Demystifying the World of Routing Security

Dan York, york@isoc.org www.manrs.org

Internet Society

About the Internet Society

We are a global nonprofit organization connecting and empowering communities to protect this essential resource since 1992.

Community members of Pu'uhonua O Waimanalo work together with the Internet Society to learn how to use and install the Internet during a training session.

The Internet Society Community: A Global Network of People

104,681

Global Members

126

Chapters, Special Interest Groups, and Standing Groups

87

Organization Members

140

Internet Society Staff

The Internet is for everyone.

We work toward this vision by building, promoting, and defending a bigger and stronger Internet.

About Me

Dan York, CISSP

Director, Internet Technology

Internet Society since 2011, online since the 1980s before the Internet

Specialty: connecting dots, engineer-to-english translation

Working on routing security since 2014

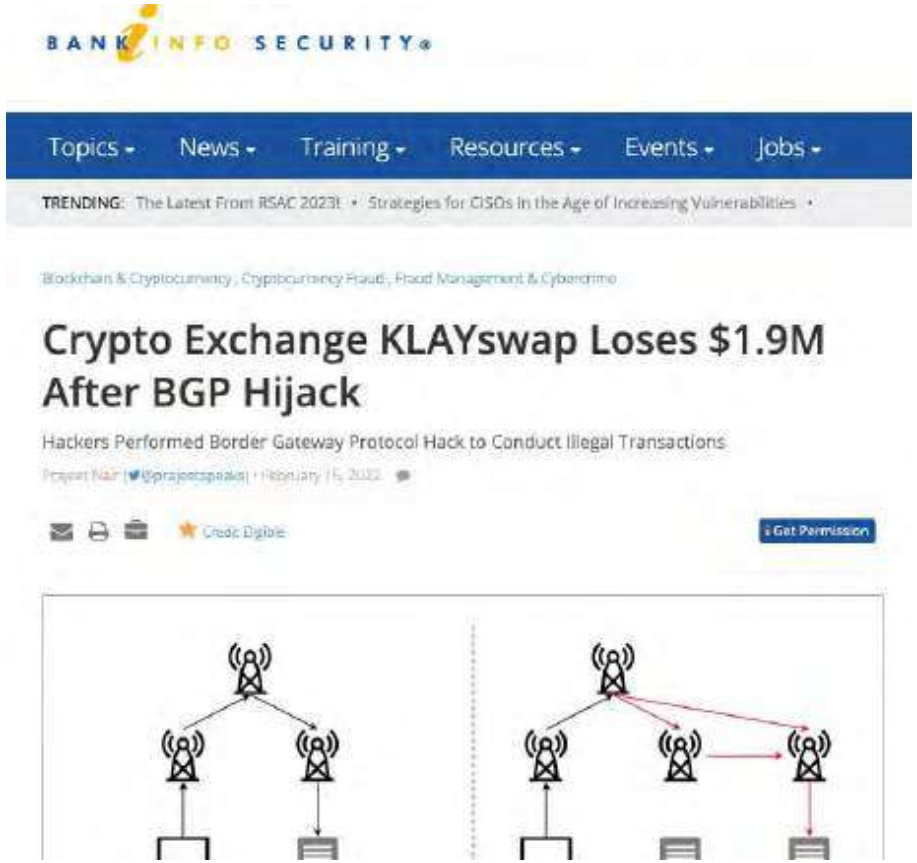
Also involved with security of LEOs, VoIP, DNS, IPv6, TLS, AI, EIEIO

https://danyork.me Mastodon: @danyork@mastodon.social

Let’s Get Into It!
First, A Scary Story

(Don’t panic! I’ll explain the acronyms)

KLAYswap: $1.9M USD Stolen



What Happened?

Hackers stole ~1.9M USD worth of cryptocurrency assets.

They didn't attack KLAYswap directly; they went after the server infrastructure of KakaoTalk, a contracted marketing and tech support service.

Attackers used a BGP hijack to serve a malicious version of KakaoTalk's JavaScript software development kit (SDK) file.

This was a supply chain attack.

This hijack could have been avoided - or at least minimized - if KakaoTalk had valid RPKI Route Origin Authorizations (ROAs) for its ASNs.

RPKI, ROA, ASN, What?

Let’s Back Up A Minute …

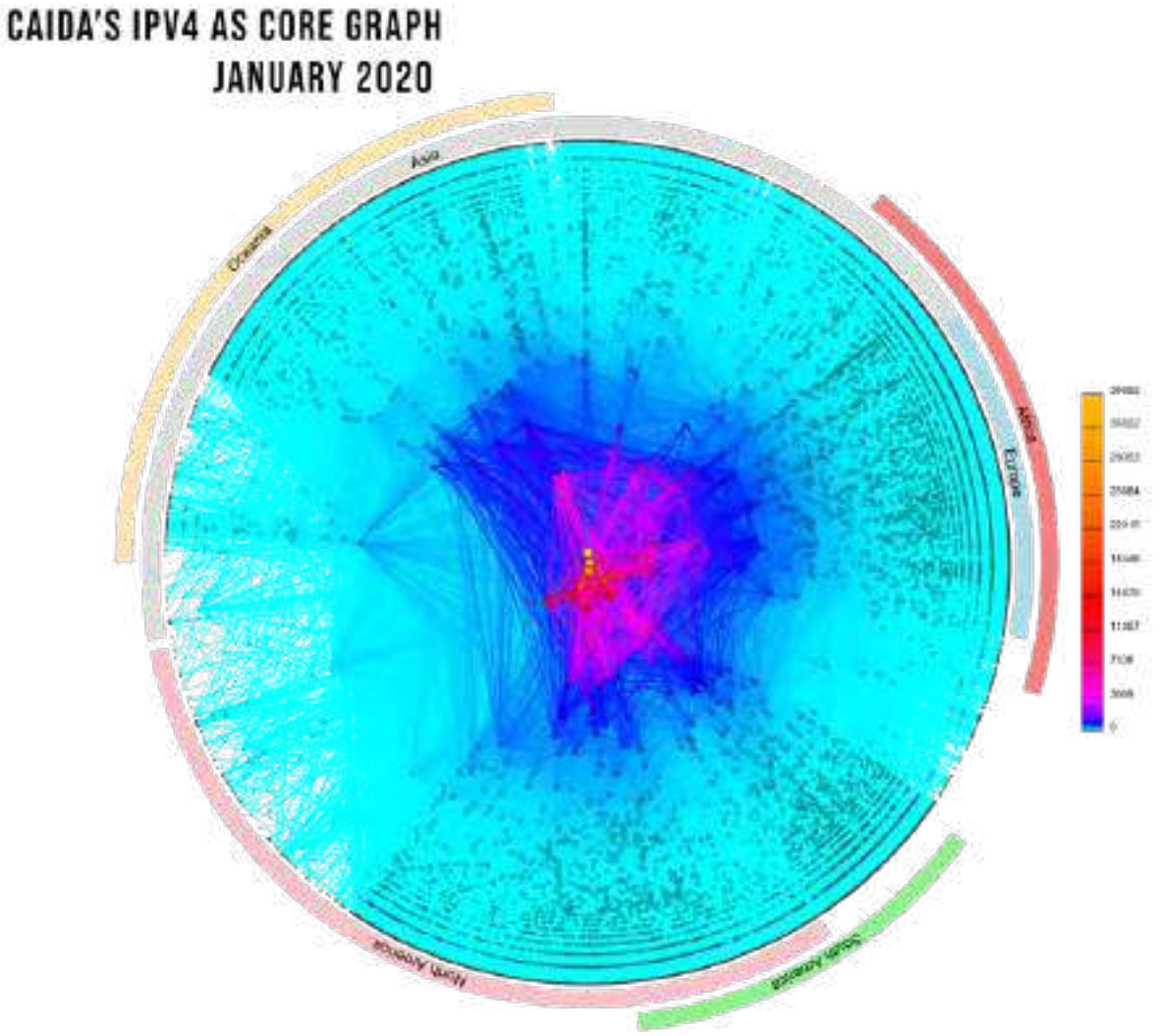
An Extremely Condensed Routing 101

There are ~75,000 independent networks that together make up the Internet.

Each network is identified by an **Autonomous System Number, or ASN**.

Each ASN makes its own decisions about how to move Internet traffic using a language called **Border Gateway Protocol, or BGP.**

BGP is a fundamental underpinning of the Internet.



Volunteers for a demo?


Photo by charlesdeluvio on Unsplash

The Problem with BGP

BGP was created in 1989, before Internet security was a concern.

