September 2017

MANRS

Mutually Agreed Norms for Routing Security

Kevin Meynell
Content & Resource Manager
meynell@isoc.org

The Problem

A Routing Security Primer

Routing Basics

~60,000 networks (Autonomous Systems) across the Internet

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

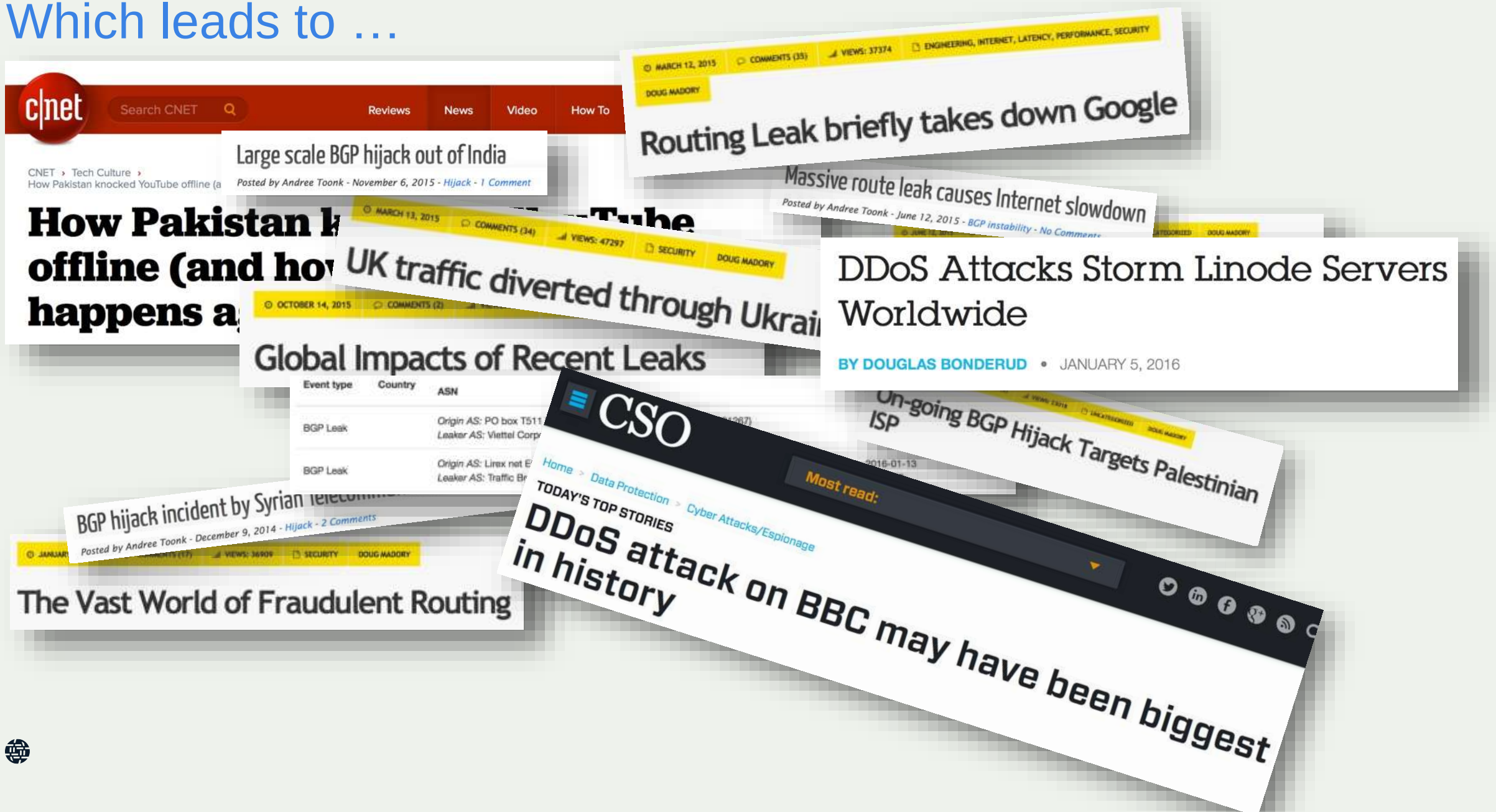
Routers use unique Autonomous System Numbers (ASNs) to identify themselves to all other routers

