MANRS

LACNIC

MANRS LACNIC intro

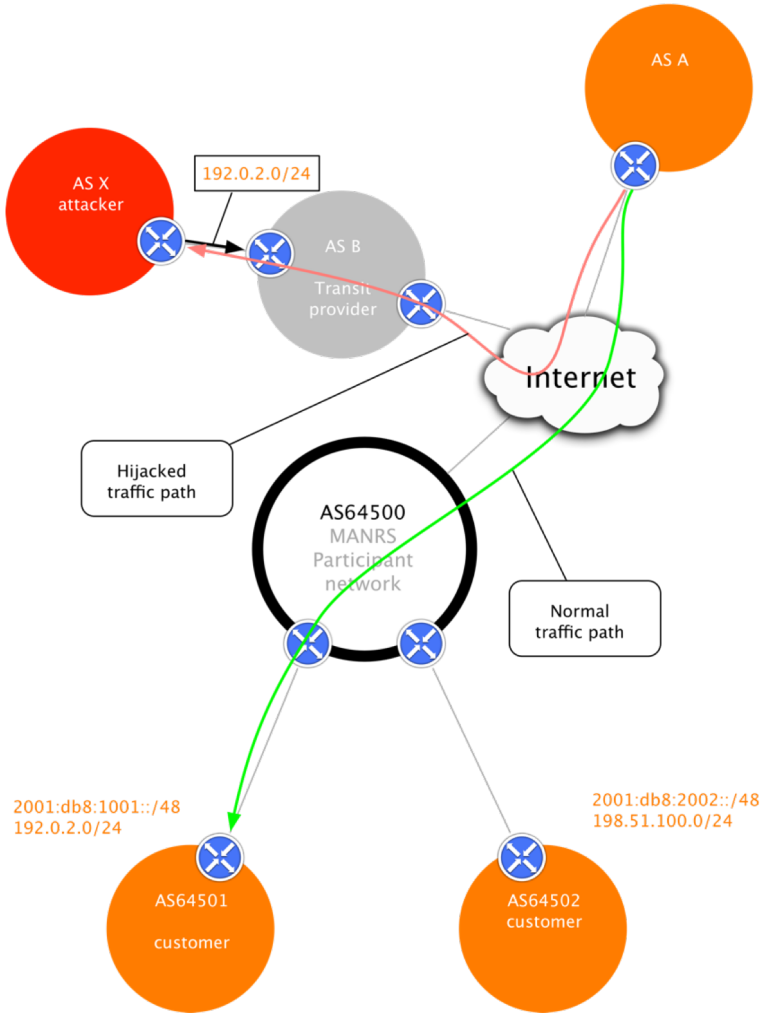
Junio 2019

No Security by Design

- When the Internet was developed, they didn’t build in security by design.
- The objective was resilience, simplicity and ease of deployment
- That created the Internet as the best effort, interdependent, general purpose network of networks supporting permission-less innovation.
- **While these qualities have made the Internet so successful, they also contribute to many of its security issues.**

The Honor System: Routing Issues

- Border Gateway Protocol (BGP) is based entirely on trust between networks
- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data



- DESTINATIONS / ANNOUNCEMENTS
- REACHABILITY
- FORWARDING

MANRS

What problems are we trying to mitigate: Routing incidents

Event	Explanation	Repercussions	Example
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	*The 2008 YouTube hijack*
Route Leak	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for traffic inspection and reconnaissance.	*September 2014. VolumeDrive began announcing to Atrato nearly all the BGP routes it learned from Cogent causing disruptions to traffic in places as far-flung from the USA as Pakistan and Bulgaria.*
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.	The root cause of reflection DDoS attacks	*March 1, 2018. Memcached 1.3Tb/s reflection-amplificationattack reported by Akamai*

MANRS

How can MANRS actions prevent incidents:

- MANRS defines four simple but concrete actions that network operators must implement to improve Internet security and reliability.
- The first two operational improvements eliminate the root causes of common routing issues and attacks, while the second two procedural steps improve mitigation and decrease the likelihood of future incidents.

- MANRS builds a visible community of security minded network operators and IXPs

MANRS

How can MANRS actions prevent incidents: MANRS Actions

- ## 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 common routing databases

- ## Global Validation

  Facilitate validation of routing information on a global scale

  - Publish your data, so others can validate

MANRS

Where are those actions configured and how users are protected?