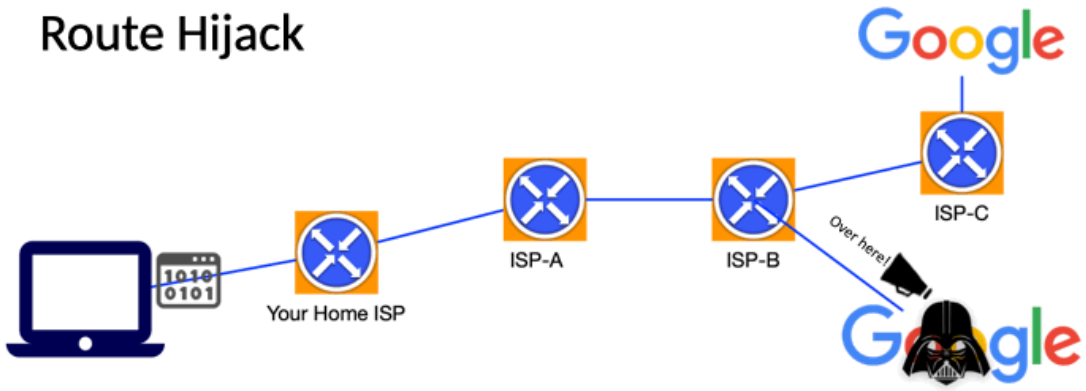
BGP assumes all networks are trustworthy. Any network can announce it has a path to any other network, even if it does not.

There is no built-in security mechanism to check if traffic is legitimate or not.

On today's Internet, this is a problem.

BGP is vulnerable to both malicious attacks and human mistakes.

Problem: BGP Hijacks



A network or attacker impersonates another network, pretending that a server or network is their client.

Result: Packets are forwarded to the wrong place; this can cause Denial of Service (DoS) attacks or traffic interception.

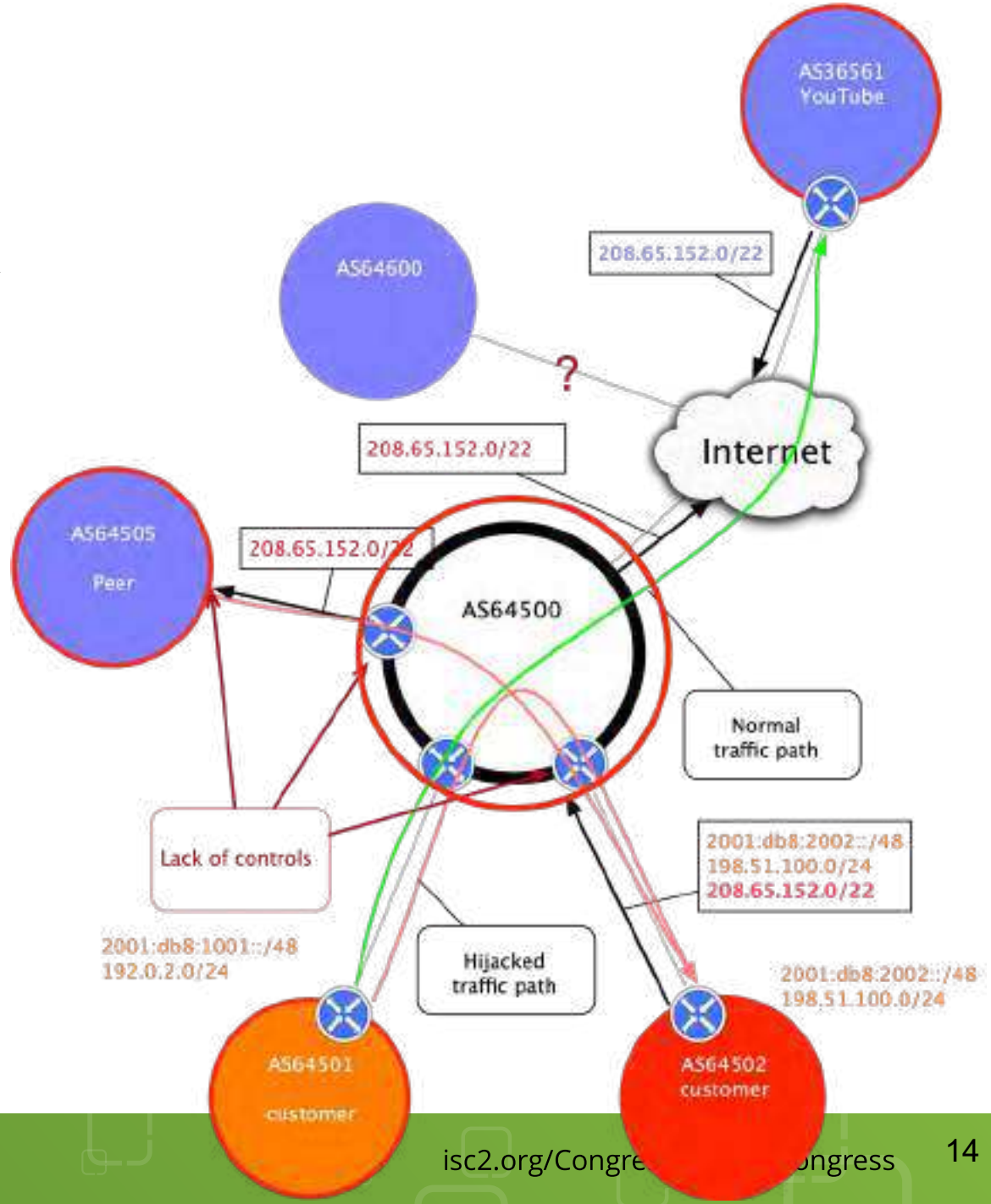
Hijacks are usually intentional.

Prefix/Route Hijacking

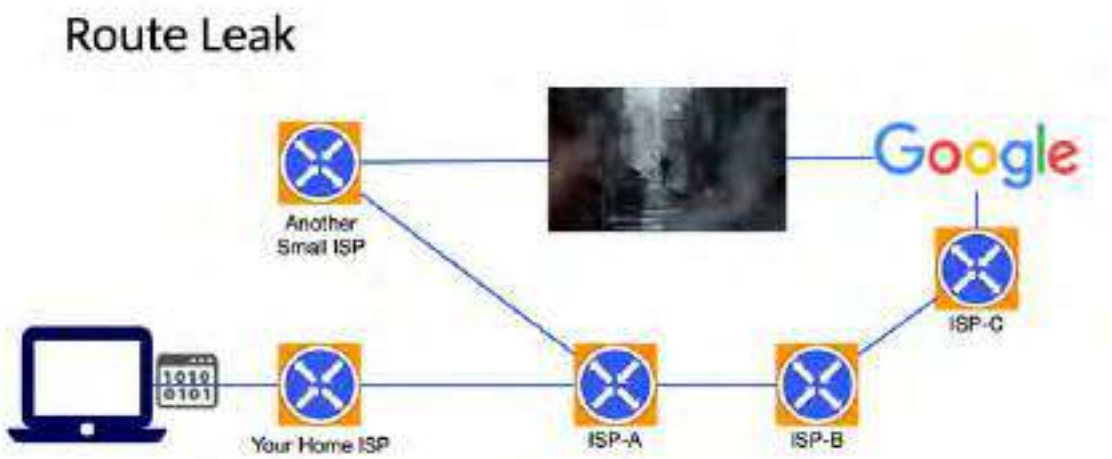
Route hijacking, also known as 'BGP hijacking', is when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretends that a server or network is their client. This routes traffic to the wrong network operator, when another real route is available.

Example: In 2008 an attempt to block YouTube through route hijacking led to much of the traffic to YouTube being dropped around the world.

Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting false announcements).



Problem: BGP Leak



A network or attacker advertises illegitimate IP prefixes, which propagate across networks and lead to incorrect or suboptimal routing.

Result: Packets can be redirected through a path that could enable eavesdropping or traffic analysis.

