Mutually Agreed Norms for Routing Security (MANRS)

aka
Routing Resilience Manifesto

IXP Workshop Paraguay

November 2014

The MANRS

- https://www.routingmanifesto.org/manrs/
- **Defines a minimum package**
- **Emphasizes collective focus**

> *"While the mass media often create awareness-knowledge of an innovation, interpersonal communication with peers is necessary to persuade most individuals to adopt a new idea"*
> *(Rogers & Kincaid, 1981).*

Collective responsibility and collaboration for routing resilience and security

- **Raise awareness and encourage actions by demonstrating commitment of the growing group of supporters**
- **Demonstrate industry ability to address complex issues**
- **Clear and tangible message:**

  "We do at least this and expect you to do the same"

The MANRS, in more detail

- **Principles of addressing issues of routing resilience**
  - **Interdependence and reciprocity (including collaboration)**
  - **Commitment to Best Practices**
  - **Encouragement of customers and peers**
- **“The package” indicating the most important actions**
  - **BGP Filtering**
  - **Anti-spoofing**
  - **Coordination and collaboration**
- **High-level document specifying “what”**
  - **“How” is in external documents (e.g. BCPs)**

Principles

1) The organization (ISP/network operator) **recognizes** the **interdependent nature** of the global routing system and its **own role** in contributing to a secure and resilient Internet

2) The organization **integrates best current practices** related to routing security and resilience in its network management processes in line with the Actions

3) The organization is **committed** to preventing, detecting and mitigating routing incidents through **collaboration and coordination** with peers and other ISPs in line with the Actions

4) The organization **encourages its customers and peers** to adopt these Principles and Actions

Good MANRS

1. **Prevent propagation of incorrect routing information**
2. **Prevent traffic with spoofed source IP address**
3. **Facilitate global operational communication and coordination between the network operators**

Actions (1)

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****.*

Actions (2)

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.*

Actions (3)

Facilitate global operational communication and coordination between the network operators

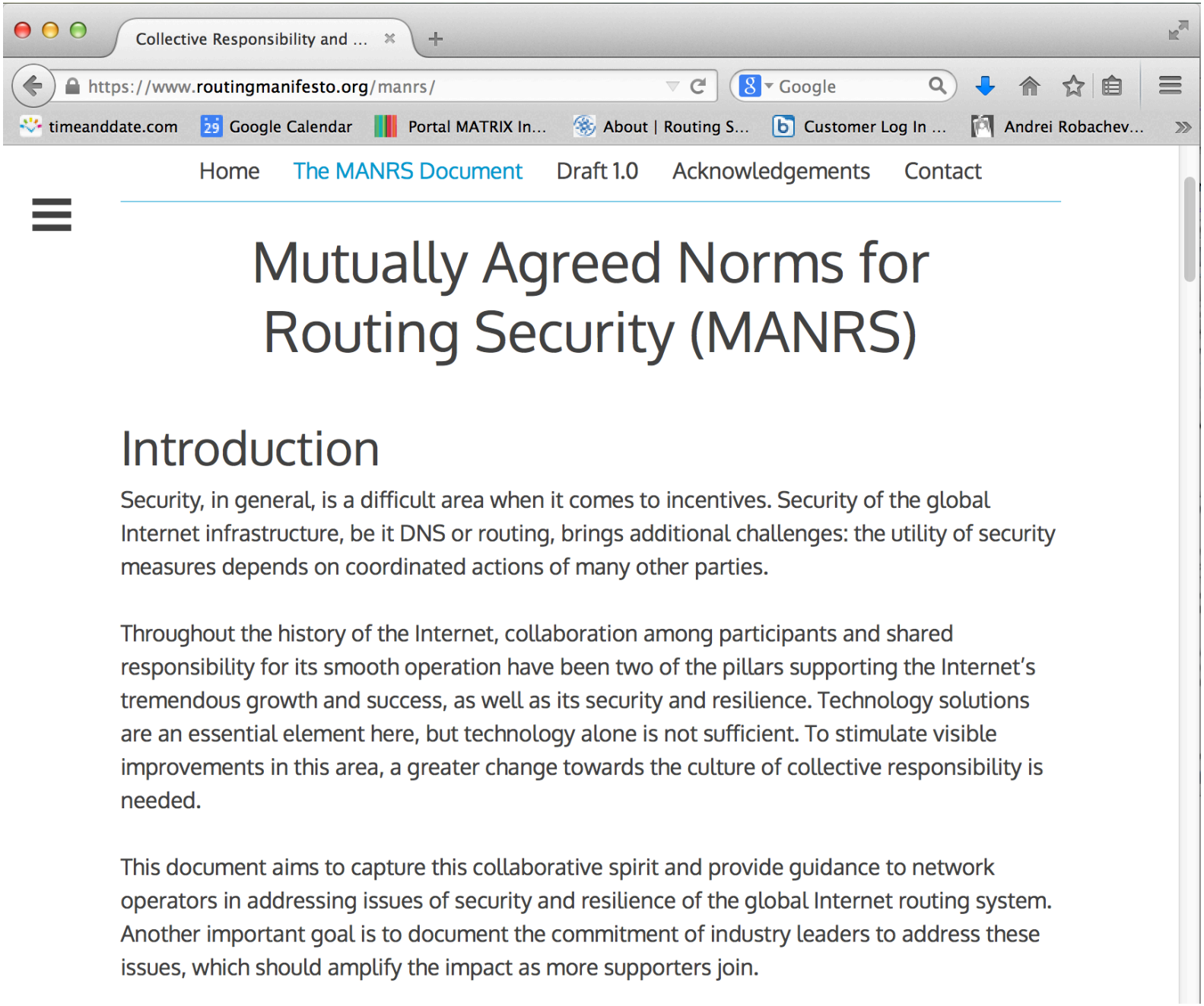
Network operators should maintain ***globally accessible up-to-date contact information.***

Actions (4)

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.*

•


Collective Responsibility and ...
https://www.routingmanifesto.org/manrs/
Google
timeanddate.com
Google Calendar
Portal MATRIX In...
About | Routing S...
Customer Log In ...
Andrei Robachev...
Home
The MANRS Document
Draft 1.0
Acknowledgements
Contact
Mutually Agreed Norms for Routing Security (MANRS)
Introduction
Security, in general, is a difficult area when it comes to incentives. Security of the global Internet infrastructure, be it DNS or routing, brings additional challenges: the utility of security measures depends on coordinated actions of many other parties.
Throughout the history of the Internet, collaboration among participants and shared responsibility for its smooth operation have been two of the pillars supporting the Internet's tremendous growth and success, as well as its security and resilience. Technology solutions are an essential element here, but technology alone is not sufficient. To stimulate visible improvements in this area, a greater change towards the culture of collective responsibility is needed.
This document aims to capture this collaborative spirit and provide guidance to network operators in addressing issues of security and resilience of the global Internet routing system. Another important goal is to document the commitment of industry leaders to address these issues, which should amplify the impact as more supporters join.

Work in Progress

- Draft document was published
- Feedback was collected and discussed
- Final version has been produced
- Redesigning the site for the launch

Participating in the Manifesto

1) The company **supports the Principles and implements at least one of the Expected Actions** for the majority of its infrastructure. Implemented Actions are marked with a check-box.

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.

3) This category is for network operators, or other entities acting in this role (e.g. a network equipment vendor, running its own network infrastructure)

Are you interested in participating?

Filtering	Anti-Spoofing	Coordination	Global scale
			

http://www.routingmanifesto.org/

robachevsky@isoc.org