MANRS

Mutually Agreed Norms for Routing Security

Aftab Siddiqui

siddiqui@isoc.org

The Problem

A Routing Security Overview

Routing Incidents are Increasing

In 2017 alone, 14,000 routing outages or attacks – such as hijacking, leaks, and spoofing – led to a range of problems including stolen data, lost revenue, reputational damage, and more.

About 40% of all network incidents are attacks, with the mean duration per incident lasting 19 hours.

Incidents are global in scale, with one operator’s routing problems cascading to impact others.

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 even recognize.

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

The Basics: How Routing Works

There are ~60,000 networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks.

Routers use Border Gateway Protocol (BGP) to exchange “reachability information” - networks they know how to reach.

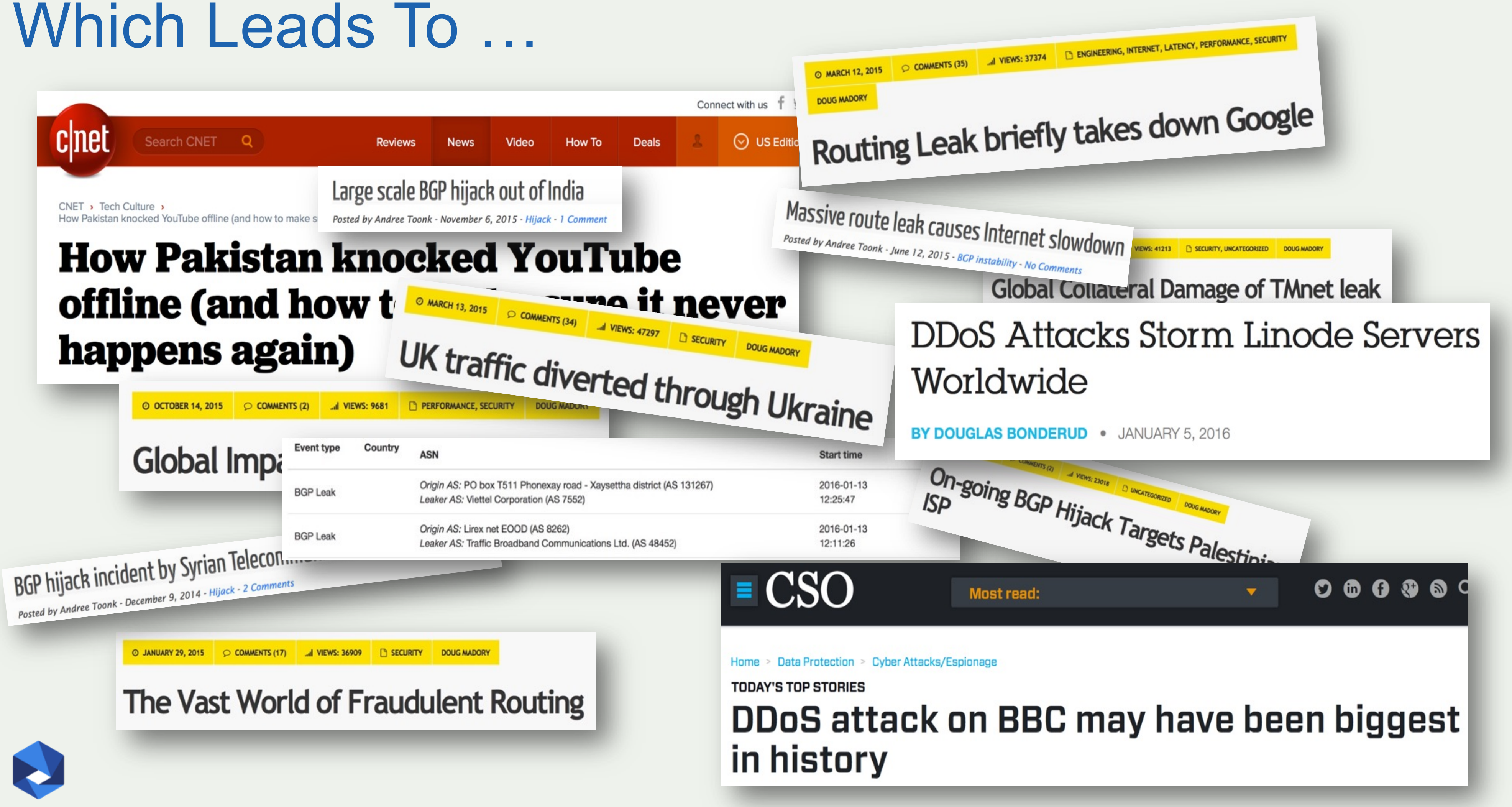
Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path.