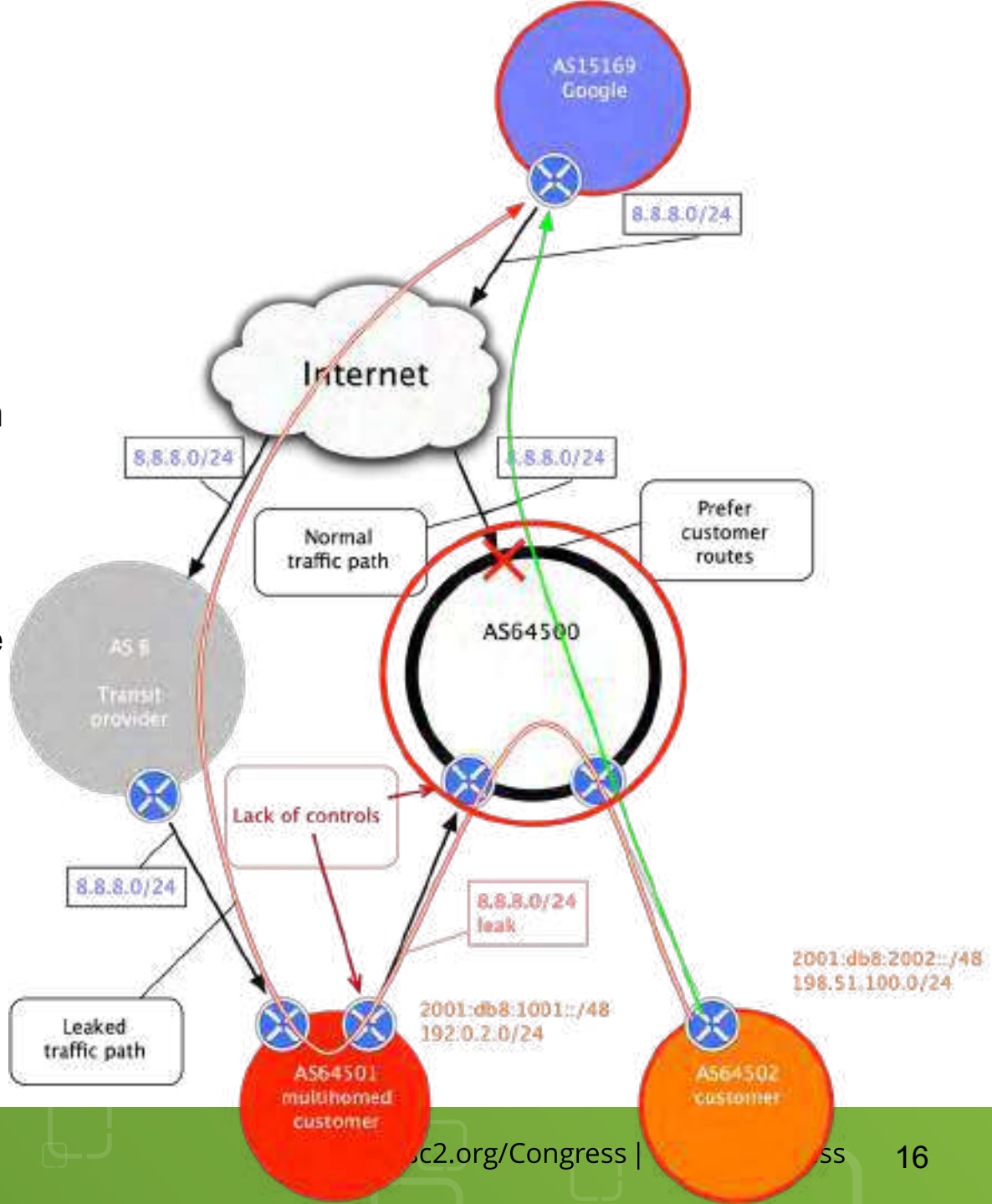
Leaks can be malicious, but are often accidental misconfigurations.

Route Leak

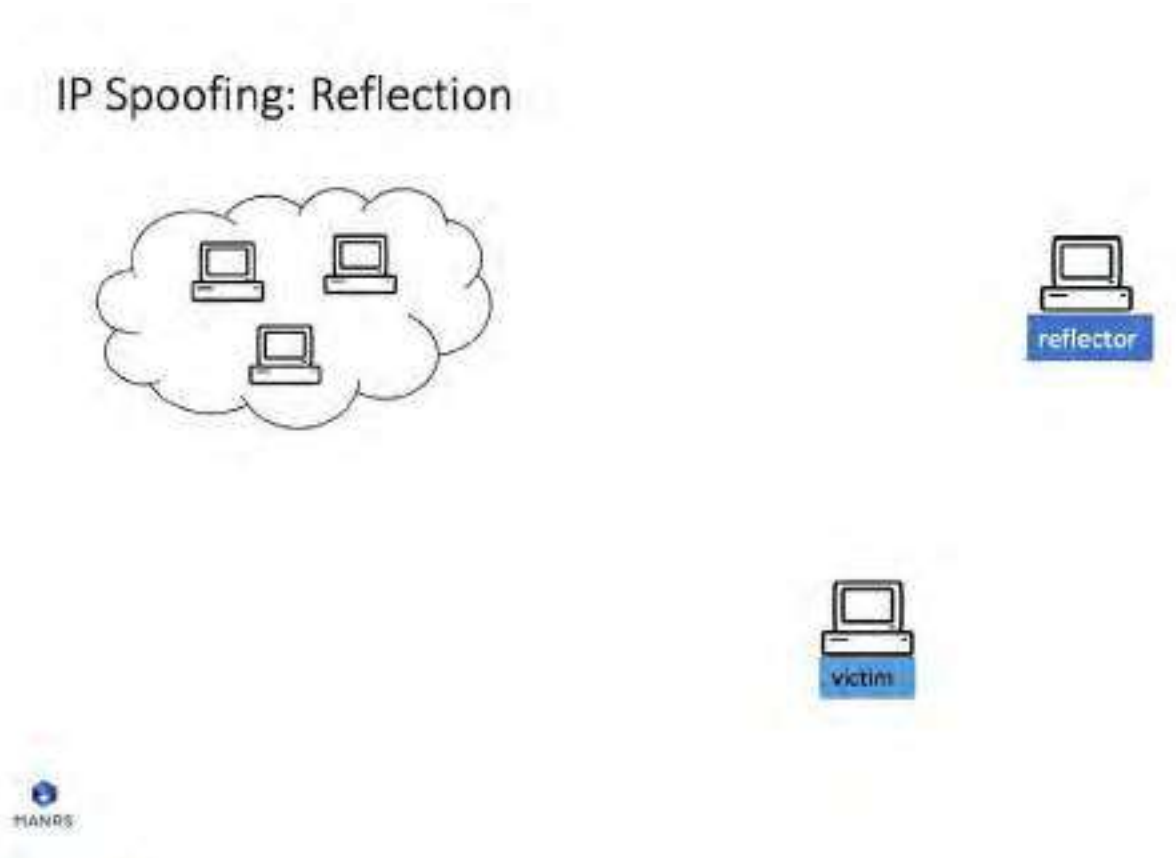
A route leak is where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that is has a route to a destination through the other upstream provider. This makes the network an intermediary network between the two upstream providers, with one sending traffic through the network to get to the other.

Example: In 2015, Malaysia Telecom told a network of Level 3 — a major backbone provider — that it was capable of delivering traffic anywhere on the Internet. Once Level 3 decided the route through Malaysia Telecom looked like the best option, it diverted a huge amount of traffic to Malaysia Telecom.

Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting announcements that don't make sense).



Problem: IP Address Spoofing



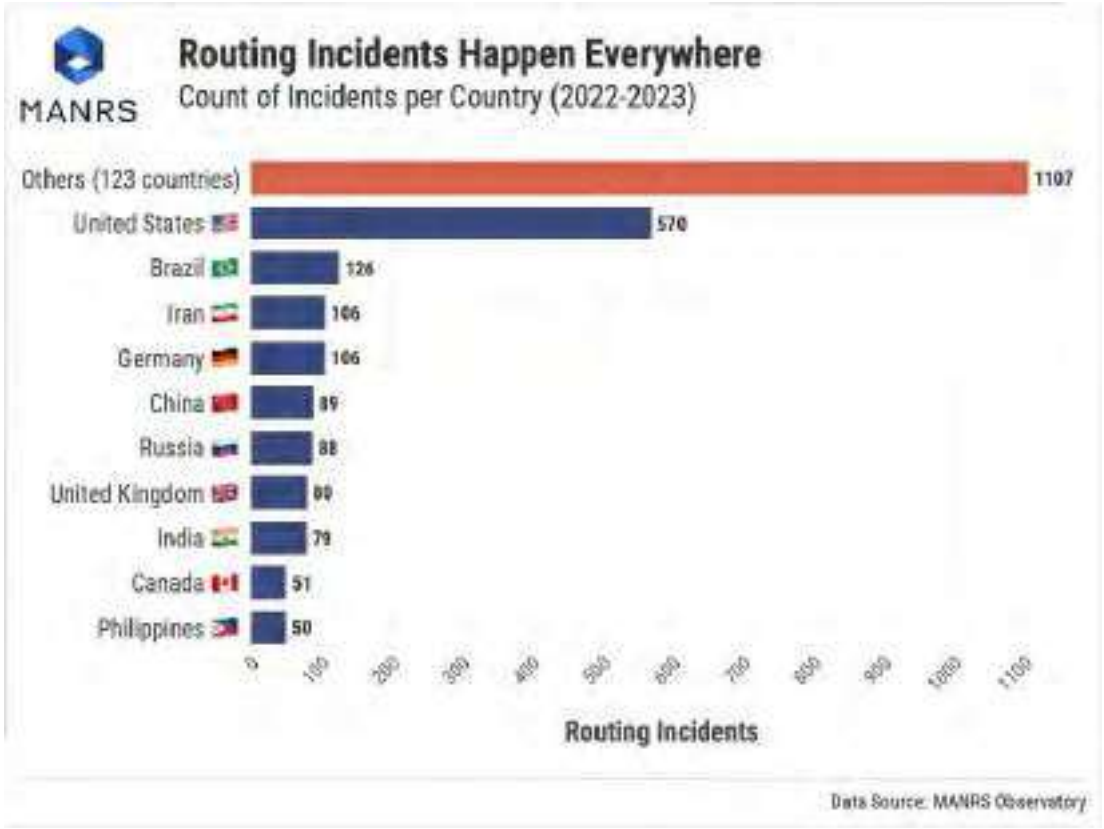
Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another network.

