How can we work together to improve security and resilience of the global routing system?

Andrei Robachevsky <robachevsky@isoc.org>

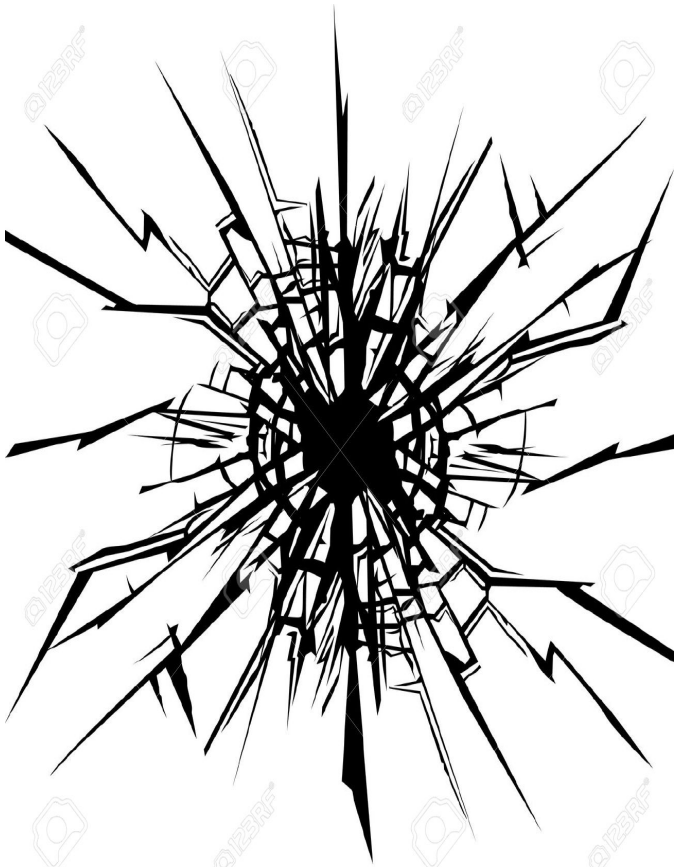
Routing Resilience Manifesto, aka MANRS

https://www.routingmanifesto.org/

https://www.manrs.org/

The problems

- **Prefix hijack**
  - **Denial of service, impersonating a network or a service, traffic intercept**
- **“Route leak”**
  - **Traffic intercept, but may result in denial of service**
- **IP spoofing**
  - **The root cause of reflection DDoS attacks**



What is available to address these problems?

- **Building blocks, but not solutions**
  - **Prefix and AS-PATH filtering, RPKI, IRR, …**
  - **BGPSEC under development at the IETF**
  - **Ingress and egress anti-spoofing filtering, uRPF, …**
  - **Whois, Routing Registries and Peering databases**

Challenges

- **Your network security is in someone else's hands. Securing just one individual network does not make it more secure.**

- **Too many problems to solve, too many cases. Is there a clear, visible and industry supported line between good and bad?**

Mutually Agreed Norms for Routing Security (MANRS)

MANRS builds a visible community of security-minded operators

- **Promotes culture of collaborative responsibility**

Defines four concrete actions that network operators should implement

- **Technology-neutral baseline for global adoption**

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.

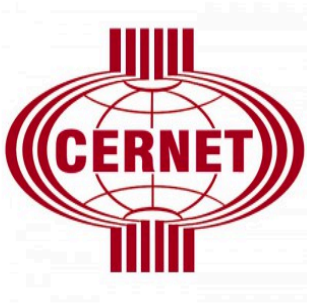
*Network operator has **publicly documented routing policy**, ASNs and prefixes that are intended to be advertised to external parties.*

MANRS is not (only) a document – it is a commitment

1) The company supports the Principles and implements at least one of the Actions for the majority of its infrastructure.

2) The company becomes a Participant of MANRS, helping to maintain and improve the document and to promote MANRS objectives

Public launch of the initiative - 6 November 2014



A growing list of participants

	Country	ASNs	Filtering	Anti-spoofing	Coordination	Global Validation
KPN	NL	1136, 5615, 8737	✓	✓	✓	✓
Seeweb	IT	12637	✓	✓	✓	✓
Gigas	ES, US	57286, 27640	✓	✓	✓	✓
NTT	US	2914	✓	✓	✓	✓
BIT BV	NL	12859	✓	✓	✓	✓
Algar Telecom	BR	16735, 53006, 27664	✓		✓	✓
OpenCarrier eG	DE	41692		✓	✓	✓
SpaceNet	DE	5539	✓	✓	✓	✓
CERNET	CN	4538	✓		✓	✓
SpeedPartner GmbH	DE	34225	✓	✓	✓	✓
Comcast	US	7015, 7016, 7725, 7922, 11025, 13367,	✓	✓	✓	✓

Current Activities

- **Expanding the group of participants**
  - **Looking for industry leaders in the region**
- **Building a community around MANRS**
  - **A trusted mailing list, possible other activities**
- **Developing better guidance**
  - **Tailored to MANRS**
  - **In collaboration with existing efforts, like BCOP**

Are you interested in participating?

Filtering 

Anti-Spoofing 

Coordination 

Global scale 

I suspect some of you are asking yourself

My company has always taken security seriously, we've implemented many of the Actions and much more long time ago…

- Why joining MANRS now? What difference will it make?

Is any of these a good reason?

Because routing security is a sum of all contributions

Because this is a way to demonstrate a new baseline

Because a community has gravity that can attract others

MANRS is not a firewall

- **But it is a tool that can lead to better overall security and resilience of the routing system**
- **MANRS as a reference point**
- **MANRS as a platform you can build related activities**

What the participants say

We believe the security, stability, and resiliency of the Internet operation can be improved via distributed and shared responsibilities as documented in MANRS. As one of the largest academic networks in the world, CERNET is committed to the MANRS actions. Xing Li, Deputy Director, CERNET

Adherence to MANRS is an important commitment that operators make back to the Internet community. Together we aim to remove the havens from which miscreants maintain the freedom and anonymity to attack our network and our customers. David Freedman, Claranet Group

Comcast is committed to helping drive improvements to the reliability of the Internet ecosystem. We are thrilled to be engaged with other infrastructure participants across the spectrum and around the globe in pursuit of these goals. Jason Livingood, Vice President, Internet Services, Comcast

Cogent supports the efforts championed by the MANRS document. The issues being promoted need practical, effective improvements to support the continued growth and reliance on the Internet. Hank Kilmer, Cogent

Workonline implements the recommendations contained in the MANRS document by default. By publicly stating the measures that we take to ensure the robustness of our network, we hope to encourage our customers and peers to do the same. Ben Maddison, Director - Network Operations' Strategy, Workonline Communications (Pty) Ltd

https://www.routingmanifesto.org/

https://www.manrs.org/