# Collective responsibility for security and resilience of the global routing system

Michuki Mwangi <Mwangi@isoc.org>

# Let us look at the problem first

- **BGP is based on trust**
  - **No validation of the legitimacy of updates**
  - **Tools outside BGP exist, but not widely deployed**
  - **BGPSEC is under development in the IETF**

# Let us look at the problem first

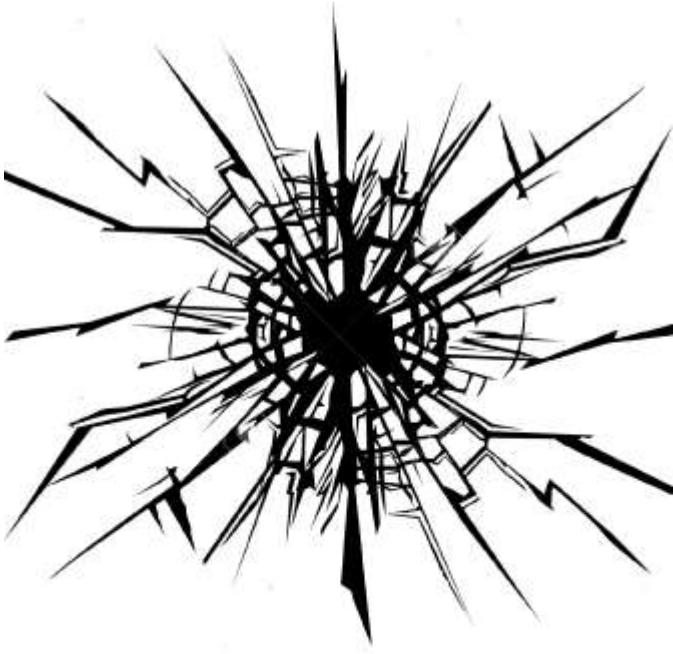
- **Prefix hijack**
  - **Announcing a prefix that does not belong to a network**
  - **Can involve “ASN hijacking”**
- **“Route leak”**
  - **Violation of a “valley-free” principle**
  - **E.g. a customer becoming a transit provider**

# But also

- Source IP address spoofing
  - Forging the source IP address of packets
- Collaboration
  - How you reach someone on the other side of the Net to help you out?
  - How do you mitigate a DDoS?

# Impact

- **Prefix hijack**
  - **Denial of service, impersonating a network or a service, traffic intercept**
- **“Route leak”**
  - **Traffic intercept, but may result in denial of service**
- **IP spoofing**
  - **The root cause of reflection DDoS attacks**



# How do we address these problems?

- Tools
  - Prefix and AS-PATH filtering, RPKI, IRR, …
  - Ingress and egress anti-spoofing filtering, uRPF, …
  - Coordination and DDoS mitigation
- Challenges
  - Your safety is in someone other’s hands
  - Too many problems to solve, too many cases

# The Mutually Agreed Norms for Routing Security (MANRS)

- **Aka Routing Resilience Manfesto:**
  - **https://www.routingmanifesto.org/manrs/**

- **Defines a minimum package: 4 Actions**
  - **Too many problems to solve, too many cases**

- **Collective focus and commitment**
  - **Your safety is in someone other’s hands**

# Good MANRS

1. Prevent propagation of incorrect routing information

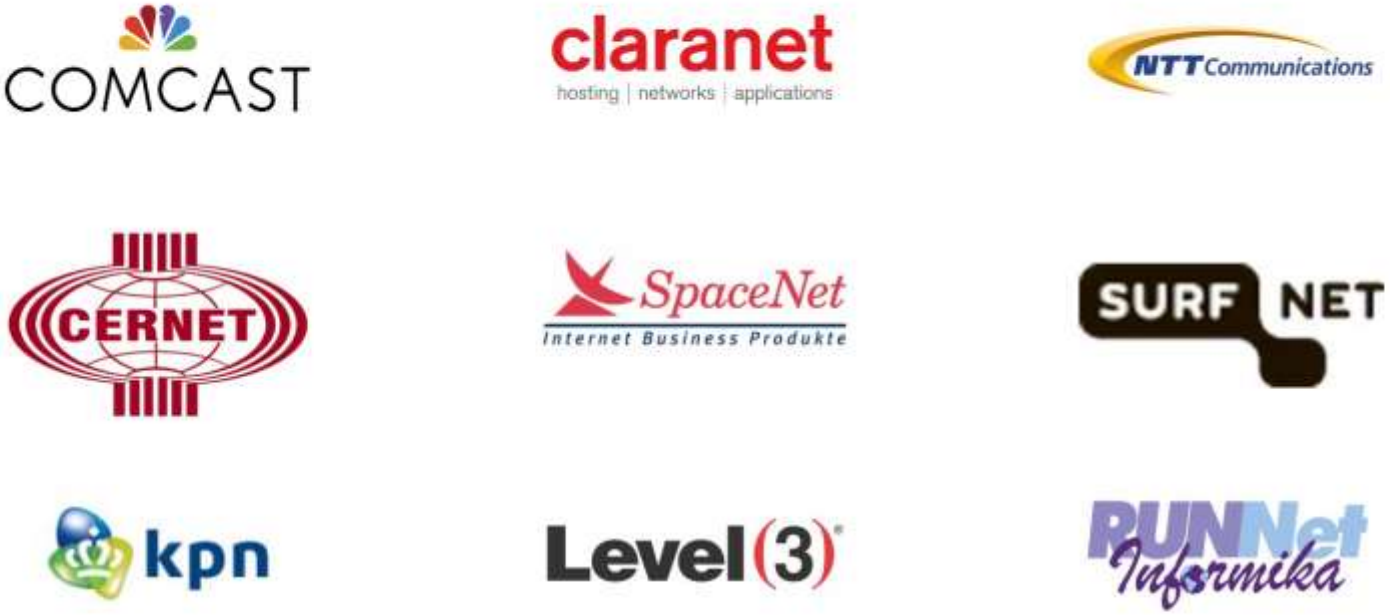
2. Prevent traffic with spoofed source IP address