The Honor System: Routing Issues

Border Gateway Protocol (BGP) is based entirely on trust between networks

- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data

Which Leads To …



Connect with us

c|net

Search CNET

Reviews News Video How To Deals US Editio

CNET › Tech Culture ›
How Pakistan knocked YouTube offline (and how to make s

How Pakistan knocked YouTube offline (and how t ure it never happens again)

Large scale BGP hijack out of India

Posted by Andree Toonk - November 6, 2015 - Hijack - 1 Comment

MARCH 12, 2015 | COMMENTS (35) | VIEWS: 37374 | ENGINEERING, INTERNET, LATENCY, PERFORMANCE, SECURITY | DOUG MADORY

Routing Leak briefly takes down Google

Massive route leak causes Internet slowdown

Posted by Andree Toonk - June 12, 2015 - BGP instability - No Comments

VIEWS: 41213 | SECURITY, UNCATEGORIZED | DOUG MADORY

Global Collateral Damage of TMnet leak

MARCH 13, 2015 | COMMENTS (34) | VIEWS: 47297 | SECURITY | DOUG MADORY

UK traffic diverted through Ukraine

DDoS Attacks Storm Linode Servers Worldwide

BY DOUGLAS BONDERUD • JANUARY 5, 2016

OCTOBER 14, 2015 | COMMENTS (2) | VIEWS: 9681 | PERFORMANCE, SECURITY | DOUG MADORY

Global Impa

Event type	Country	ASN	Start time
BGP Leak		*Origin AS:* PO box T511 Phonexay road - Xaysettha district (AS 131267) *Leaker AS:* Viettel Corporation (AS 7552)	2016-01-13 12:25:47
BGP Leak		*Origin AS:* Lirex net EOOD (AS 8262) *Leaker AS:* Traffic Broadband Communications Ltd. (AS 48452)	2016-01-13 12:11:26

COMMENTS (2) | VIEWS: 23018 | UNCATEGORIZED | DOUG MADORY

On-going BGP Hijack Targets Palestinia ISP

BGP hijack incident by Syrian Telecom

Posted by Andree Toonk - December 9, 2014 - Hijack - 2 Comments

JANUARY 29, 2015 | COMMENTS (17) | VIEWS: 36909 | SECURITY | DOUG MADORY

The Vast World of Fraudulent Routing

CSO

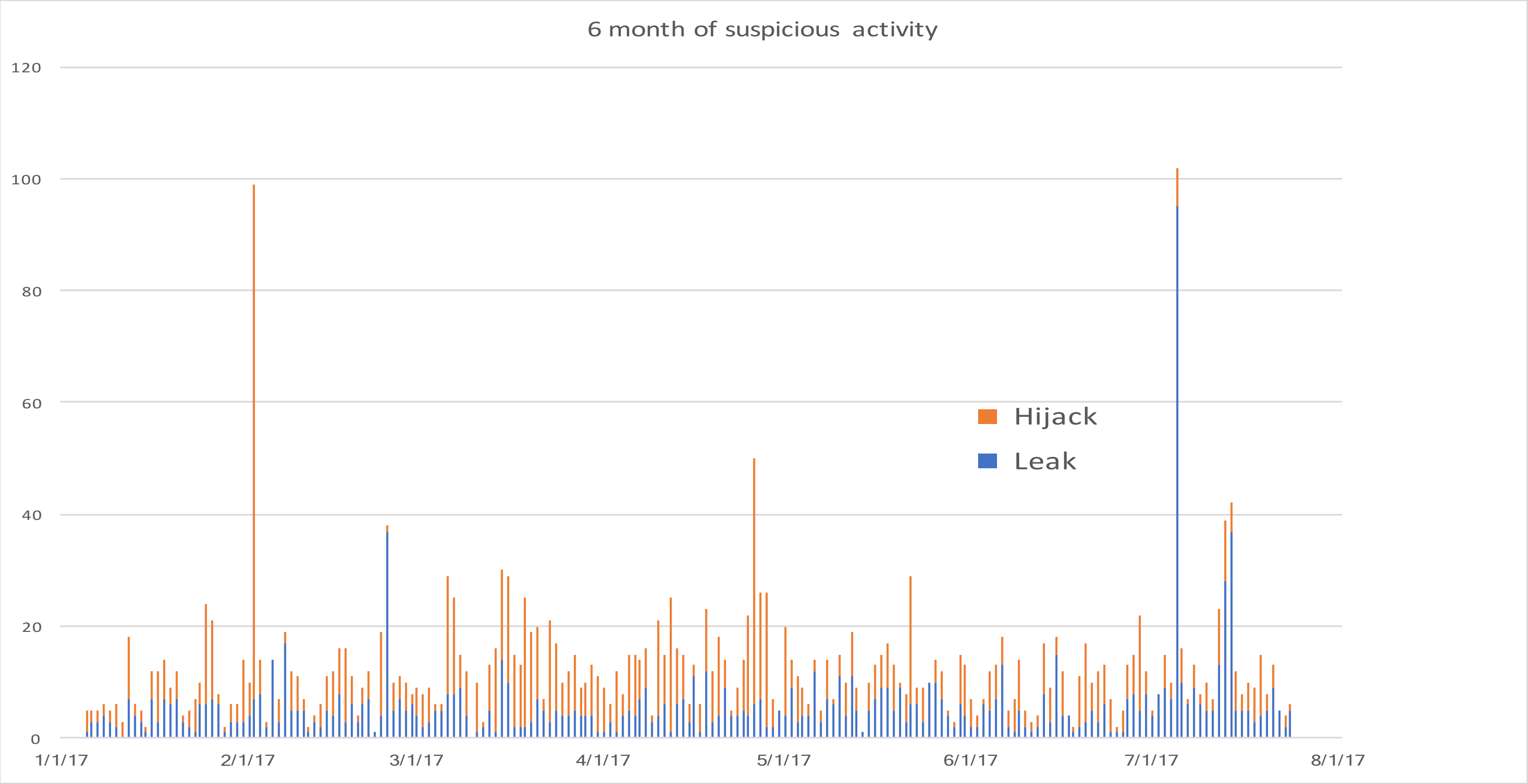
Most read:

Home > Data Protection > Cyber Attacks/Espionage

TODAY'S TOP STORIES

DDoS attack on BBC may have been biggest in history

No Day Without an Incident



http://bgpstream.com/

The Threats: What's Happening?