- Actions 1 BGP configuration
  - core network team
  - network planning & engineering
  - Prevents route leaks & Hijacking
- Action 2 RPF & packet filtering
  - user port configuration
  - service delivery team, process and BCOP implementation
  - DDoS impact
- Action 3 (core team socialization)
- Action 4 core team
  - IRR
  - LACNIC on RPKI

MANRS

How to contribute to MANRS in your country

- Identify networks not following BCOPS
  - Usually involved in security incidents
  - Reported in CAIDA spoofer or rpki violations
  - Networks not present in peering db, whois or IRR
- Help them
  - Promote NOGs, IXPs, NRENS, operational communities
  - Refer them to MANRS.org
  - Engage them in LACNOG
- Generating awareness regarding routing incidents (reports, presentations, surveys, etc)
- There are tools available

MANRS

MANRS resources

Christian O'Flaherty – Internet Society

MANRS Training Modules

Module 1: Introduction to MANRS

What is MANRS, and why should you join? MANRS is a global initiative to implement crucial fixes needed to eliminate the most common routing threats. In this module you will learn about vulnerabilities of the Internet routing system and how four simple steps, called MANRS Actions, can help dramatically improve Internet security and reliability.

Module 2: IRRs, RPKI, and PeeringDB

This module helps you understand the databases and repositories MANRS participants should use to document routing policy and maintain contact information. You'll learn what database objects to use to document routing information related to your network and how to register information in the RPKI system. Finally, you will learn how to use the Peering DB and other databases to publish your contact information.

Module 3: Global Validation: Facilitating validation of routing information on a global scale

In this module, you will learn how to prevent incorrect routing announcements from your customers and your own network. The module explains how filters can be built, including the tools used to build them. It also shows how to signal to other networks which announcements from the network are correct.

Module 4: Filtering: Preventing propagation of incorrect routing information

This module will help you apply anti-spoofing measures within your network. After this module you will be able to identify points/devices in the network topology where anti-spoofing measures should be applied, identify adequate techniques to be used (for example, uRPF, or ACL filtering), configure your devices to prevent IP spoofing, and verify that the protection works.

Module 5: Anti-Spoofing: Preventing traffic with spoofed source IP addresses

This module is to understand how to create and maintain contact information in publicly accessible places. It explains why it is important to publish and maintain contact information, how to publish contact information to Regional Internet Registries (RIRs), Internet Routing Registries (IRRs), and PeeringDB, and what contact information you should publish to a company website.

Module 6: Coordination: Global communication between network operators

This module helps you understand how to enable others to validate route announcements originating from your network by documenting a Network Routing Policy. You'll learn what a Network Routing Policy is, how to document your organization's Network Routing Policy and make it publicly available in order to signal to other networks which announcements from your network are correct.

MANRS Implementation Guide

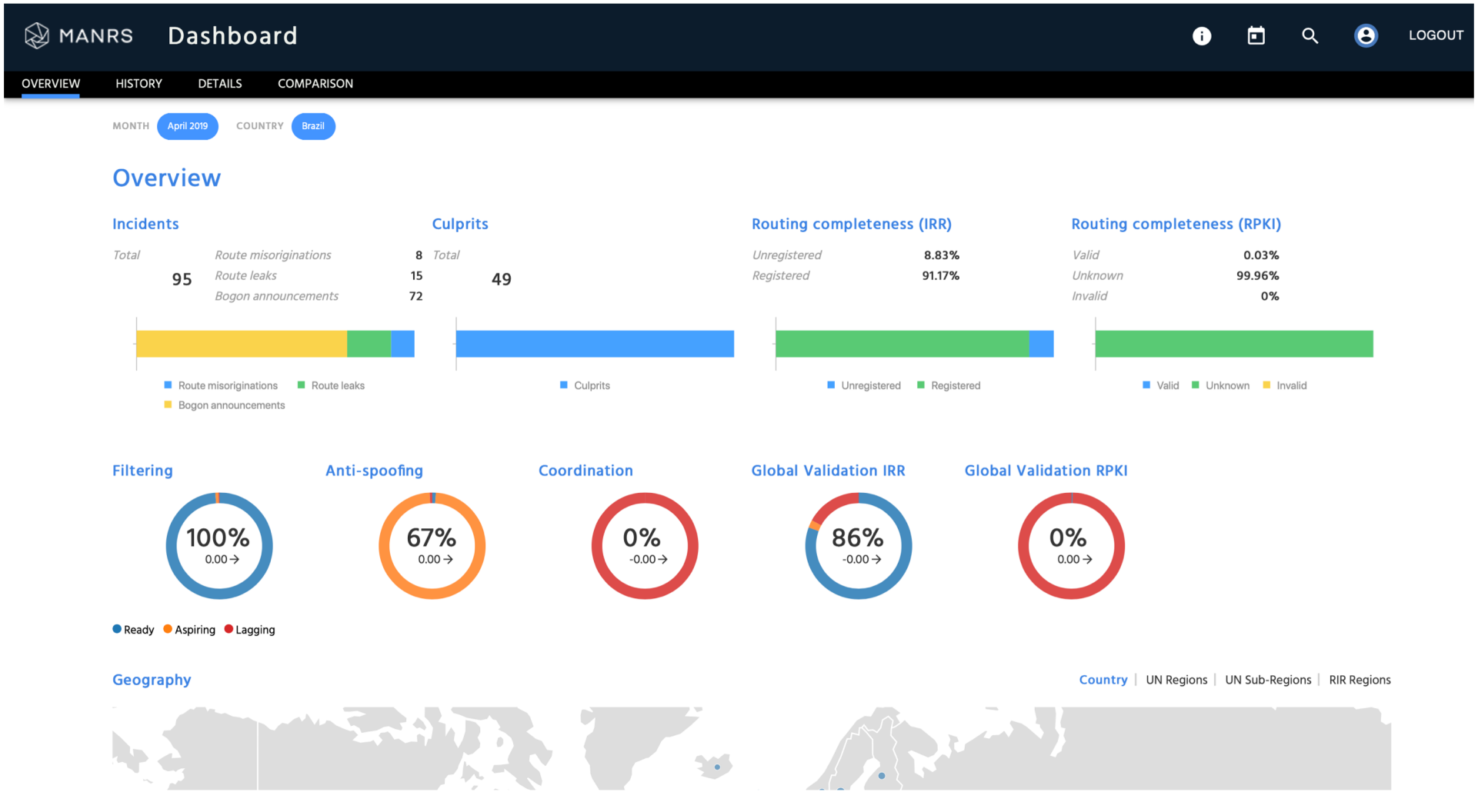
- If you're not ready to join yet, implementation guidance is available to help you.
- Based on Best Current Operational Practices deployed by network operators around the world
- https://www.manrs.org/bcop/

Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Version 1.0, BCOP series
Publication Date: 25 January 2017

MANRS

MANRS observatory



MANRS

How to use MANRS information

- Where is the information available ?
  - BGP Stream https://bgpstream.com
  - Caida Report http://www.caida.org/data/overview/
  - RIPE Stat
  - CAIDA Spoofer Project https://www.caida.org/projects/spoofer/
  - Peeringdb https://peeringdb.com
  - Whois.[RIR].net
  - lacnic rpki, IRRs
    - Radb, RIPE, Level3, etc.
    - https://rpki.lacnic.net
- MANRS observatory https://observatory.manrs.org/

MANRS

MANRS IXPP

MANRS IXP Partnership Programme

- There is synergy between MANRS and IXPs
- IXPs form a community with a common operational objective
- MANRS is a reference point with a global presence – useful for building a “safe neighborhood”

- How can IXPs contribute?
- Technical measures: Route Server with validation, alerting on unwanted traffic, providing debugging and monitoring tools
- Social measures: MANRS ambassadors, local audit as part of the on-boarding process
- A development team is working on a set of useful actions

Acciones para el IXPP

- **Acción 1. Facilitar la prevención de la propagación de información de enrutamiento incorrecta. (Obligatorio)**
  - El IXP implementa el filtrado de anuncios de ruta en el route server usando IRR y / o RPKI. Los anuncios no válidos se filtran de acuerdo con la política publicada de IXP.
- **Acción 2. Promover MANRS entre los miembros del IXP. (Obligatorio)**
  - El IXP promueve o prove asistencia para que los miembros implementen las acciones de MANRS. (Hay 4 casillas de verificación separadas para diferentes niveles de incentivos, se debe verificar una o más).

Acciones para el IXPP

- **Acción 3. Proteger la plataforma de peering.**
  - El IXP tiene una política publicada de tráfico no permitido en el switch de peering y realiza el filtrado de dicho tráfico. (higiene de capa 2)
- **Acción 4. Facilitar la comunicación y coordinación operativa global entre los operadores de red.**
  - El IXP y cada uno de sus miembros tienen al menos una dirección de correo electrónico válida y activa y un número de teléfono que otros miembros pueden usar para casos de abuso, seguridad e incidentes operacionales.
- **Acción 5. Proporcionar herramientas de monitoreo y depuración a los miembros.**
  - El IXP proporciona un looking glass para sus miembros.

MANRS

MANRS is a community effort

Message to Network Operators:

”Your security is in someone else’s hands. The actions of others directly impact you and your network security (and vice versa)”

QUESTIONS?

oflaherty@isoc.org

MANRS

Q&A

Lucimara Desidera – NIC.br
Christian O'Flaherty – Internet Society – oflaherty@isoc.org

Junio 2019