East African Communications Organisation

Communication for all in East Africa

IP NETWORKS BEST CURRENT SECURITY PRACTICES

Prepared by EACO

JULY 2019

TABLE OF CONTENTS

ACRONYMS

BCP	Best Current Practice
DDoS	Distributed Denial of Services
DNS	Domain Name Server
Dos	Denial of Service or
IXP	Internet Exchange Point
MANRS	Mutually Agreed Norms for Routing Security
RFC	Request for Comments

1 INTRODUCTION

As the Internet is growing rapidly, so are the number of network attacks. These attacks are mainly Denial of Service (DoS) or Distributed Denial of Services (DDoS) attacks, respectively known as DoS or DDoS attacks. If nothing is done, the situation will become worse, especially, with the advent of the Internet of Everything; the problem will grow exponentially.

To solve the problem, the Internet community of engineers have elaborated some best practices namely the Best Current Practice 38 (BCP 38), Request for Comments 2827 (RFC2827) and more recently Mutually Agreed Norms for Routing Security (MANRS), which comes in two flavours; MANRS for Network operators and MANRS for Internet Exchange Point (IXP) operators.

In addition, it is crucial and imperative for everyone to play a role in ensuring a stable and secure Internet ecosystem. It is not the responsibility of some specific players or countries; it is everyone's responsibility.

2 WHAT PROBLEM ARE THESE BEST PRACTICES TRYING TO SOLVE?

First, let us agree that the Internet (i.e. the entirety of it) is made of many other big, medium and small networks. Each network can reach another network on Internet, meaning packets flow from/to any direction. This is a perfect situation, considering that everyone on the internet has ethical behaviour. Unfortunately, that is not the case. There are some networks that originate Internet traffic with "spoofed" IP addresses, in other terms, their use "forged" source IP addresses, and they can literally generate enough traffic to "flood" one particular target (this is a Denial of Service - DoS attack).

3 EXAMPLES OF THE RECENT DOS/DDOS ATTACKS

THE GITHUB ATTACK (FEB 28, 2018) *https://thehackernews.com/2018/03/biggest-ddos-attack-github.html*

THE DYN ATTACK (2016) https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

On October 21, 2016, Domain Name Server (DNS) provider Dyn was struck three times by DDoS attacks. Websites taken offline by the attack included Twitter, Tumblr, Paypal, Pinterest, the BBC, Etsy, Fox News, GitHub, GroupHub, HBO, HostGator, iHeartRadio, Mashable, the New York Times, Reddit, Shopify, Slack, Spotify, Starbucks and more.

THE GITHUB ATTACK (2015) https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

THE SPAMHAUS ATTACK
https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

4 WHAT CAN BE DONE

4.1 Implementing BCP38/BCP84 - "Ingress filtering"

BCP38 - RFC 2827, is designed to limit the impact of distributed denial of service attacks, by denying traffic with spoofed addresses access to the network, and to help ensure that traffic is traceable to its correct source network. BCP84 - RFC 3704, updates BCP38/RFC 38 in the sense that it considers the aspect of multi homed networks.

As per the RFC 3704, there are at least five ways one can implement BCP 38 - RFC 2827, with varying impacts. These include (the names are in relatively common usage):

- Ingress Access Lists;
- Strict Reverse Path Forwarding;
- Feasible Path Reverse Path Forwarding;
- Loose Reverse Path Forwarding;
- Loose Reverse Path Forwarding ignoring default routes;

A complete description of each option can be found in the RFC 3704. In a nutshell, these procedures allow an ISP to filter any traffic coming into its network from a customer or a peer network. Only legitimate traffic will be accepted, whereas the non-legitimate traffic will be dropped.

4.2 Implementing MANRS

MANRS is a global initiative, supported by the Internet Society that provides crucial fixes to reduce the most common routing threats.

4.2.1 MANRS for Network Operators

MANRS outlines four simple but concrete actions that network operators should take:

- **Filtering** – Ensure the correctness of your own announcements and of announcements from your customers to adjacent networks with prefix and AS-path granularity;
- **Anti-spoofing** – Enable source address validation for at least single-homed stub customer networks, your own end-users, and infrastructure;
- **Coordination** – Maintain globally accessible up-to-date contact information;
- **Global Validation** – Publish your data, so others can validate routing information on a global scale.

Each action point is detailed at the following URL: https://www.manrs.org/isps/manrs-actions-fornetwork-operators/

4.2.2 MANRS for IXP Operators

Besides, the Network Operators actions, there set of rules applicable to Internet Exchange Points (IXP) operators.

The website of MANRS continues stating that the MANRS Actions were initially designed for network operators, but IXPs should also play an active role in protecting the Internet. IXPs represent active communities with common operational objectives and already contribute to a more resilient and secure Internet infrastructure.

MANRS can help IXPs build safe neighbourhoods, leveraging the MANRS security baseline. It also demonstrates an IXP's commitment to security and sustainability of the Internet ecosystem, and dedication to providing high quality services.

The IXP Programme Action set are:

- Action 1. Prevent propagation of incorrect routing information. (Mandatory)
- Action 2. Promote MANRS to the IXP membership. (One or more must be checked)
- Action 2-1: Offer assistance to its members to maintain accurate routing information in an appropriate repository (IRR and/or RPKI)
- Action 2-2: Offer assistance in implementing MANRS ISP Actions for the members,
- Action 2-3: Indicate MANRS participation on the member list and the website • Action 2-4: Provide incentives linked to MANRS readiness
- Action 3. Protect the peering platform.
- Action 4. Facilitate global operational communication and coordination between network operators.
- Action 5. Provide monitoring and debugging tools to the members.

