24 May 2018

MANRS

Mutually Agreed Norms for Routing Security

Kevin Meynell
Manager, Technical & Operational Engagement
meynell@isoc.org

Internet Society © 1992–2018

The Problem

A Routing Security Overview

The Basics: How Routing Works

There are ~61,000 networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks.

Routers use Border Gateway Protocol (BGP) to exchange “reachability information” - networks they know how to reach.

Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path.

The Routing Problem

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

MANRS

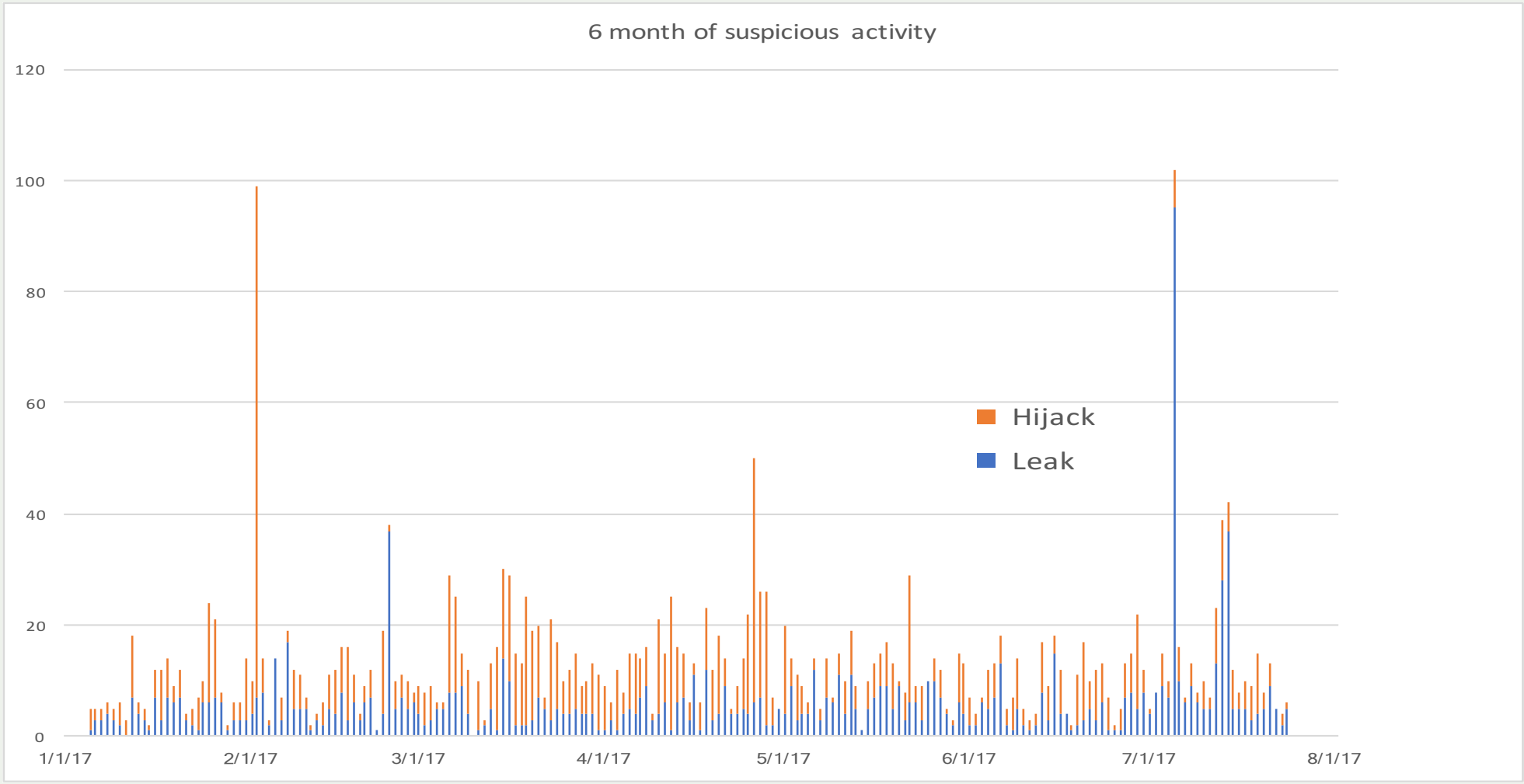
Routing Incidents are Increasing

In 2017 alone, 14,000 routing outages or attacks – such as hijacking, leaks, and spoofing – led to a range of problems including stolen data, lost revenue, reputational damage, and more.