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

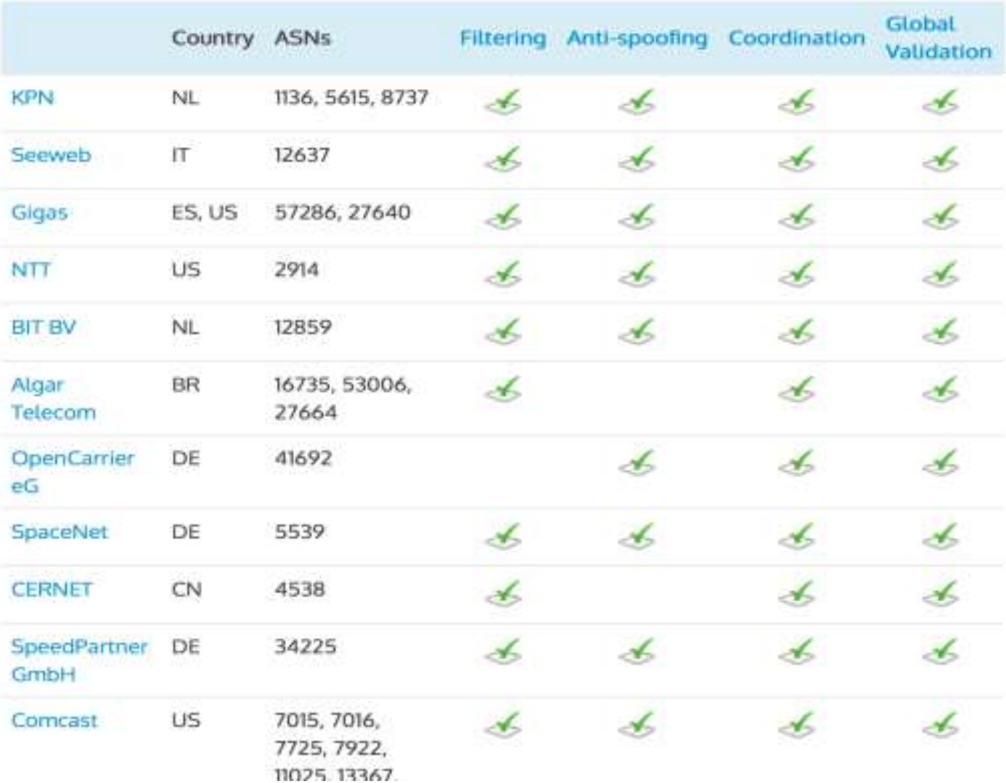
# MANRS is not (only) a document – it is a commitment

1) The company **supports the Principles and implements at least one of the Actions** for the majority of its infrastructure. Implemented Actions are marked with a check-box. The Action "Facilitate global operational communication" cannot be the only one and requires that another Action is also implemented.
2) The company becomes a Participant of MANRS, helping to **maintain and improve** the document, for example, by suggesting new Actions and maintaining an up-to-date list of references to BCOPs and other documents with more detailed implementation guidance.

# Public launch of the initiative - 6 November 2014



# A growing list of participants



| | Country | ASNs | Filtering | Anti-spoofing | Coordination | Global Validation |
|---|---|---|---|---|---|---|
| KPN | NL | 1136, 5615, 8737 | ✓ | ✓ | ✓ | ✓ |
| Seeweb | IT | 12637 | ✓ | ✓ | ✓ | ✓ |
| Gigas | ES, US | 57286, 27640 | ✓ | ✓ | ✓ | ✓ |
| NTT | US | 2914 | ✓ | ✓ | ✓ | ✓ |
| BIT BV | NL | 12859 | ✓ | ✓ | ✓ | ✓ |
| Algar Telecom | BR | 16735, 53006, 27664 | ✓ | | ✓ | ✓ |
| OpenCarrier eG | DE | 41692 | | ✓ | ✓ | ✓ |
| SpaceNet | DE | 5539 | ✓ | ✓ | ✓ | ✓ |
| CERNET | CN | 4538 | ✓ | | ✓ | ✓ |
| SpeedPartner GmbH | DE | 34225 | ✓ | ✓ | ✓ | ✓ |
| Comcast | US | 7015, 7016, 7725, 7922, 11025, 13367, | ✓ | ✓ | ✓ | ✓ |

# Next Steps

- Expanding the group of participants
  - Looking for industry leaders in the region
- Expanding the scope of the MANRS
  - Raising the bar – defining new Actions
- Developing better guidance
  - Tailored to MANRS
  - In collaboration with existing efforts, like BCOP

# Are you interested in participating?

| Filtering | Anti-Spoofing | Coordination | Global scale |
|---|---|---|---|
| ☑ | □ | ☑ | □ |

MANRS

https://www.routingmanifesto.org/

https://www.manrs.org/

# 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****.*

# Actions (2)

## Prevent traffic with spoofed source IP address

*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.*

# Actions (3)

**Facilitate global operational communication and coordination between the network operators**

*Network operators should maintain* ***globally accessible up-to-date contact information.***

# 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.*