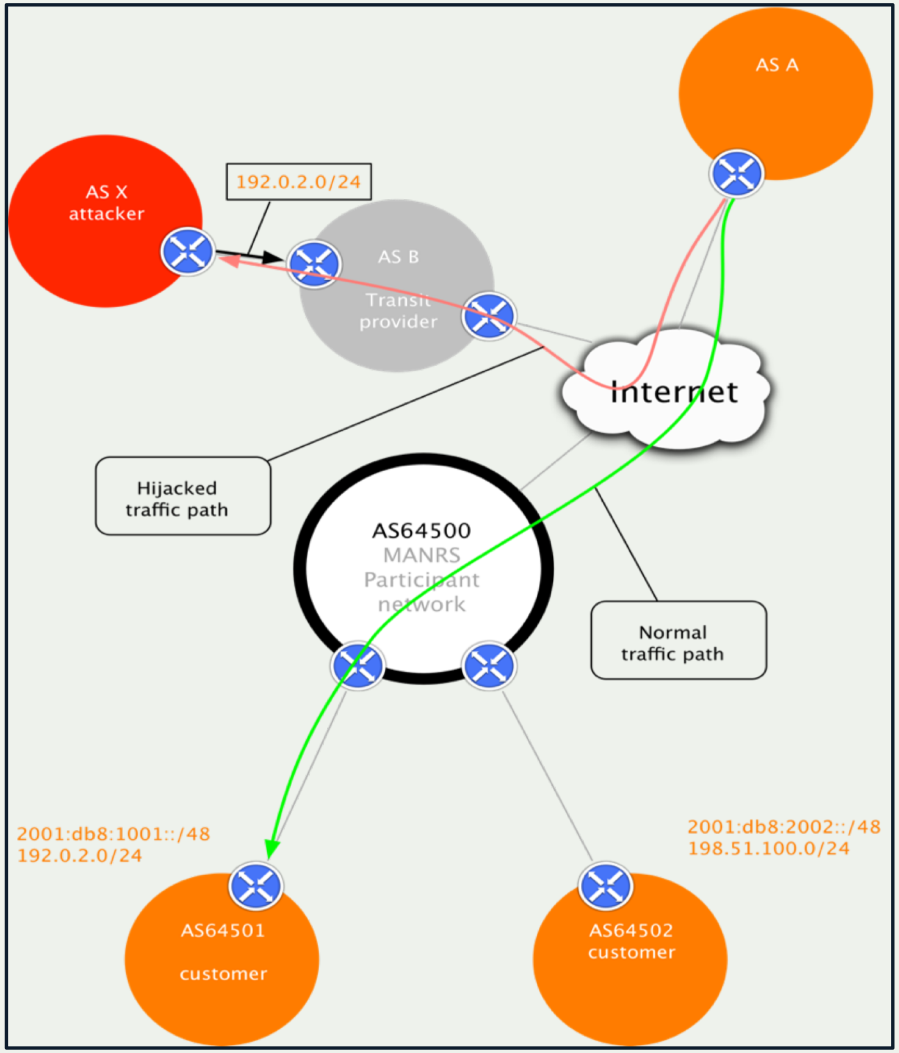
Event	Explanation	Repercussions	Solution
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	Stronger filtering policies
Route Leak	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for traffic inspection and reconnaissance.	Stronger filtering policies
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.	The root cause of reflection DDoS attacks	Source address validation

Prefix/Route Hijacking

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

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

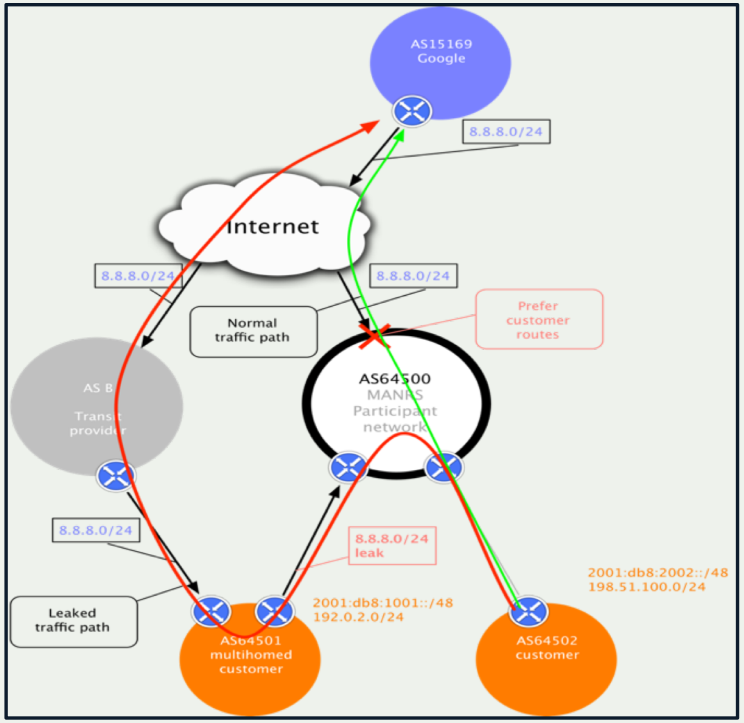
Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting false announcements).