About 40% of all network incidents are *attacks*, with the mean duration per incident lasting 19 hours.

Incidents are global in scale, with one operator's routing problems cascading to impact others.

No Day Without an Incident



http://bgpstream.com/

MANRS

Which Leads To …

MANRS

The Threats: What's Happening?

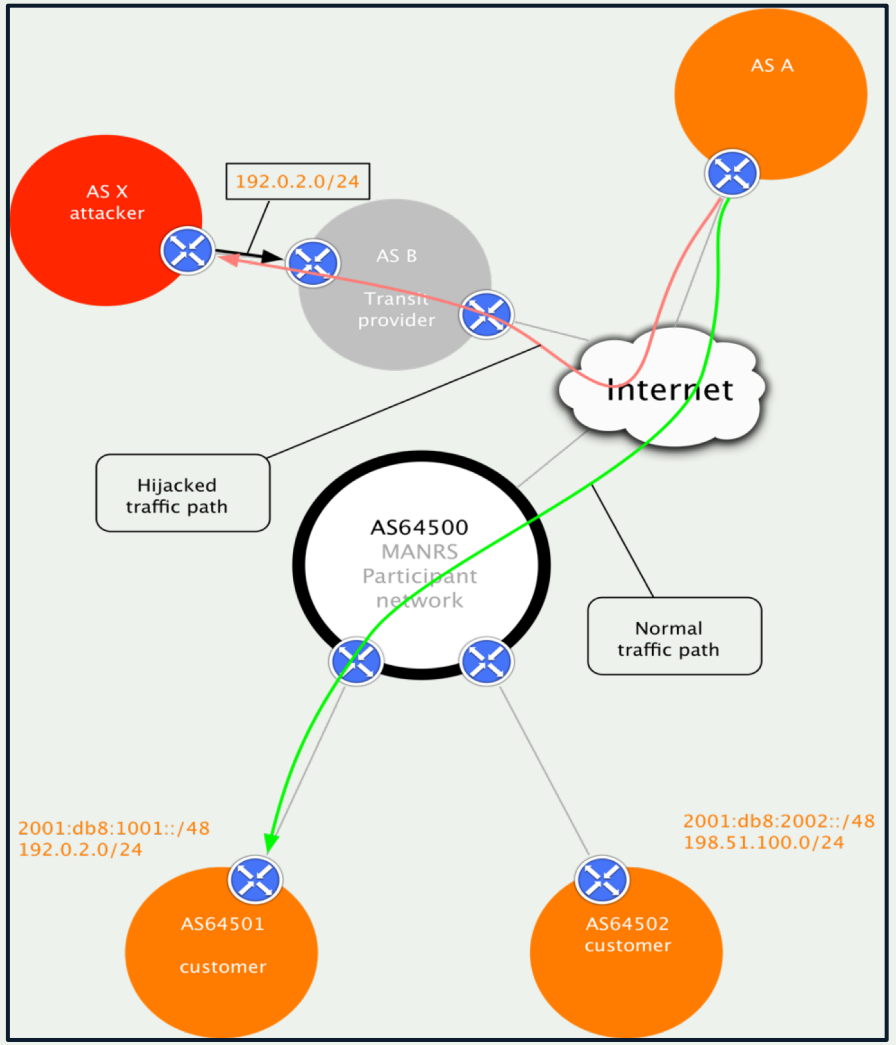
Event	Explanation	Repercussions	Solution
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	Stronger filtering policies
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.	Stronger filtering policies
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	Source address validation

Prefix/Route Hijacking

Route hijacking, also known as “BGP hijacking” when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretending that a server or network is their client. This routes traffic to a network operator, when another real route is available.

Example: The 2008 YouTube hijack; an attempt to block YouTube through route hijacking led to much of the traffic to YouTube being dropped around the world.

Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting false announcements).