Result: Attackers magnify the amount of malicious traffic and obscure the sources of the attack traffic, causing a reflection DDoS attack.

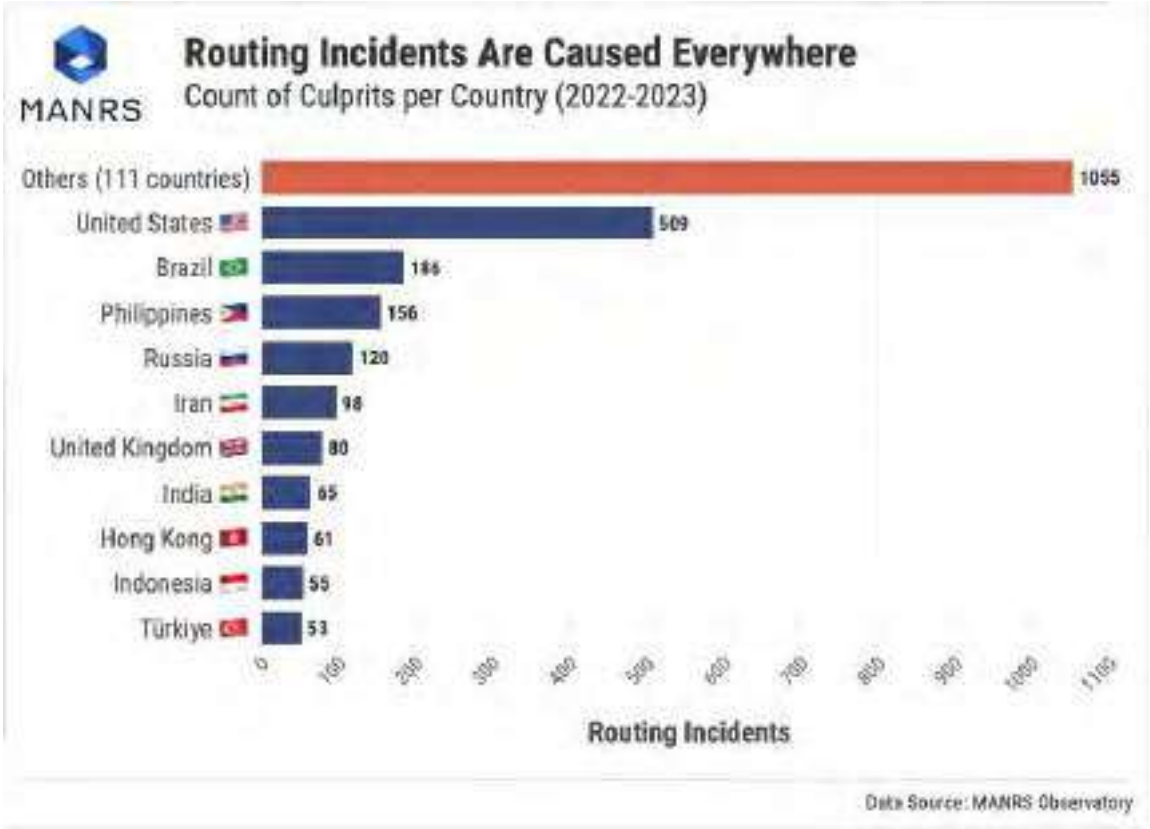
Fix: Source address validation can help tell if the end users and customer networks have correct source IP addresses (combined with filtering).

Routing Incidents Happen Everywhere

Number of incidents (a route leak or hijack) that affected networks in a country



Number of incidents (a route leak or hijack) that are caused by networks in a country

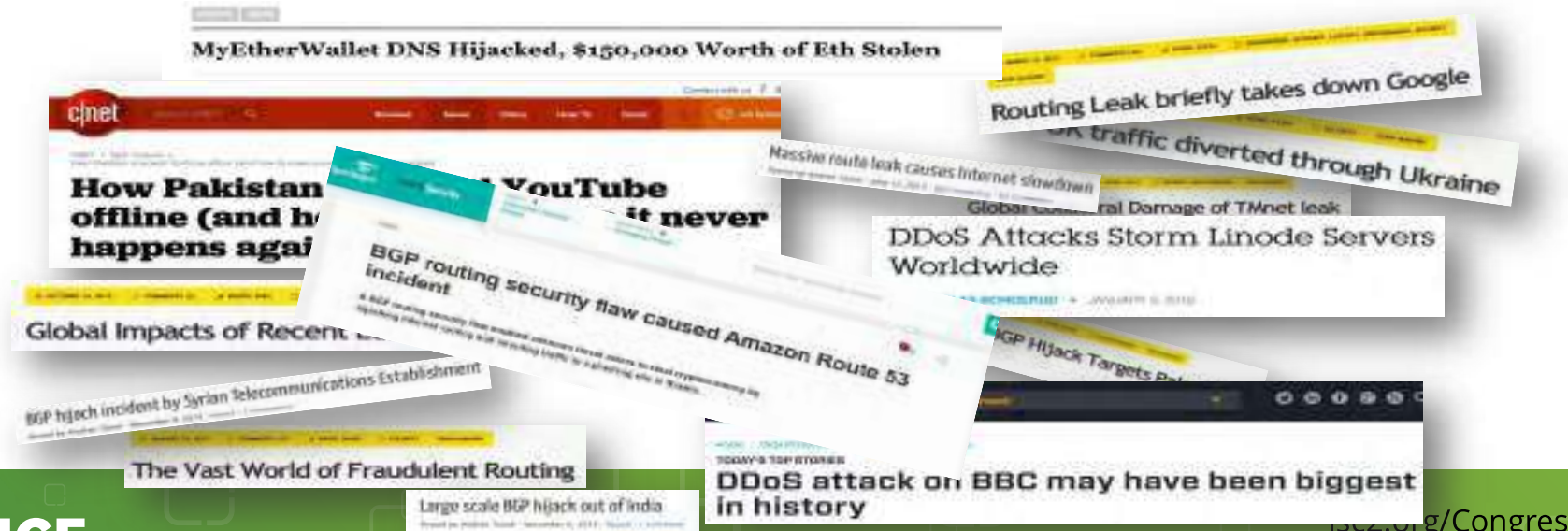


Routing Incidents Cause Real World Problems

Insecure routing is one of the most common paths for malicious threats.

Attacks can take anywhere from hours to months to recognize.

Inadvertent errors can take entire countries offline, while attackers can steal an individual's data or hold an organization's network hostage.



Why is Routing Security Hard?

Every network has a responsibility to implement basic routing security practices to mitigate threats.

But implementing best practices does not bring many immediate benefits. It costs time and money, and you probably can’t charge extra for it.

Even if you do everything right, your security is still in the hands of other networks.

This is a classic collective action problem.

Mutually Agreed Norms for Routing Security (MANRS)

Industry-led initiative of almost 1000 participating networks to implement best practices and collaborate toward a shared vision of a secure routing infrastructure.

MANRS provides concrete actions for Network Operators, IXPs, CDN/Cloud Providers & Vendors to reduce or eliminate the most common threats to routing.

There are no fees to join MANRS. MANRS is currently supported by the Internet Society.

MANRS

How to Improve Your Network

MANRS Actions

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

Routing Information

Publish your data, so others can validate routing information on a global scale

Tools

Provide monitoring and debugging tools to help others

Promotion

Actively encourage MANRS adoption among peers, customers, and partners

Routing Security Solutions

Filtering or Route Validation mitigates the risk of traffic being hijacked. When a router filters traffic, it checks that networks are only announcing the ASNs and IP prefixes they or their customers are legitimately authorized to originate.

Anti-spoofing prevents traffic with fake source IP addresses from leaving a network. This can help detect suspicious activity on your network (e.g. botnets).

Routing Information is telling other networks what to expect from you. This lets other networks protect traffic going to and from your network via filtering.

Coordination means ensuring your network has up-to-date contact information and responding in a timely fashion when incidents occur.

Routing Information: Help Others Help You

Internet Routing Registry (IRR)

Public databases where network operators publish their IP resources and routing policies.

Almost anyone can enter information, which leads to inconsistencies, stale data, and lack of real verification.

It isn't perfect, but it's better than nothing.

Resource Public Key Infrastructure (RPKI)

- A security layer that provides full cryptographic trust toward ownership where the owners have a publicly available identifier.
- Operators sign Route Origin Authorizations (ROAs), cryptographic assertions of which ASNs are authorized to originate which IP resources.
- RPKI allows much better route validation.
- It is newer and under-deployed.

We Are Making Progress

81% of all ASNs have their routes registered in an IRR and 27% in RPKI, and these numbers are growing.

Number of “culprits” – ASNs implicated in one or more suspicious routing events – is declining.

But there’s still a lot of work to do.

Data sources: MANRS Observatory, BGPStream, GRIP.