Route Leak

A route leak is a problem where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that 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 now through it to get to the other.

Example: 2015, Malaysia Telecom and Level 3, a major backbone provider. Malaysia Telecom told one of Level 3's networks that it was capable of delivering traffic to 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.



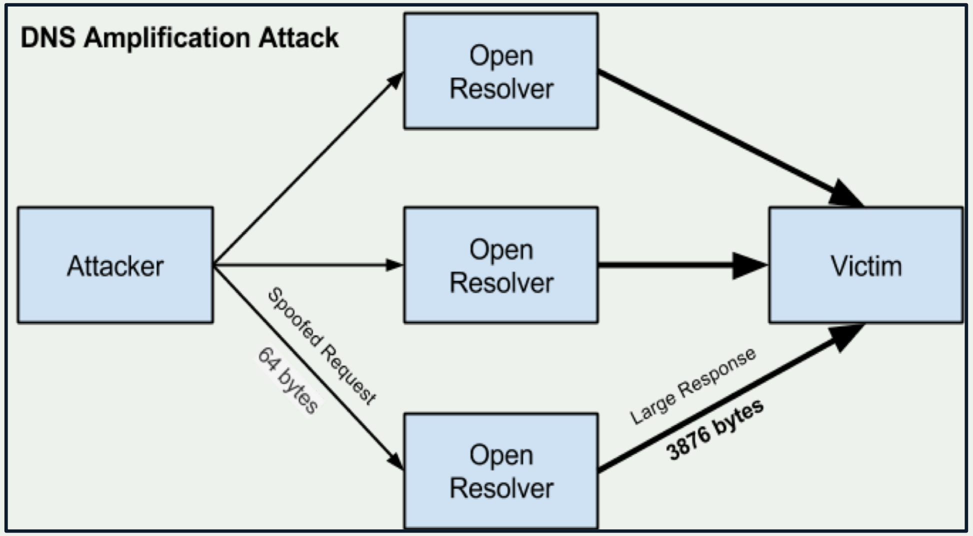
Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting announcements that don't make sense).

IP Address Spoofing

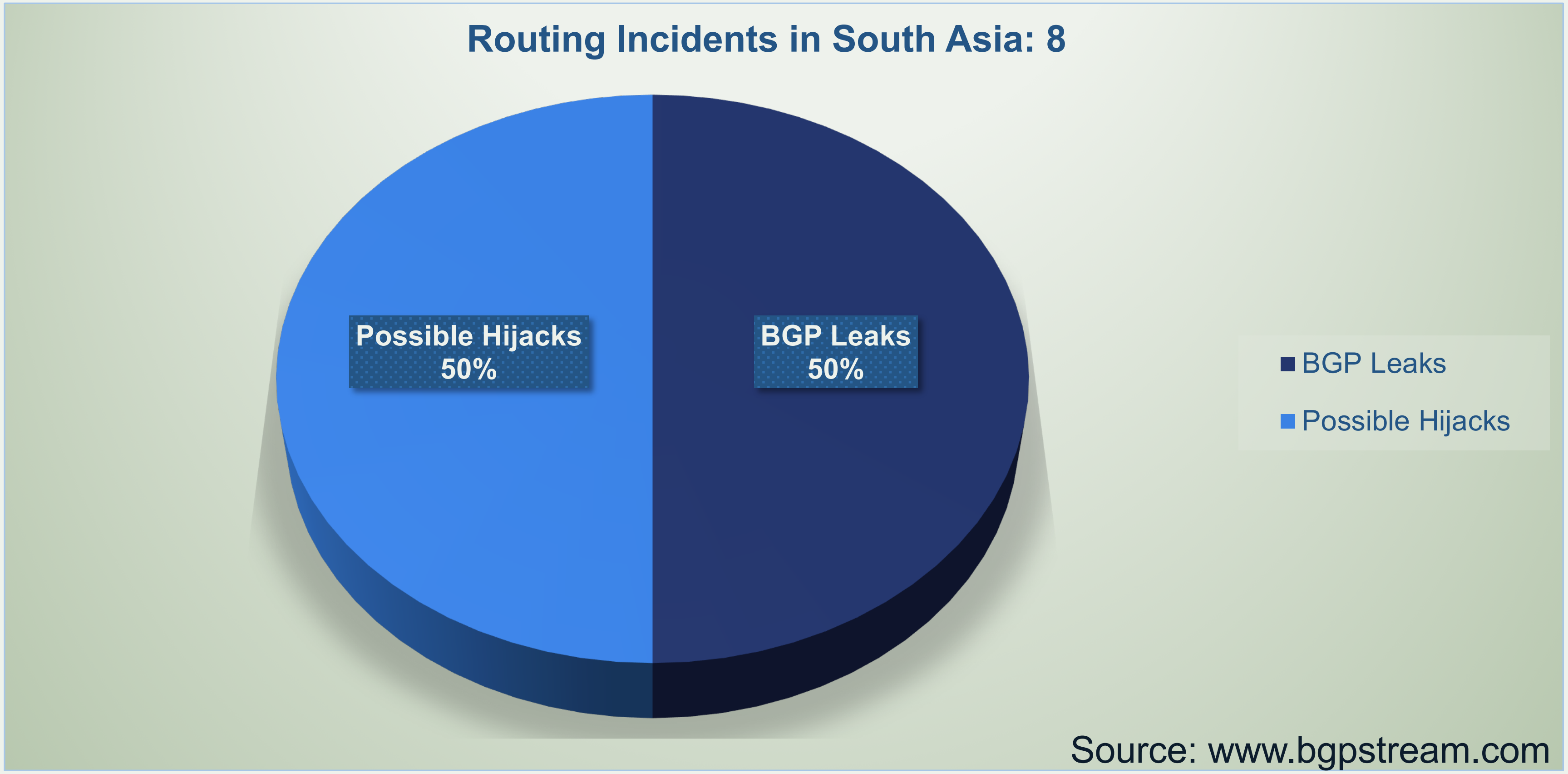
IP address spoofing is used to hide the true identity of the server or to impersonate another server. This technique can be used to amplify an attack.