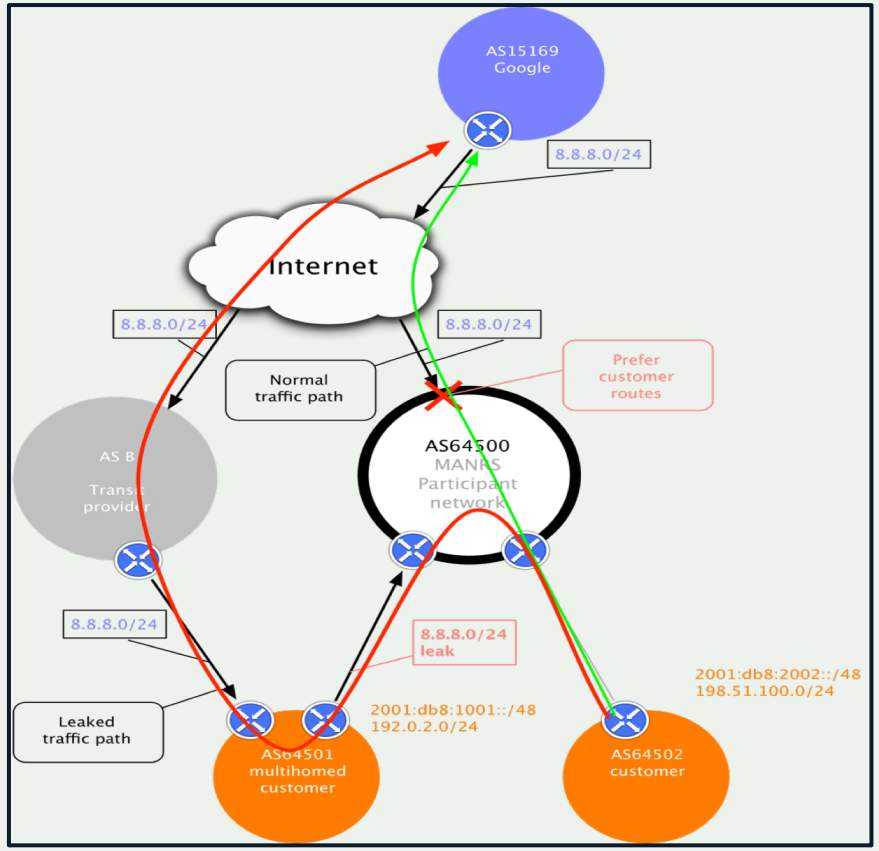


MANRS

Route Leak

A route leak is a problem where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that is has a route to a destination through the other upstream provider. This makes the network an intermediary network between the two upstream providers. With one sending traffic now through it to get to the other.

Example: 2015, Malaysia Telecom and Level 3, a major backbone provider. Malaysia Telecom told one of Level 3's networks that it was capable of delivering traffic to anywhere on the Internet. Once Level 3 decided the route through Malaysia Telecom looked like the best option, it diverted a huge amount of traffic to Malaysia Telecom.



Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting announcements that don't make sense).