The Problem

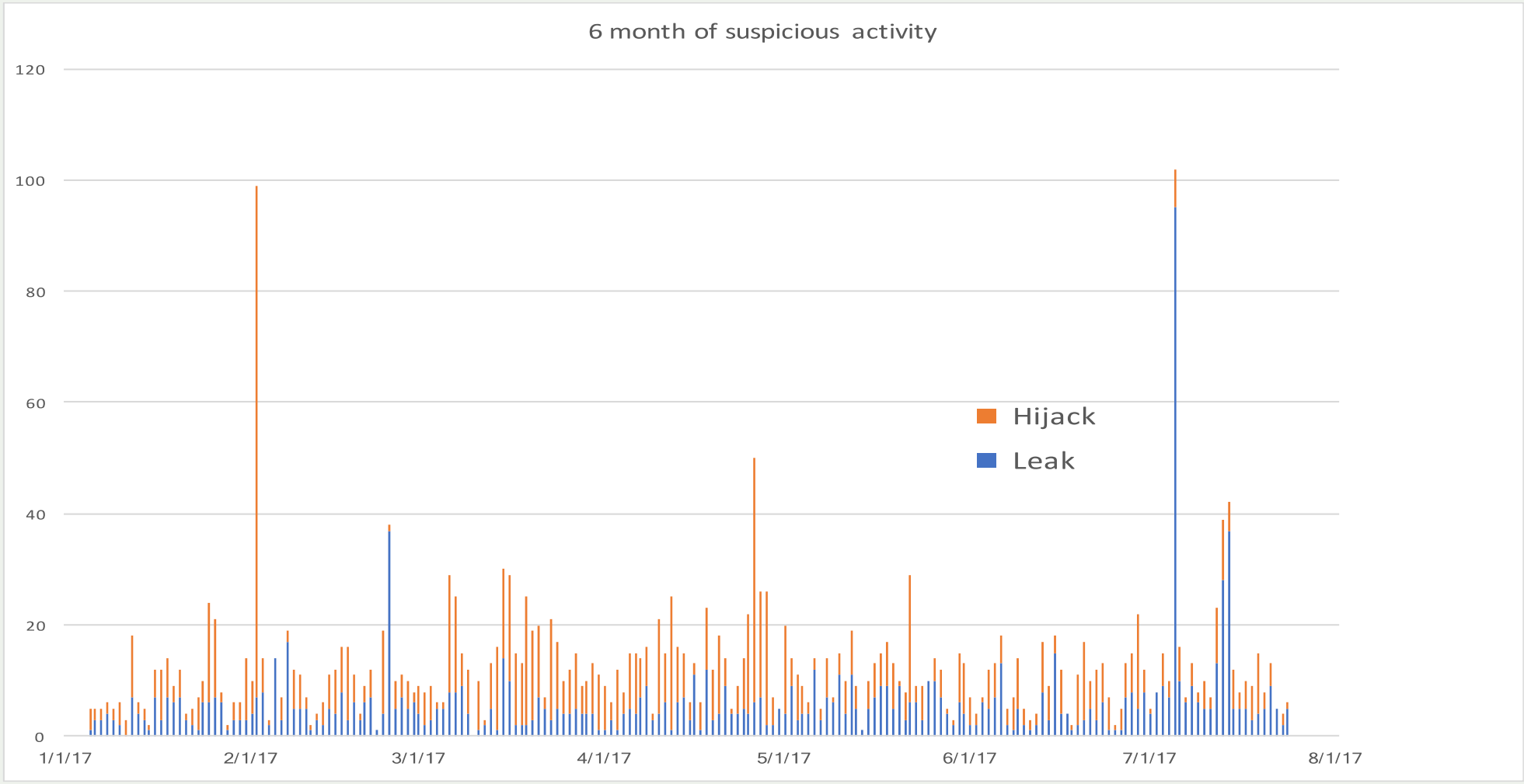
Border Gateway Protocol (BGP) is based entirely on trust

- No built-in validation of the legitimacy of updates
- The chain of trust spans continents
- Lack of reliable resource data

Which leads to …



No Day Without an Incident



http://bgpstream.com/

What’s Happening?

IP prefix hijack

- AS announces prefix it doesn’t originate and wins the ‘best route’ selection
  - AS announces more specific prefix than what may be announced by originating AS
  - AS announces it can route traffic through shorter route, whether it exists or not
- Packets end up being forwarded to wrong part of Internet
- Denial-of-Service (DoS), traffic interception, or impersonating network or service

Route leaks

- Violation of valley-free routing (e.g. re-announcing transit provider routes to another provider)
- Usually due to misconfigurations, but can be used for traffic inspection and reconnaissance
- Can be equally devastating

IP address spoofing

- Creation of IP packets with false source address
- The root cause of reflection DDoS attacks

Are There Solutions?