Example: DNS amplification attack. By sending multiple spoofed requests to different DNS resolvers, an attacker can prompt many responses from the DNS resolver to be sent to a target, while only using one system to attack.

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



Routing Incidents (SA): 1st August 2018 – 7th August 2018



Source: www.bgpstream.com

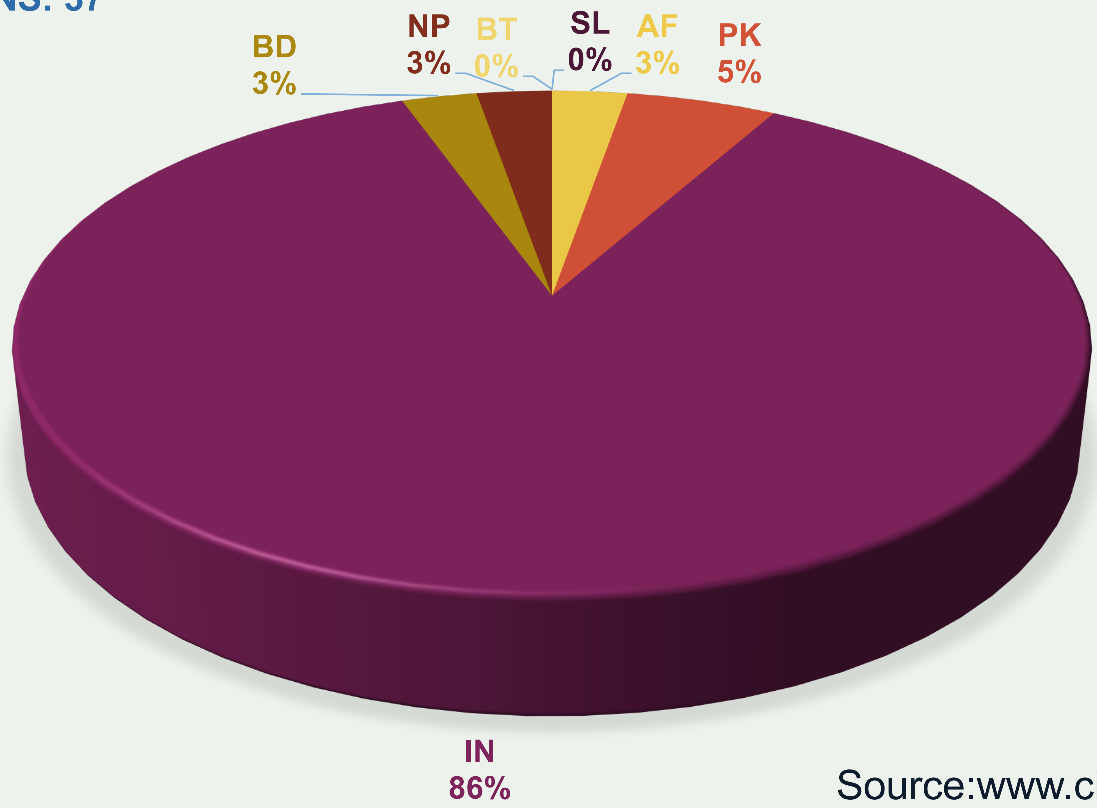
Routing Incidents (SA): 1st August 2018 – 7th August 2018

Event Type	Event Details	ASN
BGP Leak	Origin AS: MOON-AS-AP MOON NET, BD	AS136217
	Leaker AS: AAMRA-ATL-BD Aamra technologies limited, BD	AS58601
Possible Hijack	Expected Origin AS: GIGANTIC-AS Gigantic Infotel Pvt Ltd, IN	AS133275
	Detected Origin AS: ANINETWORK-IN Ani Network Pvt Ltd, IN	AS132116
BGP Leak	Origin AS: PANDORA-TECHNOLOGY-AS-AP Pandora Technology, BD	AS135517
	Leaker AS: AAMRA-ATL-BD Aamra technologies limited, BD	AS58601
BGP Leak	Origin AS:INFO-INTERNET-AS-AP Info Internet Service, BD	AS136267
	Leaker AS: AAMRA-ATL-BD Aamra technologies limited, BD	AS58601
Possible Hijack	Expected Origin AS: HOSTPALACE-IN HostPalace Web Solution Private Limited, IN	AS133229
	Detected Origin AS: HOSTPALACE-EU HostPalace Web Solution Private Limited, NL	AS134512
Possible Hijack	Expected Origin AS: GEOTEL-IT-AS-AP Geotel Bangladesh IT Ltd., BD	AS134552
	Detected Origin AS: AT TOKYO AT TOKYO Corporation, JP	AS9999
Possible Hijack	Expected Origin AS: GEOTEL-IT-AS-AP Geotel Bangladesh IT Ltd., BD	AS134552
	Detected Origin AS: AT TOKYO AT TOKYO Corporation, JP	AS9999
BGP Leak	Origin AS: MSI-AS-AP Sharmin Akter Shilpi t/a M/S. Saiba International, BD	AS135604
	Leaker AS: AAMRA-ATL-BD Aamra technologies limited, BD	AS58601