Government Interest

Improve Your Connectivity and Cloud Providers

You Are Not An Island

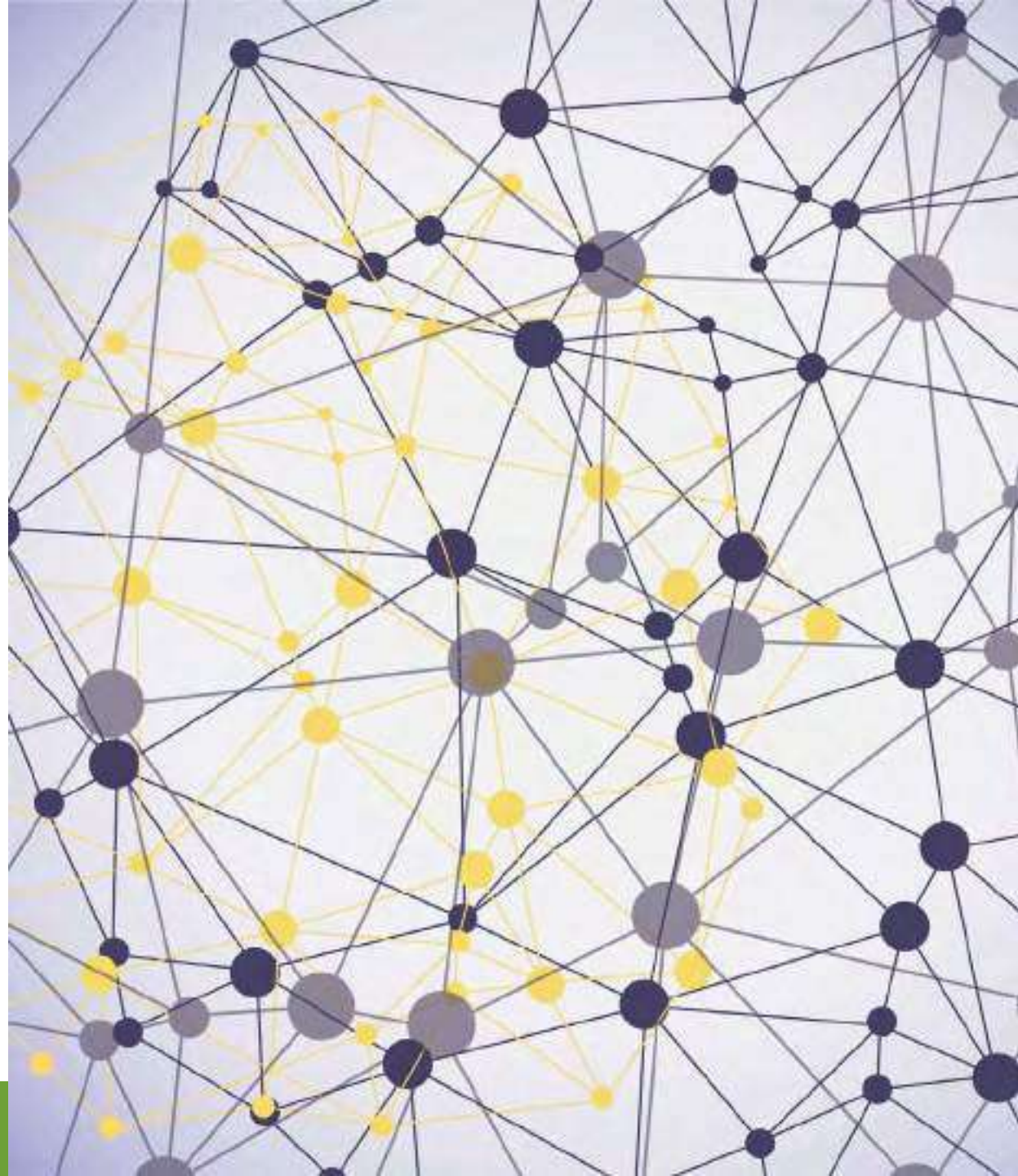
You are one of 75,000 intertwined networks on the Internet.

You use at least one Internet Service Provider. You most likely use some Cloud services.

It's important to use best practices on your network. It is even more important to choose connectivity and cloud providers that are committed to mitigating routing security threats.

Your connectivity or cloud provider could be your weakest link.

Routing security thus becomes an important part of your supply chain security.



Why Enterprises Should Require MANRS

To improve your organizational security posture

- MANRS-ready infrastructure partners increase security and service reliability, while eliminating common outages or attacks.
- Requiring MANRS adoption can help enterprises demonstrate due diligence and regulatory compliance.

To prevent and address security incidents

- Preventing traffic hijacking, detouring, and malicious traffic helps prevent data loss, denial of service, reputational damage, and more.
- Attacks and outages are resolved promptly by MANRS participants who are part of a broad network of security-minded operators.

MANRS provides a foundation for value-added services

- Incident information sharing and information feeds can directly impact the bottom line.
- Organizations can improve SLA compliance and address a host of routing deficiencies by simply seeking providers that adopt MANRS.

Back to KLAYswap

Repeat: This hijack could have been avoided - or at least minimized - if KakaoTalk had valid RPKI Route Origin Authorizations (ROAs) for its ASNs.

KLAYswap used a service with insecure routing infrastructure.

It cost them $1.9M.

These attacks happen surprisingly often.

BGP Insecurity Causes Real World Issues

3 Feb 2022	KLAYswap incident allows hackers to steal ~$1.9M USD in cryptocurrency assets
17 Apr 2021	Vodafone mistakenly announces 30K BGP routes causing a 13x increase in inbound traffic
1 Feb 2021	Myanmar military tries to block Twitter and accidentally hijacks Twitter's BGP traffic (Update: Twitter shored up its security!)
1 Apr 2020	Russian ISP Rostelecom announces prefixes belonging to Akamai, Cloudflare, Hetzner, Digital Ocean, Amazon AWS, and others
24 Jun 2019	Verizon caused outages at Cloudflare, Facebook, Amazon, and others after it wrongly accepted a network misconfiguration from a small ISP in Pennsylvania, USA.

https://www.manrs.org/2022/02/klayswap-another-bgp-hijack-targeting-crypto-wallets/
https://www.manrs.org/2021/04/a-major-bgp-hijack-by-as55410-vodafone-idea-ltd/
https://www.manrs.org/2021/02/did-someone-try-to-hijack-twitter-yes/
https://www.manrs.org/2022/03/lesson-learned-twitter-shored-up-its-routing-security/
https://www.manrs.org/2020/04/not-just-another-bgp-hijack/
https://www.manrs.org/2019/06/bgp-super-blunder-how-verizon-today-sparked-a-cascading-catastrophic-failure-that-knackered-cloudflare-amazon-etc/

Connectivity Providers and Enterprise Customers Must Work Together To Improve Routing Security

MANRS+

A second, elevated tier of MANRS participation for network operators that comply with more stringent requirements and auditing.

Work with industry partners to increase demand for security from their connectivity providers.

Connectivity Providers and their customers setting the requirements of the future quality mark for traffic security with the goal of eventually incorporating it in procurement policies and recommendations.

MANRS vs. MANRS+

MANRS

Established in 2014, nearly 1000 network operators, vendors, Internet exchange points, and CDN and cloud providers have joined.

Best practices including filtering, anti-spoofing, routing information, and coordination.

A security baseline – the bare minimum organizations of all sizes should be doing.

Historically, very little input from enterprise customers.

MANRS+

Currently in development by a MANRS+ Working Group. Please join!

Stronger and more detailed requirements enforcing best practices in traffic security.

High level of assurance of conformance. More profound technical audit and process audit.

Extended requirements, covering a broader set of risks related to routing and traffic security.

More focus on customer demands.