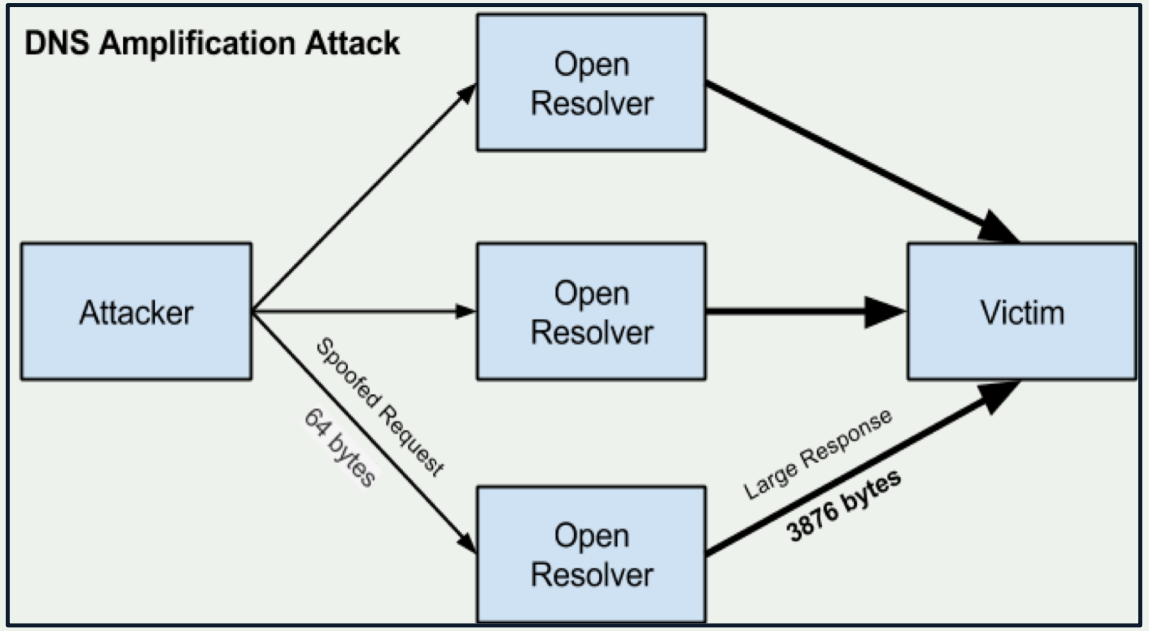
MANRS

IP Address Spoofing

IP address spoofing is used to hide the true identity of the server or to impersonate another server. This technique can be used to amplify an attack.

Example: DNS amplification attack. By sending multiple spoofed requests to different DNS resolvers, an attacker can prompt many responses from the DNS resolver to be sent to a target, while only using one system to attack

Fix: Source address validation: systems for source address validation can help tell if the end users and customer networks have correct source IP addresses (combined with filtering).



MANRS

Are there Solutions?

Yes…

- Prefix and AS-PATH filtering
- RPKI validator, IRR toolset, IRRPT, BGPQ3
- BGPSEC is standardized

But…

- Not enough deployment
- Lack of reliable data

We need a standard approach

MANRS

We Are In This Together

Network operators have a responsibility to ensure a globally robust and secure routing infrastructure.

Your network's safety depends on a routing infrastructure that weeds out bad actors and accidental misconfigurations that wreak havoc on the Internet.

The more network operators work together, the fewer incidents there will be, and the less damage they can do.

MANRS

Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to eliminate the most common routing threats

MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure.

Mutually Agreed Norms for Routing Security

MANRS defines four simple but concrete actions that network operators must implement to dramatically 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.

IANR

MANRS

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*

Everyone benefits from improved Routing Security

Joining MANRS means joining a community of security-minded network operators committed to making the global routing infrastructure more robust and secure.

Heads off routing incidents, helping networks readily identify and address problems with customers or peers.

Consistent MANRS adoption yields steady improvement, but we need more networks to implement the actions and more customers to demand routing security best practices.

The more network operators apply MANRS actions, the fewer incidents there will be, and the less damage they can do.

MANRS is an Important Step

Security is a process, not a state. MANRS provides a structure and a consistent approach to solving security issues facing the Internet.

MANRS is the minimum an operator should consider, with *low risk* and *cost-effective* actions.

MANRS is not a one-stop solution to all of the Internet's routing woes, but it is an important step toward a globally robust and secure routing infrastructure

MANRS

Why should CSIRTs get involved?

- You have a role in risk analysis, threat mitigation, and education/training
  - Ensure network operators, network admins, and technical management are aware of routing security issues
  - MANRS is looking to partner with training providers to include routing security in curriculum
- To demonstrate security proficiency and commitment to your constituency
  - Promote MANRS compliance to security-focused customers
- To add competitive value and enhance operational effectiveness
  - Growing demand from customers for managed security services
  - Customers increasing willing to pay more for secure services
- To help solve global network problems
  - Lead by example, encourage good operational practices, and help weed out bad actors
  - Being part of the MANRS community can strengthen enterprise security credentials

TF-CSIRT & MANRS

- **MANRS Participants**
  - Orange Polska (AS 5617)
  - GEANT (AS 21320/20965)
  - KPN (AS 286/1136/5615/8737)
  - RIPE NCC (AS 3333)
  - Karlsruhe Institute of Technology (AS 34878/58069/20480)
  - NORDUnet (AS 2603)
  - SURFnet (AS 1103)
  - SUNET (AS 1653)
  - TDC (AS 3292)