Source: www.bgpstream.com

Routing Incidents (Bogons): 8th August 2018

TOTAL BOGONS: 37



Source:www.cidr-report.org

Afghanistan

Unallocated ASN

AS58469 Announced by AS55330
GCN-DCN-AS AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK, AF

Pakistan

Unallocated ASN

AS15347 Announced by AS17557
PKTELECOM-AS-PK Pakistan Telecommunication Company Limited, PK

AS15347 Announced by AS38193
TWA-AS-AP Transworld Associates (Pvt.) Ltd., PK

Source:www.cidr-report.org

Nepal

Unallocated IPv6 Prefix

2400:4f80::/32 AS133149
KONNECTNEPAL-AS-AP Konnect Nepal Networks Pvt Ltd, NP

Bangladesh

Unallocated ASN

AS136555 Announced by AS58717 SUMMITCOMMUNICATIONS-BD Summit Communications Ltd, BD

Source:www.cidr-report.org

India

Unallocated ASN

AS23937 Announced by AS45820 TTSL-MEISISP Tata Teleservices ISP AS, IN

Unallocated IPv4 Prefix

45.251.14.0/24	AS135743	MAXX1-AS-IN Maxx1 Infoway Pvt Ltd, IN
103.48.112.0/24	AS132754	REALTEL-AS-IN Realtel Network Services Pvt Ltd, IN
103.48.113.0/24	AS132754	REALTEL-AS-IN Realtel Network Services Pvt Ltd, IN
103.48.114.0/24	AS132754	REALTEL-AS-IN Realtel Network Services Pvt Ltd, IN
103.48.115.0/24	AS132754	REALTEL-AS-IN Realtel Network Services Pvt Ltd, IN
103.49.236.0/22	AS133715	YPT-AS YPT Entertainment House Pvt Ltd, IN
103.66.168.0/24	AS135719	LMES-AS Lm Energy And Software Private Limited, IN
103.73.216.0/22	AS133987	PRACHAR-AS Pracharnama Media Pvt Ltd, IN
103.78.187.0/24	AS134302	WISPL-AS Wizone Internet Services Pvt. Ltd., IN
103.82.48.0/22	AS132779	RACKBANK-AS RackBank Datacenters Private Ltd, IN

Source:www.cidr-report.org

India

Unallocated IPv4 Prefix

103.206.174.0/24	AS134934	GLAN-AS GLAN SOLUTION INDIA PVT LTD, IN
103.206.175.0/24	AS134934	GLAN-AS GLAN SOLUTION INDIA PVT LTD, IN
103.207.103.0/24	AS58762	CANDOR-AS-IN Candor infosolution Pvt Ltd, IN
103.208.68.0/24	AS134866	SSCN-AS Sscn Pvt Ltd, IN
103.208.69.0/24	AS134866	SSCN-AS Sscn Pvt Ltd, IN
103.208.70.0/24	AS134866	SSCN-AS Sscn Pvt Ltd, IN
103.208.71.0/24	AS134866	SSCN-AS Sscn Pvt Ltd, IN
103.209.135.0/24	AS134852	AIRZONE-AS-IN AirZone internet Service Pvt. Ltd., IN
103.210.52.0/24	AS135795	SILICON-AS-IN Silicon Care Broadnet Pvt Ltd., IN
103.210.53.0/24	AS135795	SILICON-AS-IN Silicon Care Broadnet Pvt Ltd., IN
103.210.54.0/24	AS135795	SILICON-AS-IN Silicon Care Broadnet Pvt Ltd., IN
103.210.55.0/24	AS135795	SILICON-AS-IN Silicon Care Broadnet Pvt Ltd., IN
103.229.232.0/24	AS18002	WORLDPHONE-IN AS Number for Interdomain Routing, IN

Source:www.cidr-report.org

India

Unallocated IPv4 Prefix

103.229.235.0/24	AS133676	PNPL-AS Precious netcom pvt ltd, IN
103.243.8.0/22	AS133676	PNPL-AS Precious netcom pvt ltd, IN
110.235.216.0/24	AS135777	NECONN-AS Shreenortheast Connect And Services Pvt Ltd, IN
110.235.217.0/24	AS135777	NECONN-AS Shreenortheast Connect And Services Pvt Ltd, IN
110.235.218.0/24	AS135777	NECONN-AS Shreenortheast Connect And Services Pvt Ltd, IN
110.235.219.0/24	AS135777	NECONN-AS Shreenortheast Connect And Services Pvt Ltd, IN
110.235.236.0/22	AS55507	TEJAYS-AS Tejays Dynamic Limited, IN

Source:www.cidr-report.org

Tools to Help

- Prefix and AS-PATH filtering
- RPKI validator, IRR toolset, IRRPT, BGPQ3
- BGPSEC is standardized

But…

- Not enough deployment
- Lack of reliable data

We need a standard approach to improving routing security.