Proposed Requirements for MANRS+ Providers

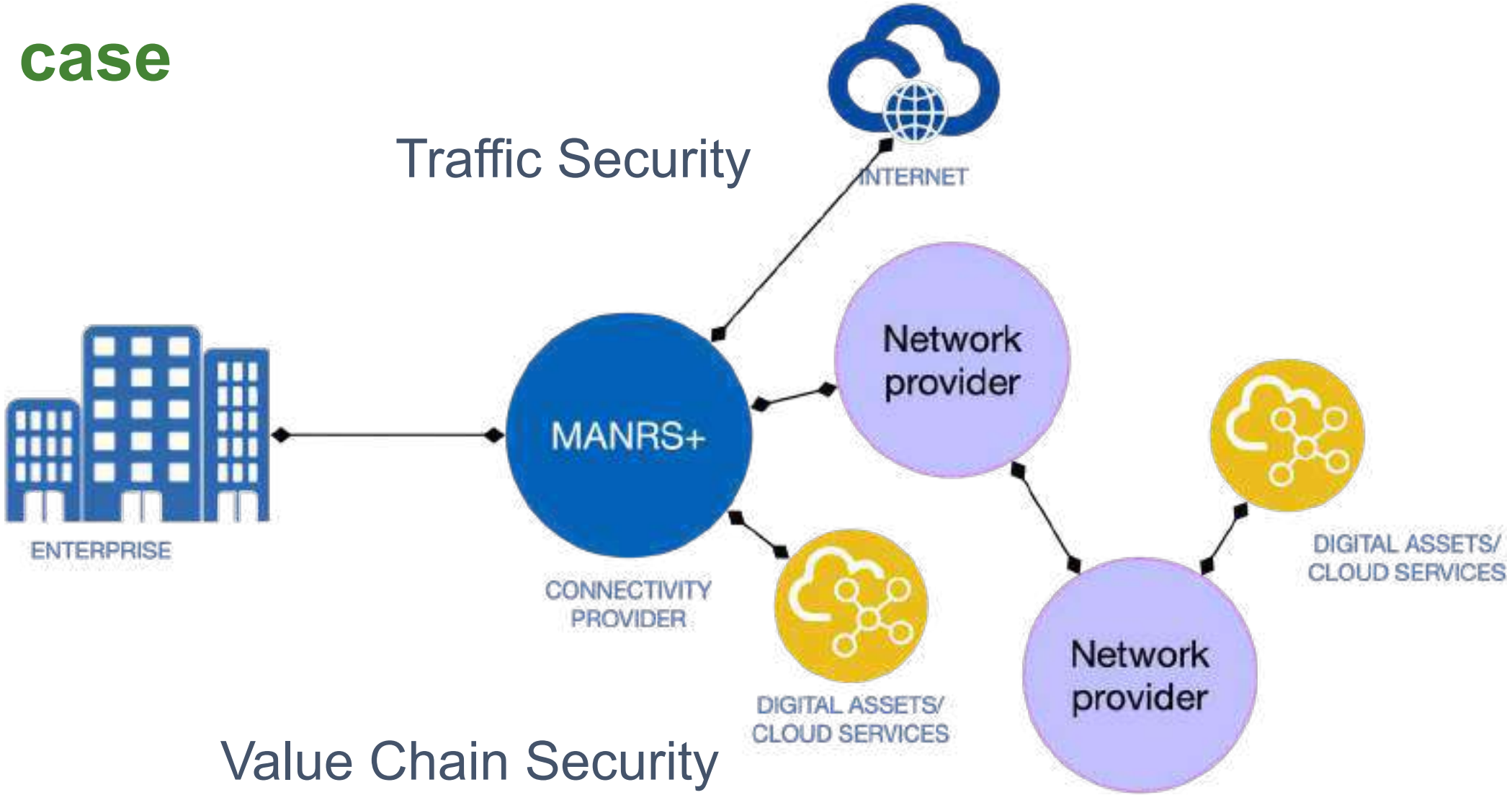
Path Security - Connectivity provider has detection capabilities and can mitigate the risk that traffic will be hijacked or detoured as a result of a mistake or an attack.

DDoS Attack Protection - Connectivity provider has detection and mitigating capabilities reducing the risk of a (volumetric) DoS attack.

Anti-Spoofing Protection - Connectivity provider detects and prevents traffic from their direct customers or peers with spoofed source IP addresses.

Routing Information - Connectivity provider has accessible complete and up-to-date documentation of the intended routing announcements (e.g. RPKI ROAs) and other information on its routing policy (e.g AS-SET) that is necessary for deploying effective security controls by the network.

A use case


Traffic Security
INTERNET
Network provider
MANRS+
ENTERPRISE
CONNECTIVITY PROVIDER
DIGITAL ASSETS/ CLOUD SERVICES
DIGITAL ASSETS/ CLOUD SERVICES
Network provider
Value Chain Security

Next Steps

Join the MANRS+ Working Group

Help identify your industry's needs and share what would make MANRS+ compelling to your business.

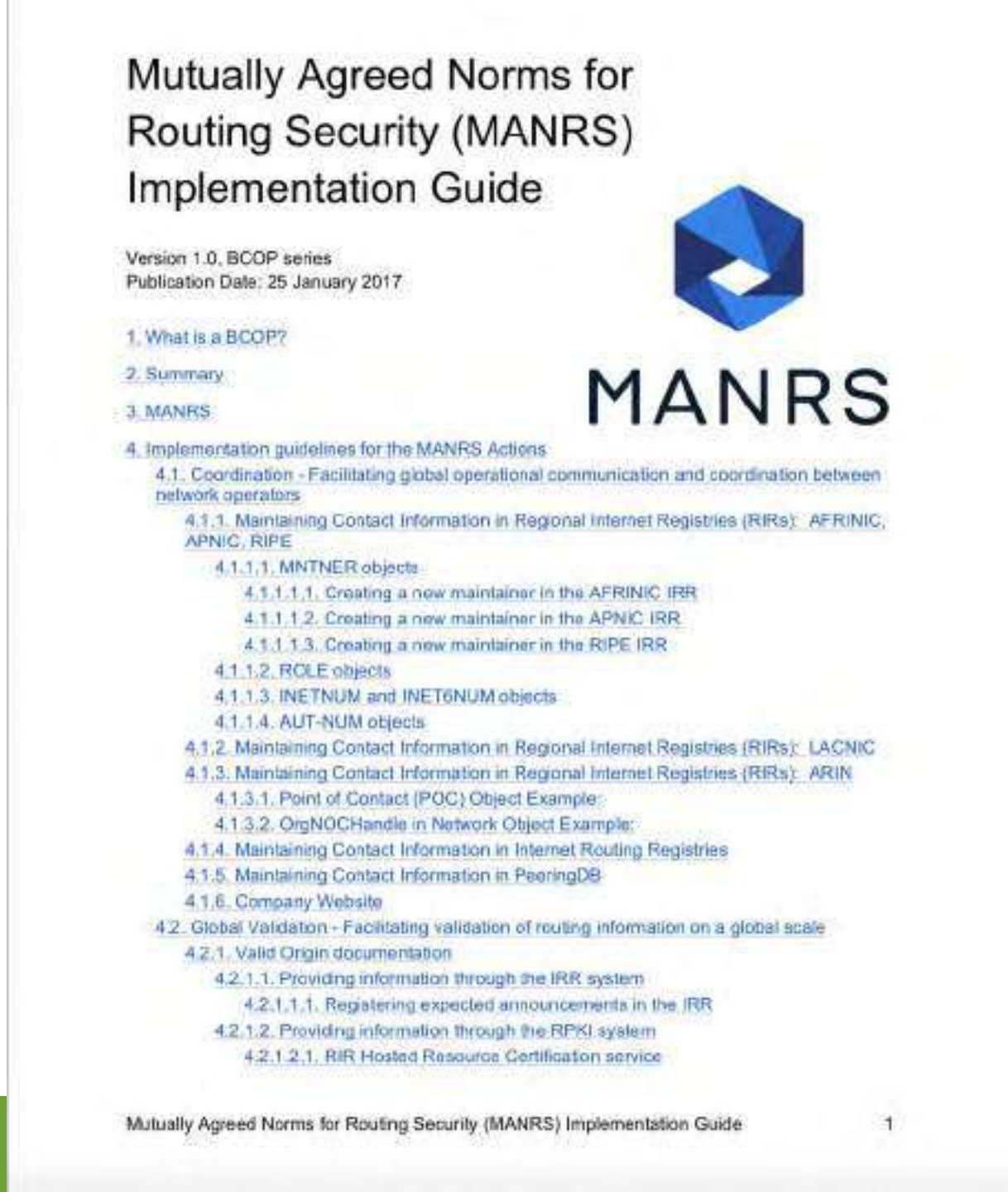
The group meets virtually 2x/month.

Membership is open to everyone. MANRS participation is not required.

MANRS Implementation Guide for Network Operators

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
- Recognition from the RIPE community by being published as RIPE-706
- https://www.manrs.org/bcop/



Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Version 1.0, BCOP series
Publication Date: 25 January 2017

MANRS

Many Tools To Help

- MANRS Observatory - https://observatory.manrs.org/
  - Specific ASN info available once you become a MANRS member

Spoofed IP Addresses

- CAIDA Spoofer - https://www.caida.org/projects/spoofer/

Filtering and Route Validation

- BGPQ4 - https://github.com/bgp/bgpq4
- BGP Filter Guides - https://bgpfilterguide.nlnog.net/
- IRR Power Tools - https://github.com/6connect/irrpt
- IRR Toolset - https://github.com/irrtoolset/irrtoolset (checks ROAs)

Tools To Help With RPKI

RPKI Verification

- Fort RPKI Validator - https://fortproject.net/en/validator
- Routinator - https://nlnetlabs.nl/projects/rpki/routinator/
- OpenBSD RPKI Client - https://www.rpki-client.org/
- MANRS ROA Stats - https://roa-stats.manrs.org/
- RPKI Documentation - https://rpki.readthedocs.io/

(many more links in MANRS Implementation Guide)