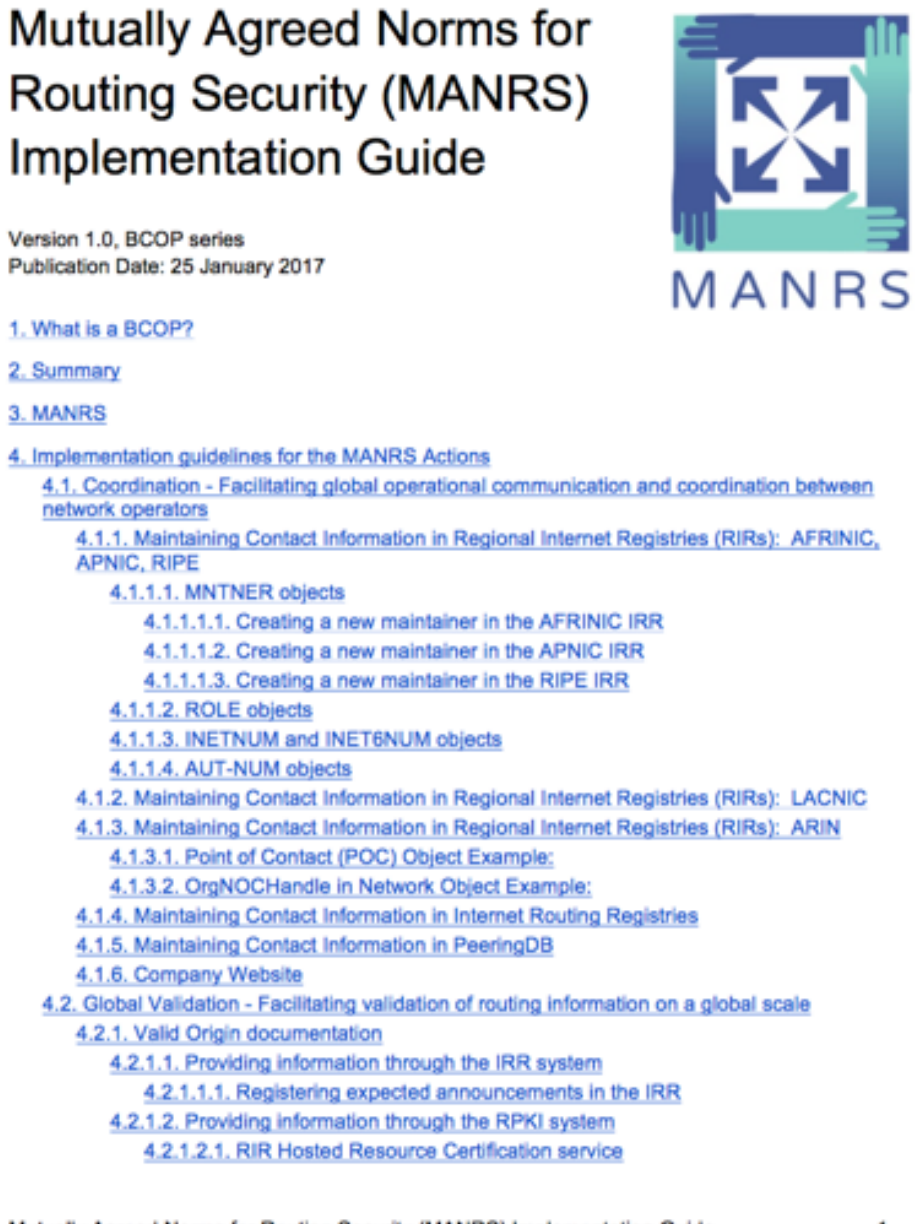
How to Implement MANRS

Documentation, Training & Tools

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

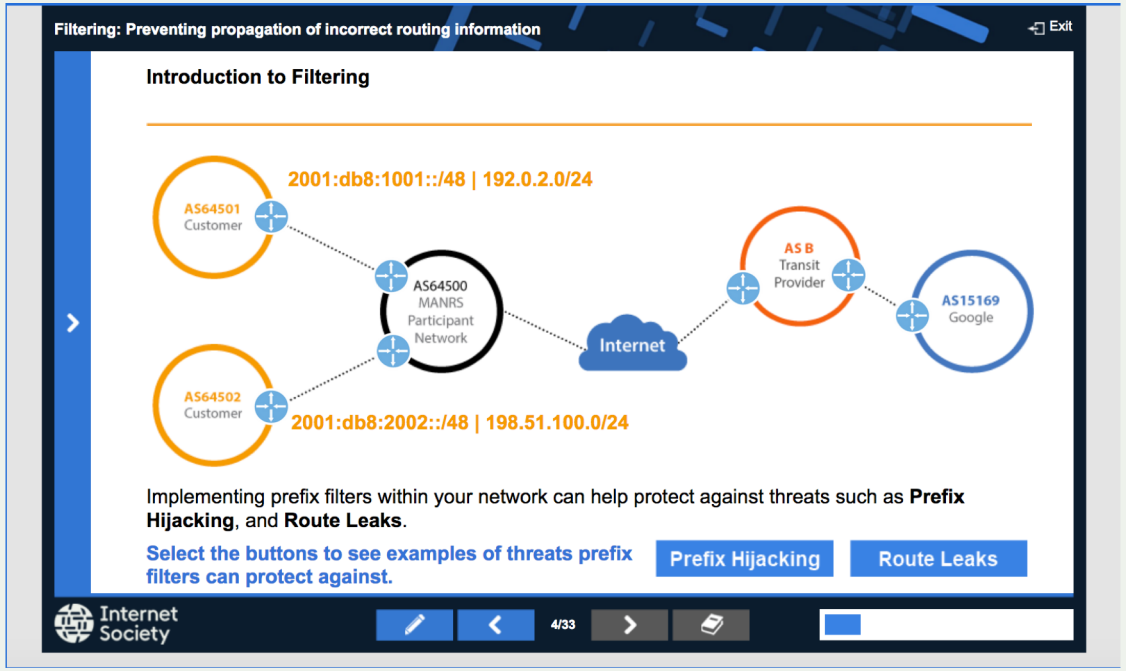
MANRS Training Modules

6 training modules based on information in the Implementation Guide

Walks through the tutorial with a test at the end of each module

Working with and looking for partners that are interested in integrating it in their curricula

https://www.manrs.org/tutorials



Measuring Routing Security: MANRS Observatory

- Impartial benchmarking of MANRS members to improve reputation and transparency
- Provide factual state of security and resilience of Internet routing system over time
- Support the problem statement with data
- Self-assessment purposes and automating sign-up
- How to Measure?
  - Transparent - Use publicly available data sources and open source code
  - Passive - No cooperation is required from a network
  - Metrics - Measure the rate of member (ASN) commitment (0 – non-compliant to 100 – fully compliant)

MANRS Observatory: What to Measure?

Metric	Description
M1	# prefixes leaked by a member AS * duration of the incident
M2	# prefixes hijacked by a member AS * duration of the incident
M1C	# prefixes leaked by a customer and not filtered by a member AS * duration of the incident