We Are In This Together

Network operators have a responsibility to ensure a globally robust and secure routing infrastructure.

Your network's safety depends on a routing infrastructure that weeds out bad actors and accidental misconfigurations that wreak havoc on the Internet.

The more network operators work together, the fewer incidents there will be, and the less damage they can do.

The Solution: Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to eliminate the most common routing threats

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

Mutually Agreed Norms for Routing Security

MANRS defines four simple but concrete actions that network operators must implement to dramatically improve Internet security and reliability.

- The first two operational improvements eliminate the root causes of common routing issues and attacks, while the second two procedural steps improve mitigation and decrease the likelihood of future incidents.

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 in common routing databases

Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate

Benefits of Improved Routing Security

Signals an organization’s security-forward posture and can eliminate SLA violations that reduce profitability or cost customer relationships.

Heads off routing incidents, helping networks readily identify and address problems with customers or peers.

Improves a network’s operational efficiency by establishing better and cleaner peering communication pathways, while also providing granular insight for troubleshooting.

Implementing best practices alleviates many routing concerns of security-focused enterprises and other customers.

Everyone Benefits

Joining MANRS means joining a community of security-minded network operators committed to making the global routing infrastructure more robust and secure.

Consistent MANRS adoption yields steady improvement, but we need more networks to implement the actions and more customers to demand routing security best practices.

The more network operators apply MANRS actions, the fewer incidents there will be, and the less damage they can do.

MANRS is an Important Step

Security is a process, not a state. MANRS provides a structure and a consistent approach to solving security issues facing the Internet.

MANRS is the minimum an operator should consider, with low risk and cost-effective actions.

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.

The Business Case for MANRS and Routing Security

Engaged 451 Research to better understand the attitudes and perceptions of Internet service providers and the broader enterprise community around the project

Why SERVICE PROVIDERS Should Join MANRS

To help solve global network problems

- Lead by example to improve routing security and ensure a globally robust and secure routing infrastructure
- Being part of the MANRS community can strengthen enterprise security credentials

To add competitive value and differentiate in a flat, price-driven market

- Growing demand from enterprise customers for managed security services (info feeds)
- To signal security proficiency and commitment to your customers

To "lock-in" - from a connectivity provider to a security partner

- Information feeds and other add-on services may increase revenue and reduce customer churn
- Enterprises indicate willingness to pay more for secure services

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

Why GOVERNMENTS Should Promote MANRS

To drive the development or adoption of best practices across the country

- Encourage industry associations to develop or strengthen and promote existing voluntary codes of conduct for network operators. MANRS can serve as both a baseline set of best practices and as a foundation to complimentary voluntary codes of conduct.

To encourage the use of routing security as a competitive best practice

- Encourage local industry to better convey security to consumers, and specify security during procurement practices.

To lead by example

- Improve infrastructure reliability and security by adopting best practices in their own networks.

Why Research & Education Networks Should Join MANRS

To show technical leadership and distinguish you from commercial ISPs

- Customers increasing willing to pay more for secure services

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 customer

To help solve global network problems

- NRENs are often early adopters of new developments. Lead by example and improve routing security for everyone
- Being part of the MANRS community can strengthen enterprise security credentials

Why join MANRS?

- Improve your security posture and reduce the number and impact of routing incidents
- Join a community of security-minded operators working together to make the Internet better
- Use MANRS as a competitive differentiator

Join Us

Visit https://www.manrs.org

- Fill out the sign up form with as much detail as possible.
- We may ask questions and run tests

