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.

Objectives

1. Raise awareness and encourage actions by demonstrating commitment of the growing group of supporters
2. Promote the culture of collective responsibility for resilience and security of the Internet's global routing system
3. Demonstrate the ability of the industry to address issues of resilience and security of the Internet's global routing system in the spirit of collective responsibility
4. Provide a framework for ISPs to better understand and help address issues related to resilience and security of the Internet's global routing system

Scope

Many different recommendations exist to improve the security and resilience of the inter-domain routing system. Some of the advice can even appear somewhat contradictory and often the key decision can come down to understanding what is most important or appropriate for a given network considering its size and resources, the number of external connections, customers and end-users it has, the size and expertise of its staff, and so forth.

The Expected and Advanced Actions below underline a set of recommendations that are definitely valuable to the overall security and resilience of the global routing system, as well as to the network operator itself. They address three main classes of problems:

- Problems related to incorrect routing information;
- Problems related to traffic with spoofed source IP addresses; and
- Problems related to coordination and collaboration between network operators.

The Expected Actions define a minimum "package" – a set of recommendations that should definitely be implemented by operators supporting this MANRS document. This package is not exhaustive and the expectation is that many network operators are implementing even stronger measures and controls already, or plan to do so in the future. The Advanced Actions later in this document further extend the minimum package.

We are conscious of the fact that any particular Action is not a comprehensive solution to the outlined problems. But each is a small step that, if multiplied by a large number of supporters, can become a significant improvement in the resilience of the global Internet routing system. Therefore the selection of actions was based on an assessment of the balance between small, incremental individual costs and the potential common benefit.

Definitions

To articulate the specifics of the Expected and Advanced Actions, it is necessary to explicitly define a number of terms, to relate to their general usage in the Internet industry.

- Infrastructure – Operator's internal networks, which must be reachable on the Internet.
- End User – Networks within an operator's routing and administrative domain.
- Peer Network – An external network with which traffic is exchanged relating to both your respective Infrastructure, and Customer Networks.
- Transit Network – An external network to which traffic relating to your Infrastructure and Customer Networks is sent, but from which traffic from the Internet in general is received.
- Customer Network – An external network for which an operator provides transit services.
- Single Homed - A single, uncomplicated link between networks, or connecting an End User to the Infrastructure. This represents a single path over which traffic can flow within or between networks.
- Multi Homed - Multiple paths between networks (even multiple networks), or connections between an End User and the Infrastructure; this can create multiple paths over the Infrastructure and the Internet over which traffic can traverse.

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.

Expected 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.

2. Prevent traffic with spoofed source IP addresses.

- 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. Facilitate global operational communication and coordination between network operators.

- Network operator maintains globally accessible up-to-date contact information.

Advanced 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.

Elaboration and References

Action 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.

Discussion: Most important is to secure inbound routing advertisements, particularly from customer networks, through the use of *explicit* prefix-level filters or equivalent mechanisms. Secondarily, AS-path filters might be used to require that the customer network be explicit about which Autonomous Systems (ASes) are downstream of that customer. Alternately, AS-path filters that block announcements by customers of ASes with which the provider has a settlement-free relationship can prevent some types of routing "leaks". Filtering customer BGP announcements by AS-path filters alone is *insufficient* to prevent catastrophic routing problems at a systemic level.

References:

"Recommended Internet Service Provider Security Services and Procedures", Section Network Infrastructure, http://www.rfc-editor.org/bcp/bcp46.txt

"BGP operations and security", http://tools.ietf.org/html/draft-ietf-opsec-bgp-security

Border Gateway Protocol Security, NIST: Special Publication SP 800-54, http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf

"Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure", http://tools.ietf.org/html/rfc3871

"Using RPSL in Practice", http://tools.ietf.org/html/rfc2650

"Using the RIPE Database as an Internet Routing Registry", https://labs.ripe.net/Members/denis/using-the-ripe-database-as-an-internet-routing-registry

BGP Security Best Practices, FCC CSRIC III WG4 Final Report, http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

Action 2. Prevent traffic with spoofed source IP addresses.

- 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 incorrect source IP address from entering and leaving the network.
- Discussion: Common approaches to this problem have involved software features such as SAV (Source-Address Validation) on cable-modem networks or strict uRPF (unicast Reverse-Path Forwarding) validation on router networks. These methods can ease the overhead of administration in cases where routing and topology are less relatively dynamic. Another approach could be to use inbound prefix filter information to create a packet-filter, which would allow only packets with source IP addresses for which the network could legitimately advertise reachability.

References:

"Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", http://tools.ietf.org/html/bcp38

"Ingress Filtering for Multihomed Networks", http://tools.ietf.org/html/bcp84

"Securing the Edge", http://www.icann.org/committees/security/sac004.txt

"RIPE Anti-Spoofing Task Force HOW-TO", http://www.ripe.net/ripe/docs/ripe-431

BGP Security Best Practices, FCC CSRIC III WG4 Final Report, http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

Action 3. Facilitate global operational communication and coordination between network operators.

- Network operator maintains globally accessible up-to-date contact information.

Discussion: Common places to maintain such information are PeeringDB, RIRs' whois databases and large IRRs like RADB and RIPE. A network operator should register and maintain 24/7 contact information in at least one of these databases. This contact information should include the operator's current point of contact information for the NOC of the AS, all netblocks, and domain names. Operators are encouraged to document their network routing policies in an IRR. Additional information is also welcome, such as, for example, a looking glass URL in the appropriate field in their PeeringDB record.

References:

"Using RPSL in Practice", http://tools.ietf.org/html/rfc2650

Peering DB, https://www.peeringdb.com

RADB, http://www.radb.net/

Action 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.

Discussion: To facilitate validation of routing information by other networks on a global scale, information about routing policy, ASNs and prefixes that are intended to be advertised to external parties is necessary.

One of the way of making the policy publicly available is through documenting them using RPSL in one of the Internet Routing Registries (IRRs) mirrored by RADB (e.g. RIPE, ARIN, RADB etc.). In this case operators must register and maintain at minimum one (or more) "as-set" IRR objects containing a list of ASNs intended to be advertised to external parties, that could be used by automatic tools to generate prefix-filters. Operators must also maintain their information in the IRR to ensure that is it up-to-date.

Another, more secure means to facilitate validation on a global scale is through the RPKI system. Operators could obtain RPKI certificates for their own prefixes from the RIRs that allocated those prefixes to them, and publish and maintain ROAs corresponding to the prefixes they announce.

Operators must encourage their Customer Network operators to do so as well. This will allow other networks to validate announcements on the global scale.

References:

"Using RPSL in Practice", http://tools.ietf.org/html/rfc2650

"Using the RIPE Database as an Internet Routing Registry", https://labs.ripe.net/Members/denis/using-the-ripe-database-as-an-internet-routing-registry

"Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)", http://www.rfc-editor.org/bcp/bcp185.txt