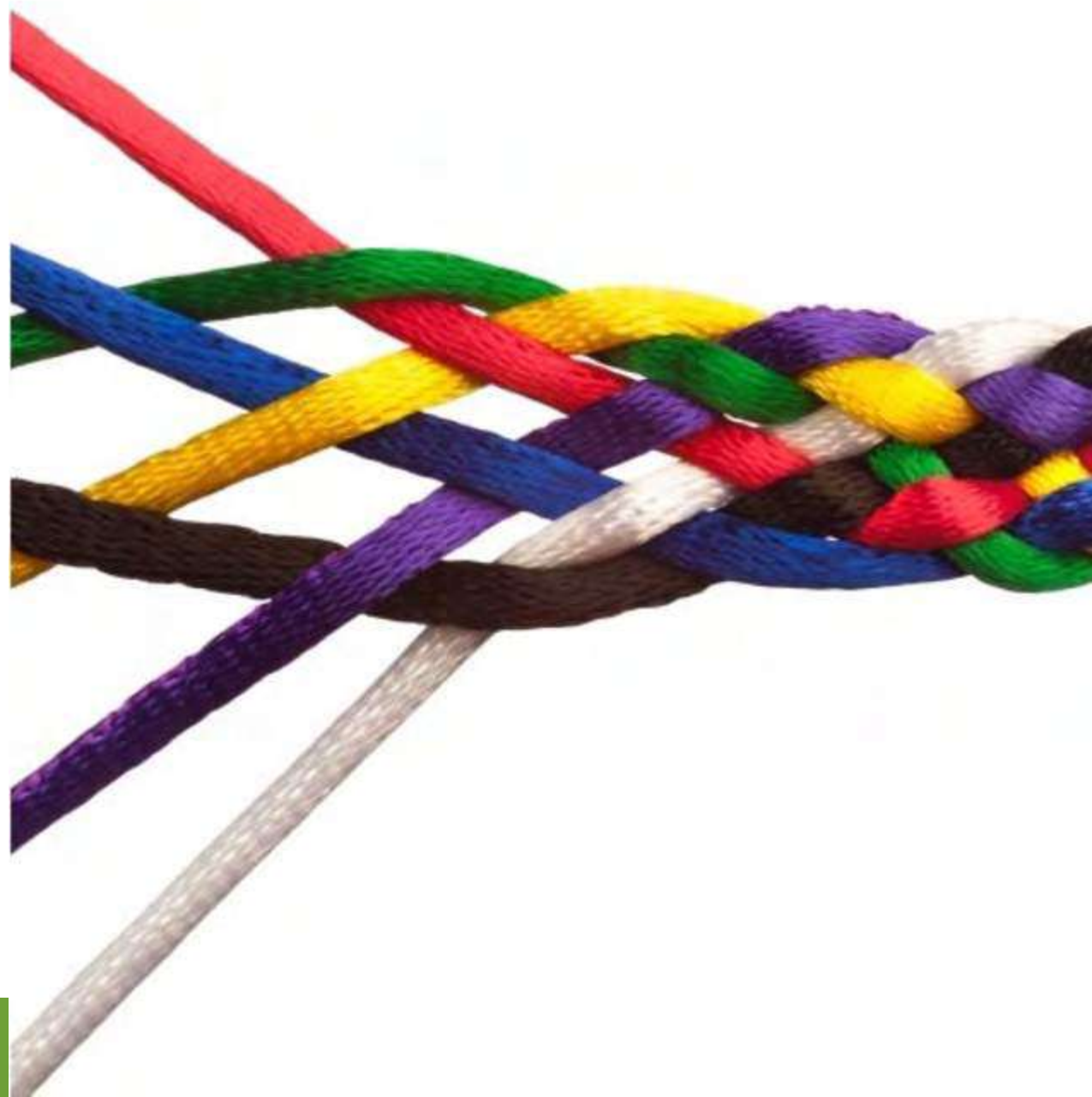
Join MANRS

Visit https://www.manrs.org and join as a network operator.

We can help you implement best practices:

- 1-pagers and primers for decision-makers
- Technical implementation guides
- Training courses
- MANRS Observatory & Tools

Contact us: contact@manrs.org



When You Go Home…

- Read more about MANRS compliance and implementation
- Ask your vendors / providers if they are MANRS-compliant
- Test (and fix) your own networks
  - Check for source address validation (ex CAIDA Spoofer)
  - Does the ASNs for the company's network(s) have ROAs?
  - Does the organization have correct info in an IRR or RIR database? Are those entries protected to whatever degree is possible so that an attacker could not put it bogus info?
  - Does your network propagate invalid routes? (**Be careful!**)
- Join MANRS!

Q&A

Question:

What do you see as the biggest threat to the Internet's future?

Please send thoughts to york@isoc.org

LEAD WITH

ISC2™ | SECURITY CONGRESS 2023

CONFIDENCE

isc2.org/Congress | #ISC2Congress

Thank You!

Dan York - york@isoc.org

Internet Society

Backup slides
(if people want specific info)

MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure.

MANRS sets a new norm for routing security.

MANRS Programs

- Network Operators
- Internet Exchange Points (IXPs)
- Content Delivery Networks (CDNs) and Cloud Providers
- Equipment Vendors

MANRS Network Operators Program

Launched in 2014 by a handful of network operators, the MANRS Network Operators program seeks to:

- Raise awareness of routing security problems and encourage the implementation of actions that can address them.
- Promote a culture of collective responsibility toward the security and resilience of the Internet's global routing system.
- Demonstrate the ability of the Internet industry to address routing security problems.
- Provide a framework for network operators to better understand and address issues relating to the security and resilience of the Internet's global routing system.

MANRS Actions for Network Operators

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 in common routing databases

Routing Information

Facilitate routing information on a global scale

Publish your data so others can validate

Gray shading = Mandatory Action

MANRS IXP Program

Internet Exchange Points (IXPs) are a collaborative focal point to discuss and promote the importance of routing security.

Launched in 2018, the IXP Program addresses the unique needs and concerns of IXPs with a separate set of MANRS actions.

IXPs can implement actions that demonstrate their commitment to routing security and bring significant improvement to the resilience and security of their peering relationships.

MANRS Actions for Internet Exchange Points

Action 1	Action 2	Action 3	Action 4	Action 5
Prevent propagation of incorrect routing information	Promote MANRS to the IXP membership	Protect the peering platform	Facilitate global operational communication and coordination	Provide monitoring and debugging tools to the members.
Implement filtering of route announcements at the Route Server based on routing information data (IRR and/or RPKI).	Provide encouragement or assistance for IXP members to implement MANRS actions.	Have a published policy of traffic not allowed on the peering fabric and perform filtering of such traffic.	Facilitate communication among members by providing necessary mailing lists and member directories.	Provide a looking glass for IXP members.

Gray shading = Mandatory Action

MANRS CDN and Cloud Program

Launched in 2020, the CDN and Cloud Provider Program helps by requiring egress routing controls so networks can prevent incidents from happening.

Leveraging CDNs' and cloud providers' peering power can have significant positive spillover effect on the routing hygiene of networks they peer with.

Goals include:

- Create a secure network peering environment
- Encourage better routing hygiene from peering partners
- Demonstrate responsible behavior
- Improve operational efficiency for peering interconnections, minimizing incidents and providing more granular insight for troubleshooting

MANRS Actions for CDNs & Cloud Providers

Action 1
Prevent propagation of incorrect routing information

Ensure correctness of own announcements and of their peers (non-transit) by implementing explicit (whitelist) filtering with prefix granularity.

Action 2
Prevent traffic with illegitimate source IP addresses

Implement anti-spoofing controls to prevent packets with illegitimate source IP address from leaving the network (egress filters).

Action 3
Facilitate global operational communication and coordination

Maintain globally accessible, up-to-date contact information in PeeringDB and relevant RIR databases.

Action 4
Facilitate validation of routing information on a global scale

Publicly document ASNs and prefixes that are intended to be advertised to external parties (IRR and/or RPKI)

Action 5
Encourage MANRS adoption

Actively encourage MANRS adoption among the peers.

Action 6
Provide monitoring and debugging tools to the peering partners

Provide a mechanism to inform peering partners if announcements did not meet the requirements of the peering policy.

Gray shading = Mandatory Action

MANRS Equipment Vendors Program

Launched in 2021, the Equipment Vendors Program outlines the support and training guidance vendors should offer to networks to more easily improve routing security.

Founding participants include global leaders in network equipment Arista, Cisco, Huawei, Juniper, and Nokia,

Routing security problems are multifaceted and good collaboration between network operators and equipment vendors is crucial. Both groups see MANRS as a neutral and trusted platform to facilitate an array of ongoing activities, from advising operators on how to use routing equipment features to developing solutions for identified problem statements.

MANRS Actions for Equipment Vendors

Action 1

Provide solutions for the implementation of specific MANRS Actions by other participants

Include routing security features in network equipment

Action 2

Promote MANRS through training and technical content

Reference MANRS and its implementation in relevant training courses, labs, and/or technical resources

Participate in the community*

Advise MANRS participants and respond to their problem statements, as well as contribute to MANRS resources and promote the program.

