Measuring MANRS readiness

Mutually Agreed Norms for Routing Security (MANRS) is a global initiative of network and IXP operators that provides crucial fixes to mitigate the most common threats to the Internet routing system. More information is available at https://www.manrs.org

MANRS aims to develop a community of security-minded organisations committed to making the global routing infrastructure more secure and robust. The operators joining MANRS demonstrate their commitment by implementing the so-called MANRS Actions:

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

More detailed description of the Actions is available here: https://www.manrs.org/manrs/

MANRS readiness

When an operator joins MANRS several checks are performed to ensure that the Actions are in fact implemented. Apart from verifying that the description of implementation of MANRS actions is complete and technically sound, we look at the network routing history for potential incident where the network might have been involved, cases of spoofed traffic, and that contact and routing information is properly registered in appropriate public databases. However, these checks are performed manually and only at the time of joining and no further monitoring if the commitment still in place is done.

To fully realize its potential MANRS has to be developed into a trusted and reputable mark of quality, recognized by the potential customers-enterprises. An objective and continuous commitment rating is an essential element in achieving this goal.

Measurements

To measure MANRS readiness for a particular network a set of metrics has been proposed, one for each action. For example, to measure to what degree Filtering (Action 1) is implemented we will measure the number of routing incidents where the network was implicated either as a culprit or an accomplice and their duration. That will produce a number – an indication of the degree of compliance, or a MANRS readiness index (MR-index) for Action1 for a specified period of time.

The measurements are passive, which means that they do not require cooperation for a measured network. That allows us to measure the MR-indices not only for the members of the MANRS initiative, but for all networks in the Internet (at the moment more than 60,000).

Calculation of Metrics and Data sources

Normalization of Periodic Events

In the current model, only routing incidents related to the network in question and adjacent networks are taken into account.

Non-action is penalized. The longer the incident takes place, the heavier it is rated. For example, the following coefficients are used:
< 30min = 0.5
< 24hour = 1
> 24hour =+1 for each subsequent 24-hour period

Also, multiple routing changes may be part of the same configuration mistake. For this reason, events related to the same metric that share the same time span are merged into an incident. This is shown in Figure 1.

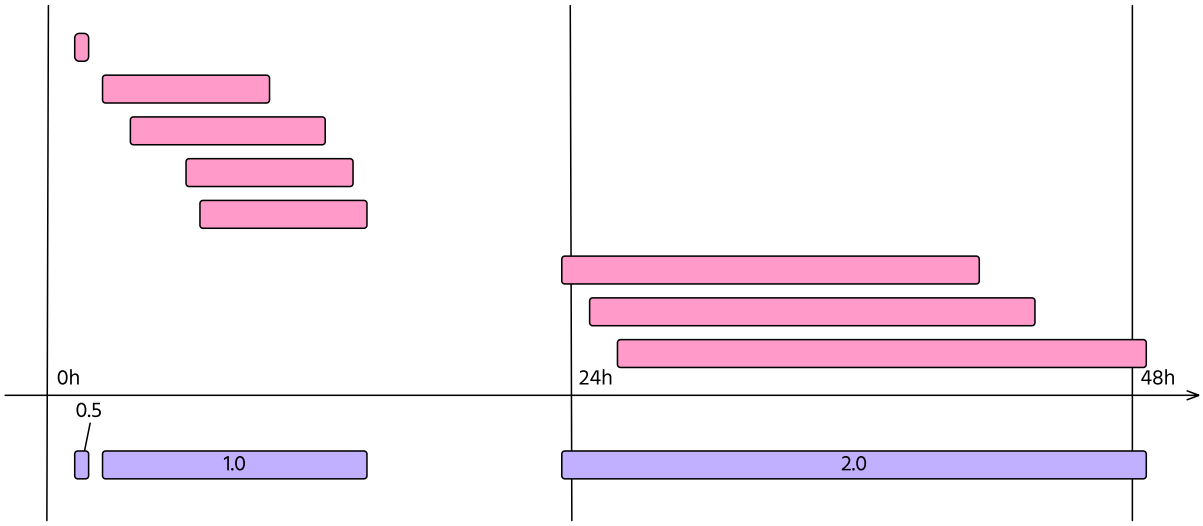

Figure 1. Routing changes, or events (in pink), may be part of the same incident (violet). In this case an operator experienced three incidents with a duration of 29 minutes, 13 hours, and 25 hours respectively. The resulting metric will be M=0.5 + 1 + 2 = 3.5

Based on this approach, for each of the MANRS actions, we can devise a composite MR-index and define thresholds for acceptable, tolerable and unacceptable – informing the members of their security posture related to MANRS.

A summary table of the metrics is provided below. A lower value indicates a higher grade of MANRS readiness.

Action	Metric	Description	Data source(s)
Filtering	M1	Route leak by the AS Calculates incidents where the AS was the culprit of BGP leakage events. In the example on Fig 1. if all pink events are route leaks by the AS, M1=3.5	bgpstream
	M2	Route misorigination by the AS calculates incidents where the AS was the culprit of BGP misorigination (hijacking) events.	bgpstream
	M1C	Route hijack by a direct customer Calculates incidents where the AS was an accomplice (the misoriginating AS was present in the AS-PATH) to BGP hijack events. Currently only incidents related to adjacent networks are taken into account.	bgpstream
	M2C	Route leak by a direct customer Calculates incidents where the AS was an accomplice (the leaking AS was present in the AS-PATH) to BGP hijack events. Currently only incidents related to adjacent networks are considered.	bgpstream
	M3	Bogon prefixes by the AS Calculates incidents where the AS announced bogon address space. Note that the duration of each incident is counted per day as the data in the CIDR report is available only on a daily basis.	CIDR report

	M4	Bogon ASNs by the AS Calculates incidents where the AS announced bogon ASNs. Note that the duration of each incident is counted per day as the data in the CIDR report is available only on a daily basis.	*CIDR report*
Anti-spoofing	M5	IP Spoofing by the AS Calculated as follows: M5 = 0 (if only positive tests are recorded) M5 = 0.5 (if no tests are found) M5 = # of negative tests in separate network segments (otherwise) Where a negative test indicates that spoofed traffic was not blocked.	*CAIDA Spoofer*
	M5C	IP Spoofing by a customer Same as M5, but it measures the ingress anti-spoofing capabilities of the AS to protect against spoofed traffic from its clients.	*CAIDA Spoofer*
Coordination	M8	Contact registration Checks if the ASN has registered contact information. For the whois, based on the authority source we check if any of the following are present: • RIPE: ['admin-c', 'tech-c']; • APNIC: ['admin-c', 'tech-c']; • AFRINIC: ['admin-c', 'tech-c']; • ARIN: ['OrgTechRef', 'OrgNocRef']; • LACNIC: ['person', 'email', 'phone']. Abuse contact information is not considered for this metric.	*RIPEstat*
Facilitate Global Validation	M7IRR	Not registered routes Calculates the percentage of routes originated by the AS that are not registered in an IRR as route objects. More specific routes that are advertised and covered by a less specific “route” object are also considered registered.	*RIPEstat*
	M7RPKI	Not registered ROAs Calculates the percentage of the routes originated by the AS that cannot be validated by any ROA in RPKI	*RPKI Validator*
	M7RPKIN	Incorrect ROAs Calculates the percentage of the routes originated by the AS that are invalidated by a corresponding ROA	*RPKI Validator*