M2C	# prefixes hijacked by a customer and not filtered by a member AS * duration of the incident
M3	# of bogon prefixes (unallocated IP space) * duration of the incident
M3C	# of bogon prefixes (unallocated IP space) not filetres by a member AS * duration of the incident
M4	# of bogon ASNs (unallocated/reserved) * duration of the incident
M4C	# of bogon ASNs (unallocated/reserved) not filetres by a member AS * duration of the incident
M5	spoofing IP blocks * duration
M5C	spoofing IP blocks of client ASNs (?)
M6	IRR policy (aut-num w/import/export, as-set)
M7IRR	registered customer routes (% of routes registered)
M7RPKI	valid ROAs for customer routes (% of routes registered)
M8	contact registration (RIR, IRR, PeeringDB)
M9	contact responsiveness (active ?)

MANRS

MANRS Observatory: What to Report?

- **Long-term historical data and trends**
  - Region/Economy/Network (AS)
  - Something similar to https://radar.qrator.net/as3333

- **Health of Internet routing**
  - Begin with a couple of metrics, normalized/unnormalised
  - Something similar to http://stats.cybergreen.net/

MANRS Observatory Timeline

- Next week — Sample report with limited set of metrics
- Now – Q3 — Development of the software package with NLNetLabs
- Q3 — Implement MANRS Observatory and dashboard (pilot)
- Q3 – Q4 — Feedback and enhancement by MANRS members

MANRS ‘Ambassadors’

Overview

What is a MANRS ‘Ambassador’?

