Mind Your MANRS:

Improving the Security and Resilience of the Global Routing System

Andrei Robachevsky
robachevsky@isoc.org

(Not me!)

www.internetsociety.org

Internet Society

The Internet appears seamless due to trust

- **IP prefixes are learned in BGP from a customer, propagated to all your "peers," who pick the "best" announcement and propagate that path to their customers**
  - **These relationships may span continents**
  - **The reverse path must signal correctly too for the Internet to work and this path may traverse different networks**
- **IP packets are forwarded from one hop to the next hop closer to the destination with minimal inspection**

This trust can break down

- My network accepts an invalid routing announcement which I propagate, my peer decides it is the “best path” and announces it to their customers
- The “best path” was not selected because it can deliver traffic to the destination, but rather for lower cost, “nearest exit”
- Traffic is being discarded, but how does the affected party contact the correct person to fix a problem that may traverse continents?

What is available to improve Internet security?

Tools

- Prefix and AS-PATH filtering, RPKI, IRR, …
- Ingress and egress anti-spoofing filtering, uRPF, …
- Coordination and DDoS mitigation

Challenges

- Your safety is in someone else's hands
- Implementing control plane fixes at just one network to network interface does not resolve the problem
- Technological fixes and mitigation efforts can sometimes break seamless end-to-end forwarding of legitimate traffic

Welcome, Mutually Agreed Norms for Routing Security (MANRS)!

The Internet is successful because of its long history of collaboration.

To stimulate visible security improvements, we need a culture of collective responsibility.

The *Routing Resilience Manifesto*, underpinned by the "Mutually Agreed Norms for Routing Security (MANRS)" document, aims at supporting this goal.

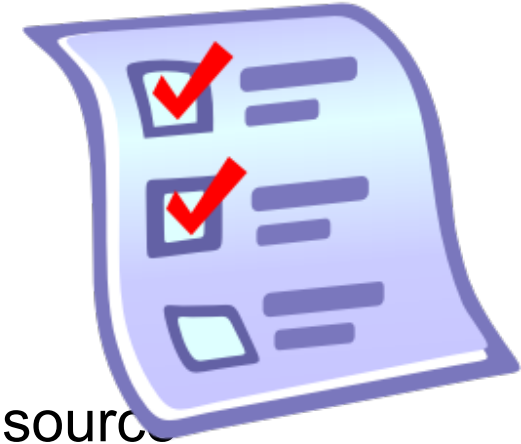
Mutually Agreed Norms for Routing Security (MANRS)

Defines four concrete actions that network operators should implement.

The problem cannot be solved alone - the real effect of the measures depends on how broadly they are adopted.

MANRS tries to merge technology and people together to help craft a solution.

Good MANRS



1. **Filtering –** Prevent propagation of incorrect routing information.
2. **Anti-spoofing –** Prevent traffic with spoofed source IP addresses.
3. **Coordination –** Facilitate global operational communication and coordination between network operators.
4. **Global Validation –** Facilitate validation of routing information on a global scale.

1. Filtering

Prevent propagation of incorrect routing information

Network operator defines a clear routing policy and implements a system that ensures ***correctness*** *of their* ***own announcements*** *and* ***announcements from their customers*** *to adjacent networks with prefix and AS-path granularity.*

Network operator is ***able to communicate*** *to their adjacent networks which announcements are correct.*

Network operator applies due diligence when checking the correctness of their customer's announcements, specifically that the ***customer legitimately holds the ASN and the address space it announces****.*

2. Anti-Spoofing

Prevent traffic with spoofed source IP address

Network operator implements a system that ***enables source address validation*** *for at least* ***single-homed stub customer networks, their own end-users and infrastructure****. Network operator implements anti-spoofing filtering to prevent packets with an incorrect source IP address from entering and leaving the network.*

3. Coordination

Facilitate global operational communication and coordination between the network operators

Network operators should maintain ***globally accessible up-to-date contact information.***

4. Global Validation

Facilitate validation of routing information on a global scale.

*Network operator has **publicly documented routing policy**, ASNs and prefixes that are intended to be advertised to external parties.*

MANRS is a document – and it is a commitment

1) The company **supports the Principles and implements at least one of the Actions** for the majority of its infrastructure. Implemented Actions are marked with a check-box. The Action "Facilitate global operational communication" cannot be the only one and requires that another Action is also implemented.
2) The company becomes a Participant of MANRS, helping to **maintain and improve** the document, for example, by suggesting new Actions and maintaining an up-to-date list of references to BCOPs and other documents with more detailed implementation guidance.

Some history and numbers

Officially launched in November 2014

9 initial participants from across North America and Europe

Now at 25 participants from across the globe

WE NEED YOU!

Next Steps

Expanding the group of participants

- Looking for industry leaders in the region

Expanding the scope of the MANRS

- Raising the bar – defining new Actions

Developing better guidance

- Tailored to MANRS
- In collaboration with existing efforts, like BCOP

Are you interested in participating?

Filtering 

Anti-Spoofing 

Coordination 

Global scale 

http://www.routingmanifesto.org/signup/

https://www.routingmanifesto.org/

https://www.manrs.org/

Internet Society

Technical Q&A with crowd-sourced answers?

Andrei Robachevsky
robachevsky@isoc.org

(Want more details, ask this guy!)

Internet Society