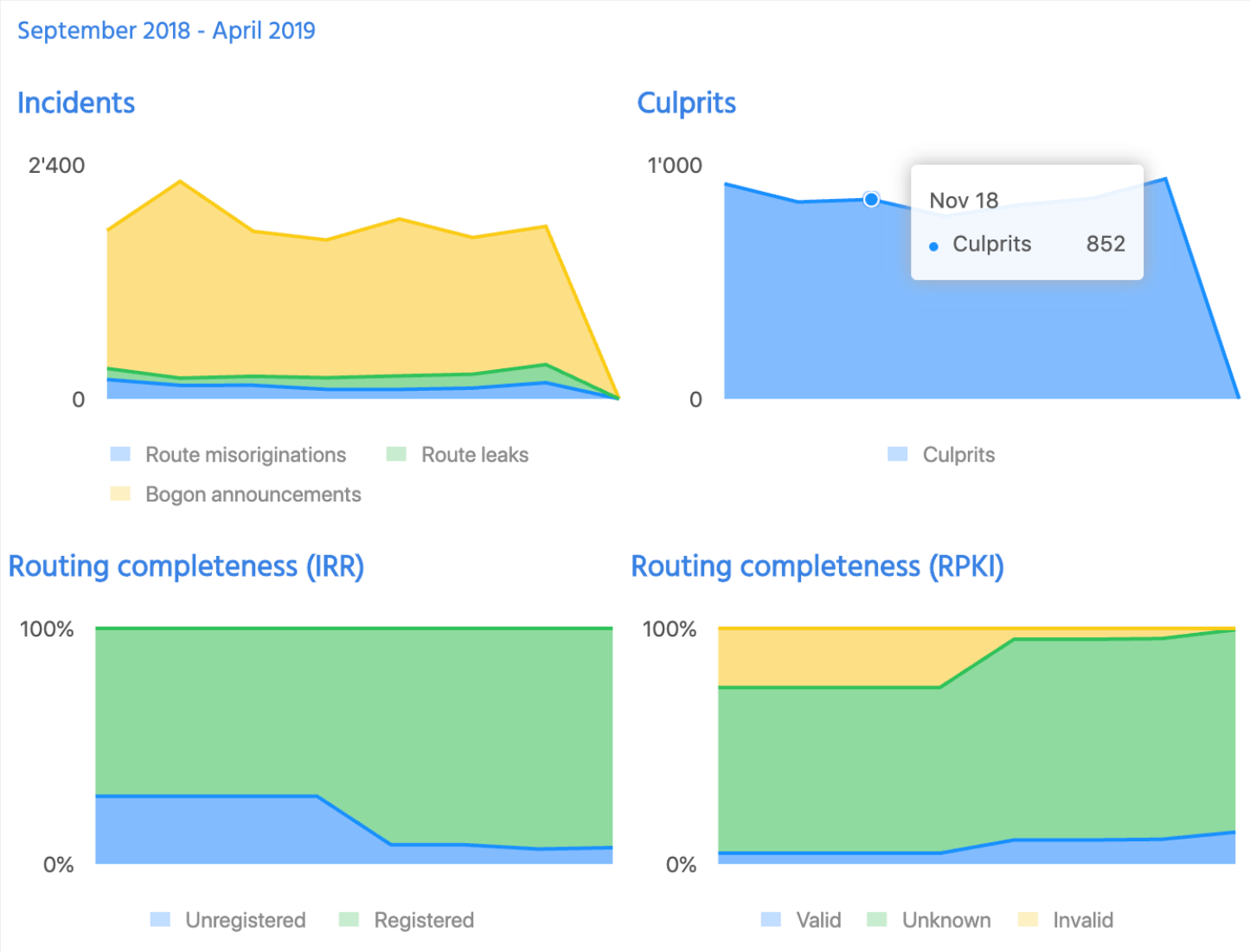
32 IXPs are MANRS participants

10 partners (promotion, capacity building etc..)

(as of May 2019)



Routing Security – is the Problem getting better or worse?



Objectives of the Meeting

- Goal is to establish routing security measures as an industry norm
- Make the MANRS community self-sustaining and self-policing
- Raise awareness of MANRS Observatory as tool to display and monitor conformance
- Development of documentation to aid deployment and procurement
- Opportunity to provide feedback on the MANRS process
- How can the MANRS process be improved and sustained in an ongoing manner?



Improving the MANRS Auditing Process

MANRS applicants are evaluated on conformance with **a majority** of the MANRS actions:

1) Filtering, 2) Anti-Spoofing, 3) Coordination & 4) Global Validation

Current MANRS Action document needs updating to clarify actions and effective criteria

Questions:

- Only Action 3 is compulsory – should this be changed to Actions 1, 3 and 4?
- Action 2 is currently optional - should this be required, and what should *pass criteria* be?
- There are effectively 5 actions: *Routing Completeness (RPKI)*

Not currently evaluated

Should this be Action 5 and what should the *pass criteria* be for this?



Next steps towards maintaining and improving MANRS conformance (talking points)

- MANRS participants are currently audited for conformance with MANRS Actions upon application only
- Some participants will likely not maintain the same levels of conformance over time - how to handle these issues?
- How can recognition of the value of implementing routing security measures be improved?
- Should there be a MANRS trustmark-type approach, linked to ongoing conformance?
- Discuss!



Routing Security Requirements for Peering & Connectivity Procurements

- Is something similar needed to RIPE-554 “Requirements for IPv6 in ICT Equipment” for connectivity procurements?
- Is something similar needed for NANOG IPv6 Peering & Transit BCOP?
- Should routing security measures be specified when arranging peering with another network?
- Should routing security measures be requested when procuring connectivity?
- Any experienced peering and procurement people willing to contribute?
- Can this be developed as RIPE document?



MANRS Implementation Guide for IXPs

- The MANRS Implementation Guide for Network Operators explains how to implement and deploy the MANRS Actions, a BCOP agreed by subject matter experts (ripe-706)
- Something similar needed for IXPs on how to implement these Actions?
- ISOC can provide editor (me), but any subject matter experts willing to contribute content towards this?
- Can also be submitted as RIPE Document



MANRS Implementation Guide for IXPs

MANRS IXP Actions:

Action 1: Use route server to validate route announcements from peers (using IRR and/or RPKI)

Action 2: Encouraging IXP members to employ MANRS (via capacity building, discounting, acclaim)

Action 3: Layer 2 filtering

Action 4: Ensure every member is contactable and responsive in mitigating network incidents

Action 5: Provide monitoring and debugging tools for routing incidents/anomalies (e.g. Looking Glass)



<https://www.manrs.org>