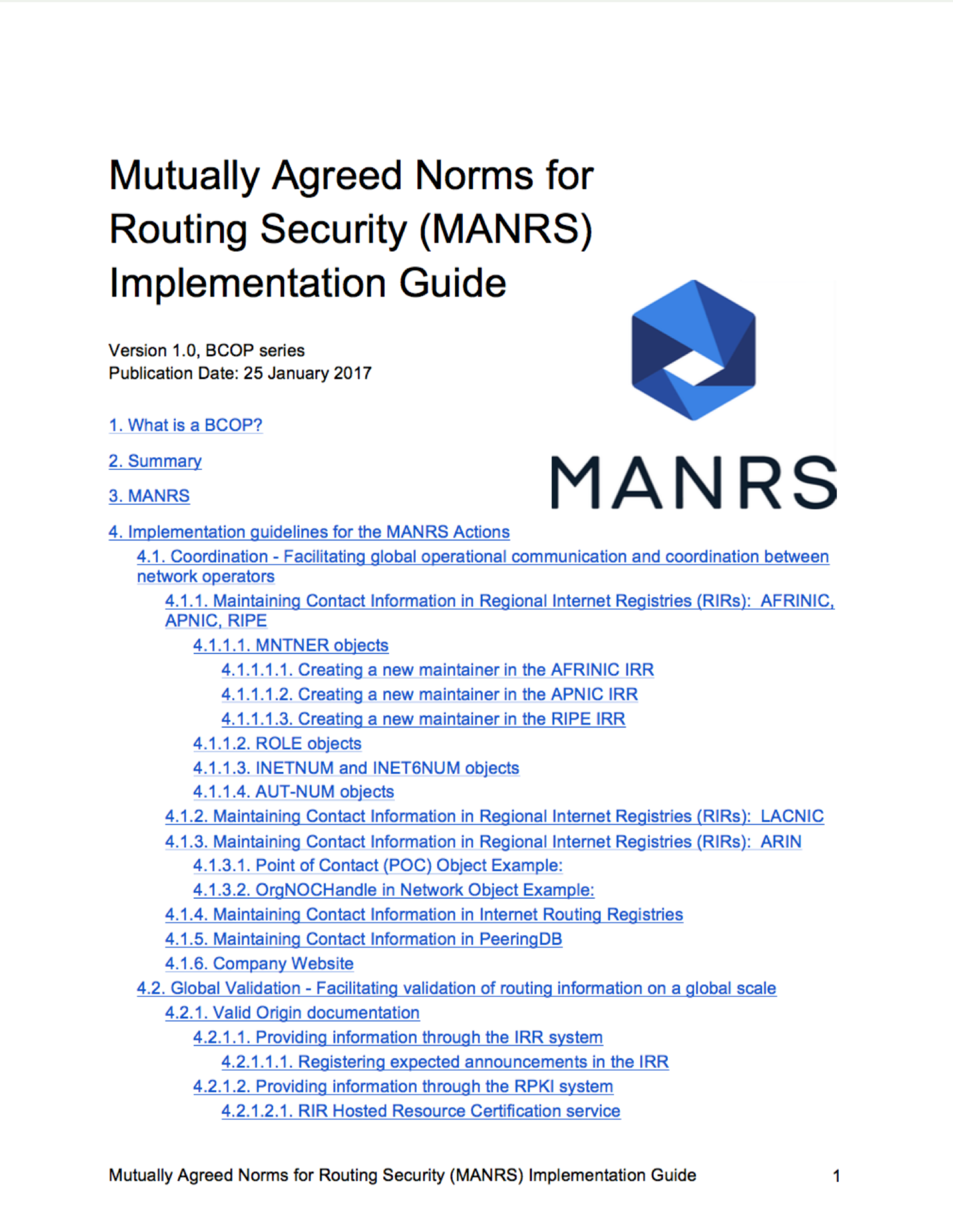
Get Involved in the Community

- Members support the initiative and implement the actions in their own networks
- Members maintain and improve the document and promote MANRS objectives

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



Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Version 1.0, BCOP series
Publication Date: 25 January 2017

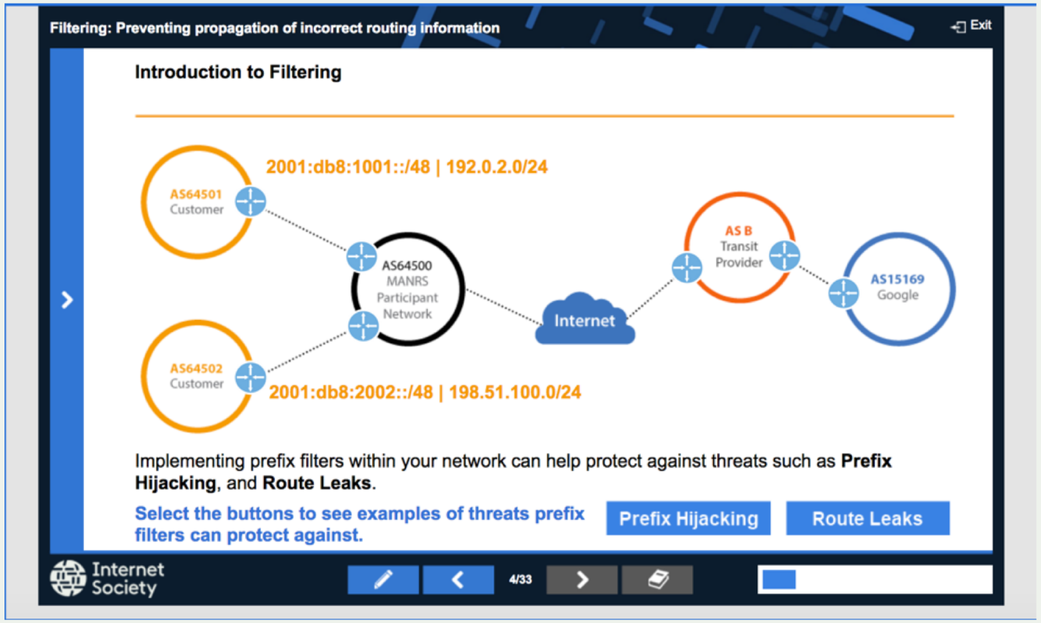
MANRS Training Modules

6 training modules based on information in the Implementation Guide.

Walks through the tutorial with a test at the end of each module.

Working with and looking for partners that are interested in integrating it in their curricula.

https://www.manrs.org/tutorials



Filtering: Preventing propagation of incorrect routing information

Introduction to Filtering

Implementing prefix filters within your network can help protect against threats such as **Prefix Hijacking**, and **Route Leaks**.

Select the buttons to see examples of threats prefix filters can protect against.

What’s Next: MANRS IXP Partnership Programme

There is synergy between MANRS and IXPs

- IXPs form a community with a common operational objective
- MANRS is a reference point with a global presence – useful for building a “safe neighborhood”

How can IXPs contribute?

- Technical measures: Route Server with validation, alerting on unwanted traffic, providing debugging and monitoring tools
- Social measures: MANRS ambassadors, local audit as part of the on-boarding process
- A development team is working on a set of useful actions

LEARN MORE:

https://www.manrs.org

Thank you.

Aftab Siddiqui

siddiqui@isoc.org

manrs.org