MANRS should be (and is) a collaborative initiative of Internet operators

- Internet operators undertaking MANRS principles need to encourage use of best practices
- A MANRS ‘ambassador’ is is an opinion leader in his/her community who strongly believes that routing security is an essential component for the future well being of the Internet
- Generate MANRS awareness through word-of-mouth, presentations and social media in their communities
- Bring forward feedback and recommendations for improving MANRS principles, tools and disseminating best practices, e.g. MANRS observatory, network monitoring tools, and training materials
- Internet Society can help with presentations, informational materials and merchandise (shirts and stickers)

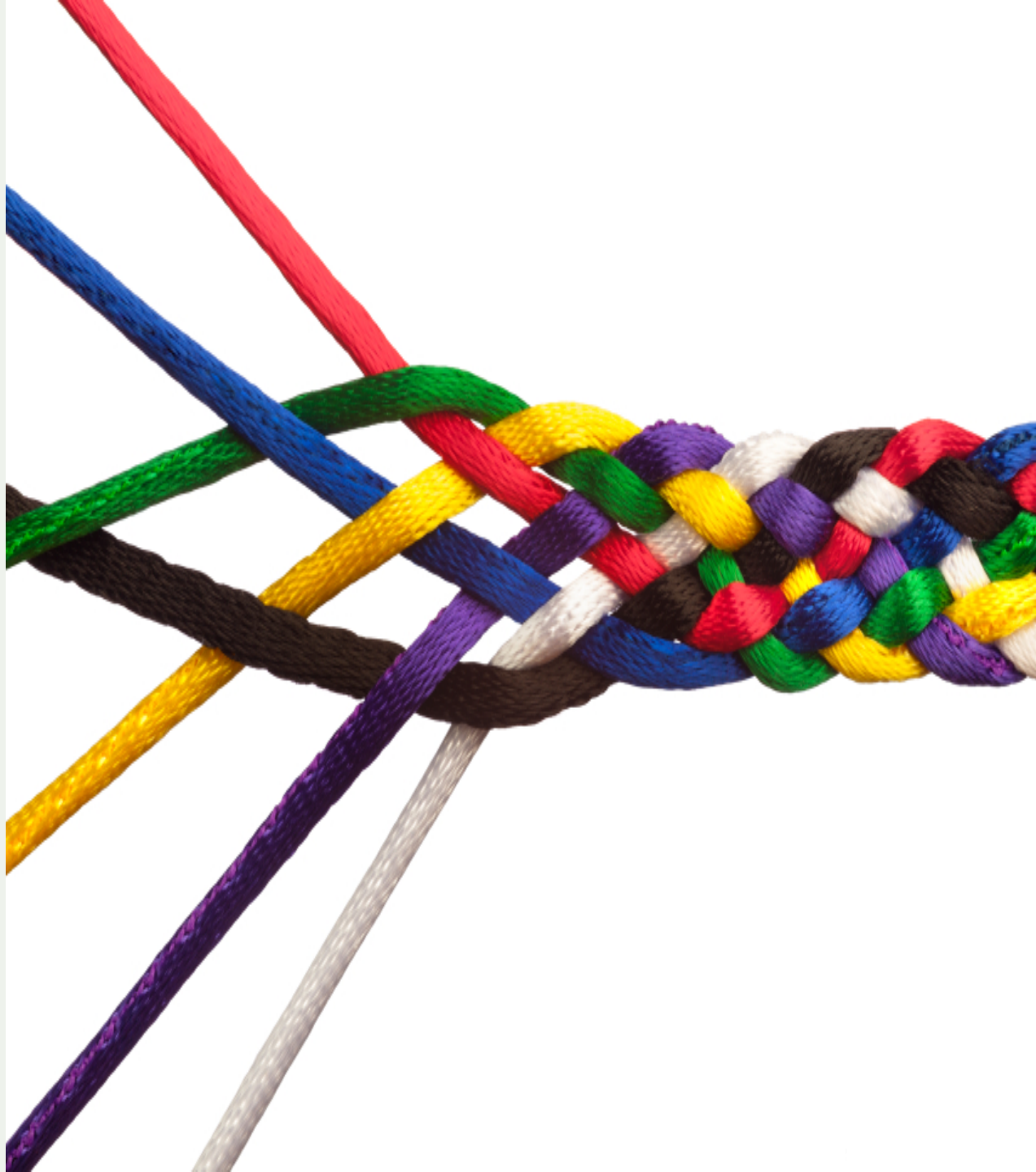
Join Us

Visit https://www.manrs.org

- Fill out the sign up form with as much detail as possible.
- We may ask questions and run tests

Get Involved in the Community

- Members support the initiative and implement the actions in their own networks
- Members maintain and improve the document and promote MANRS objectives



MANRS

Thank you.

Kevin Meynell
meynell@isoc.org

Visit us at
www.internetsociety.org
Follow us
@internetsociety

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120