Tools - Yes!

- Prefix and AS-PATH filtering, RPKI, IRR, …
- BGPSEC under development at the IETF
- Whois, Routing Registries and Peering databases

But…

- Lack of deployment
- Lack of reliable data

A Tragedy of the Commons

From a routing perspective, securing your own network does not necessarily make it more secure. Network security is in someone else's hands.

— The more hands – the better the security

Is there a clear, visible, and industry-supported line between good and bad?

— A cultural norm?

MANRS

A vital part of the security solution

MANRS was founded with the ambitious goal of improving the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for Internet infrastructure.

Mutually Agreed Norms for Routing Security

MANRS defines four concrete actions that network operators should implement

- Technology-neutral baseline for global adoption
- A *minimum* set of requirements

MANRS builds a visible community of security-minded operators

- Promotes culture of collaborative responsibility

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*

Global Validation – Facilitate validation of routing information on a global scale

- *Publish your data, so others can validate*

A Note on MANRS' Limitations

MANRS is an *absolute minimum* an operator should consider, with *low risk* and *cost-effective* Actions

The more operators implement MANRS, the fewer routing incidents we will see, and the smaller will be their scope

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

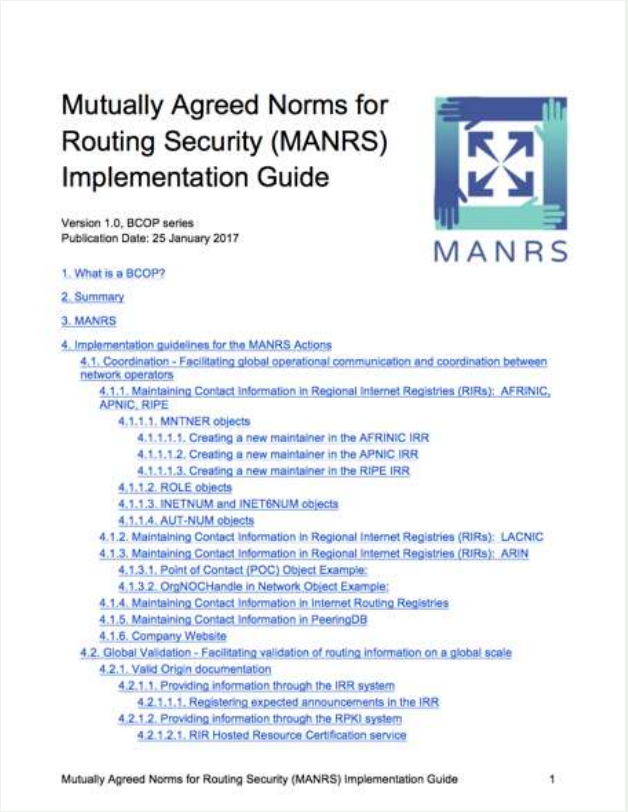
Why NRENs Should Join MANRS…

- To add competitive value and enhance operational effectiveness
  - Growing demand from customers for managed security services
- To show security proficiency and commitment to your customers
  - Promote MANRS compliance to security-focused customers
- To show technical leadership and distinguish you from commercial ISPs
  - Customers increasing willing to pay more for secure services
- To help solve global network problems
  - Lead by example and improve routing security for everyone
  - Being part of the MANRS community can strengthen enterprise security credentials

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
- http://www.manrs.org/bcop/



Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

MANRS

Version 1.0, BCOP series
Publication Date: 25 January 2017

What’s Next: MANRS Training and Certification

Routing security is hard. How can we make it more accessible? The “simple” MANRS Implementation Guide is a 50-page document that assumes a certain level of expertise..

Online training modules

- Based on the MANRS Implementation Guide
- Walks a student through the tutorial with a test at the end
- Working with and looking for partners that are interested in integrating it in their curricula

A hands-on lab to achieve MANRS certification

- Completing the online modules as a first step in MANRS certification
- Looking for partners

NRENs and their members can help with this!

Can you stand up publicly and say:

✓ I care about routing security

✓ I am prepared to spend resources on it

✓ I am prepared to be held accountable by the community

Join MANRS Today

Commit to Routing Security, Collaborative Action,
and the Good of the Internet

https://www.manrs.org/

Thank you.

Kevin Meynell

Content & Resource Manager
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