The MANRS Actions for IXP operators are outlined and detailed at this URL: https://www.manrs.org/ ixps/manrs-actions-for-ixps/

5 CONCLUSIONS

- The security of Internet is critical, and it is everyone's business to ensure its stability and security;

- There are a number of Best practices that are used; BCP38, BCP84, MANRS, etc. In the Annex, there are a number of other Best practices documents/work (Source: https://startupinc.nl/wpcontent/uploads/2017/10/20171027-Quickscan-on-routing-measures-to-increase-the-security-ofthe-Internet.pdf);

- There is a continuous need to training more engineers about IP networks best current security practices. This can be done at the ISP level, which would train its customers, at the IXP level, and/ or regional level with EACO members.

ANNEX

1. [BCP38] - Network Ingress Filtering (aka RFC2827)
   Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
   https://tools.ietf.org/html/bcp38
   Publication: May 2000

2. [BCP46] - Recommended Internet Service Provider Security Services and Procedures (aka RFC3013)
   http://www.rfc-editor.org/bcp/bcp46.txt
   Publication: November 2000

3. [BCP84] - Ingress Filtering for Multihomed Networks (aka RFC3704)
   https://tools.ietf.org/html/bcp84
   Publication: March 2004

4. [BCP185] - Origin Validation Operation, Based on the Resource Public Key Infrastructure (RPKI) (aka RFC7115)
   https://www.rfc-editor.org/bcp/bcp185.txt
   Publication: January 2014

5. [BCP194] - BGP Operations and Security (aka RFC7454)
   https://tools.ietf.org/html/rfc7454
   Publication: February 2015

6. [BGPHE] - BGP Toolkit
   https://bgp.he.net/

7. [BGPJob] - Practical everyday BGP filtering with AS_PATH filters
   Job Snijders - Peerlocking - NANOG67
   https://www.nanog.org/sites/default/files/Snijders_Everyday_Practical_Bgp.pdf

8. [CAIDA-Spoof] - State of IP Spoofing CAIDA - Center for Applied Internet Data Analysis - State of IP Spoofing
   https://spoofer.caida.org/summary.php

9. [CSAN2016] - Cyber Security Assessment Netherlands 2016
   Cyber Security Assessment Netherlands 2016: Professional criminals are an ever greater danger to digital security in the Netherlands
   https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2016.html
   Publication: October 24, 2016

10. [CSAN2017] - Cyber Security Assessment Netherlands 2017
Cyber Security Assessment Netherlands 2017: Digital resilience is lagging behind the increasing threat
https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2017.html
Publication: August 31, 2017

11. [CSRIC3BGP] - BGP Security Best Practices, FCC CSRIC III WG4 Final Report
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202_013.pdf
Publication: March 2013

12. [ITHI] - ICANN Identifier Technology Health Indicators project
https://www.icann.org/ithi

13. [ISO27000] - ISO/IEC 27000 family - Information security management systems
https://www.iso.org/ isoiec-27001-information-security.html

14. [FIRST] - Forum of Incident Response and Security Teams
https://www.first.org

15. [MANRS] - Mutually Agreed Norms for Routing Security (aka Routing Manifesto)
https:// www.routingmanifesto.org/

16. [NaWas] - Nationale anti-DDoS Wasstraat
https://nbip.nl/web/guest/nawas
https://slideshare.net/splend/hsb-nationale-anti-ddos-wasstraat-alexbik

17. [NDN] - National Detection Network
https://www.ncsc.nl/english/Cooperation/national-detectionnetwork.html

18. [NIST800-54] - Border Gateway Protocol Security - NIST Special Publication SP 800-54
http:// csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf
Publication: July 2007

19. [PeeringDB] - Peering DB
https://www.peeringdb.com

20. [RADB] - Routing Assets Database

http://www.radb.net/

21. [RFC3871] - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure
    https://tools.ietf.org/html/rfc3871
    Publication: September 2004

22. [RFC2650] - Using RPSL in Practice
    https://tools.ietf.org/html/rfc2650
    Publication: August 1999

23. [RFC6192] - Protecting the Router Control Plane
    https://tools.ietf.org/html/rfc6192
    Publication: March 2011

24. [RIPE431] - RIPE Anti-Spoofing Task Force HOW-TO
    http://www.ripe.net/ripe/docs/ripe-431
    Publication: May 9, 2008

25. [RipeDbIRR] - Using the RIPE Database as an Internet Routing Registry
    https://labs.ripe.net/Members/denis/using-the-ripe-database-as-an-internet-routing-registry
    Publication: August 22, 2013

26. [SAC004] - Securing the Edge, Paul Vixie, ISC. Not referenced
    http://www.icann.org/committees/security/sac004.txt
    Publication: October 17, 2002

27. [SAVI] - Source Address Validation Improvement Framework (aka RFC7039)
    https://tools.ietf.org/html/rfc7039
    Publication: October 2013

28. [TNI] - Trusted Networks Initiative
    https://tn-init.nl/
    https://www.thehaguesecuritydelta.com/images/TNI_Info_Sheet_01-04-2015.pdf
    http://procon.bg/article/trusted-networks-initiative-netherlands-response-ddos-attacks
    https:// www.thehaguesecuritydelta.com/projects/project/60-trusted-networks-initiative