(*Not a formal Action)

Gray shading = Mandatory Action

MANRS Observatory

MANRS Observatory

Provides a factual state of security and resilience of the Internet routing system and tracks it over time

Measurements are:

- Transparent – using publicly accessible data.
- Passive – no cooperation from networks required.
- Evolving – MANRS community decide what gets measured and how.

MANRS Observatory Access

Publicly launched in August 2019

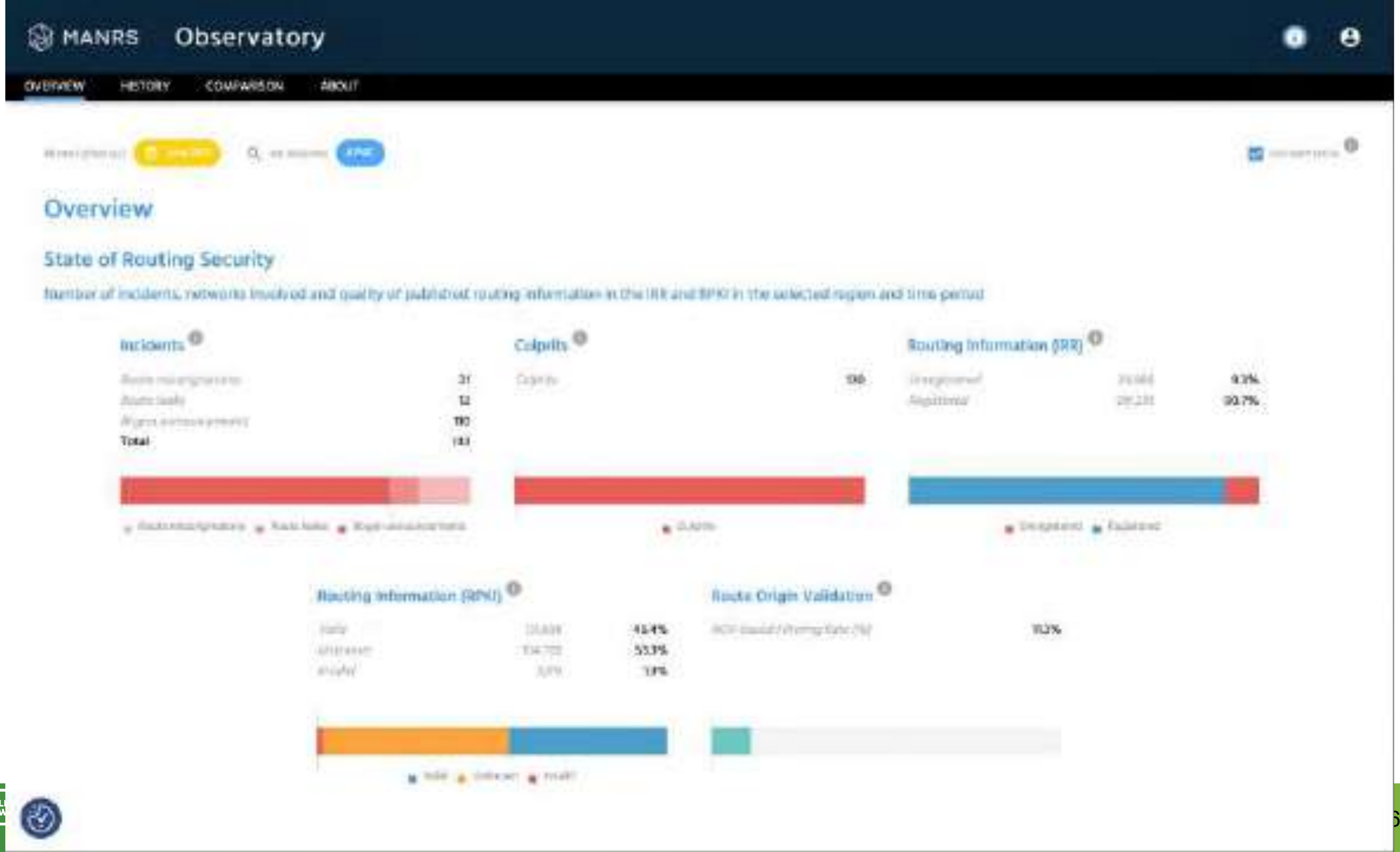
Uses trusted, publicly available third-party data

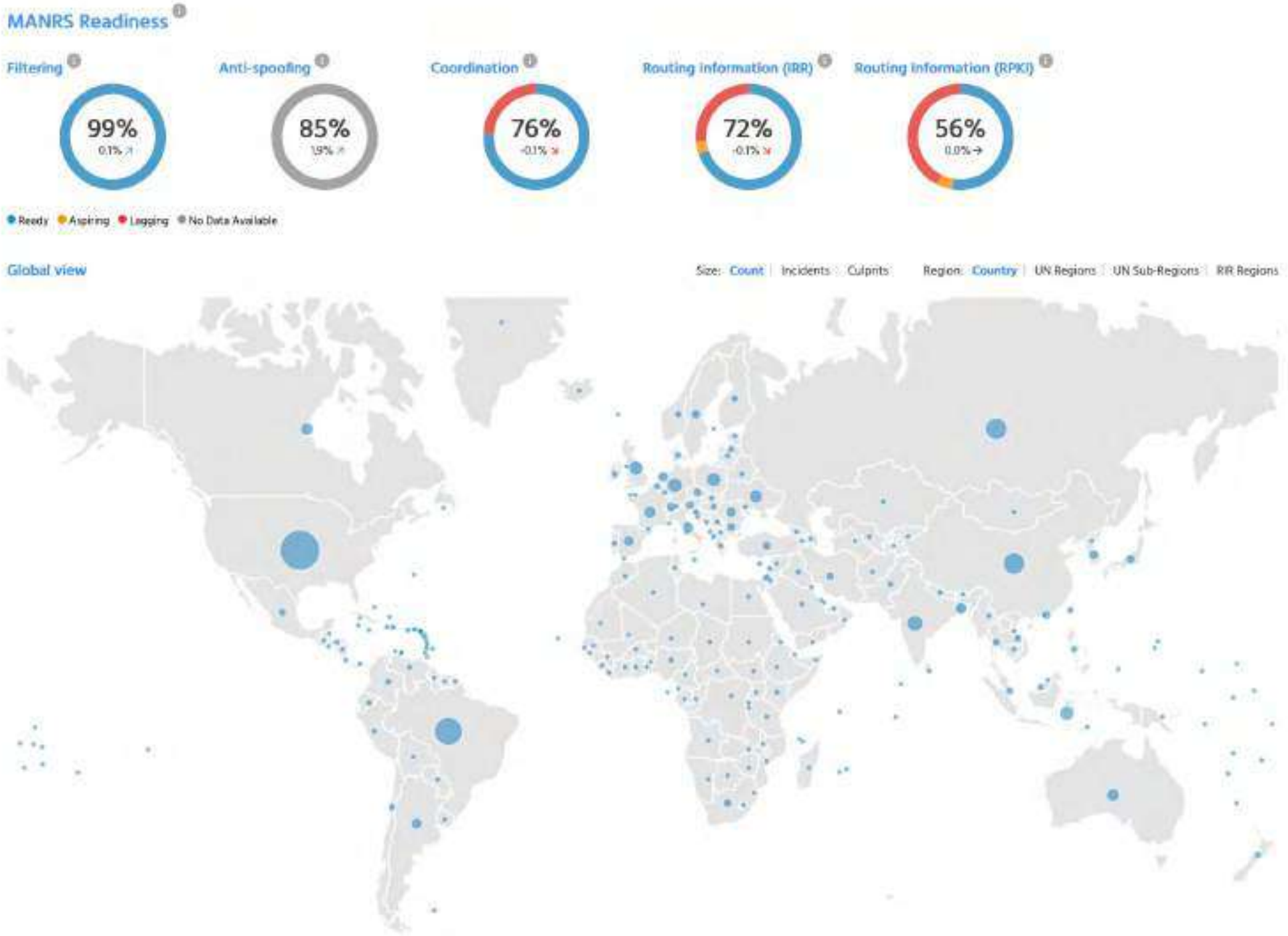
Anyone may view aggregated data

Only MANRS Participants have access to detailed data about their own network

Caveats:

- There are still some false positives
- Lack of security controls is not always visible


MANRS Observatory
OVERVIEW
HISTORY
COMPARISON
ABOUT
Overview
State of Routing Security
Incidents
Culprits
Routing Information (IRR)
Routing Information (RPKI)
Route Origin Validation


MANRS Readiness
Filtering
99%
0.1%
Anti-spoofing
85%
Coordination
76%
-0.1%
Routing information (IRR)
72%
-0.1%
Routing information (RPKI)
56%
0.0%
Ready
Aspiring
Lagging
No Data Available
Global view
Size: Count | Incidents | Culprits
Region: Country | UN Regions | UN Sub-Regions | RR Regions