MANRS

Mutually Agreed Norms for Routing Security

Christian O'Flaherty (ISOC)

oflaherty@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 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.

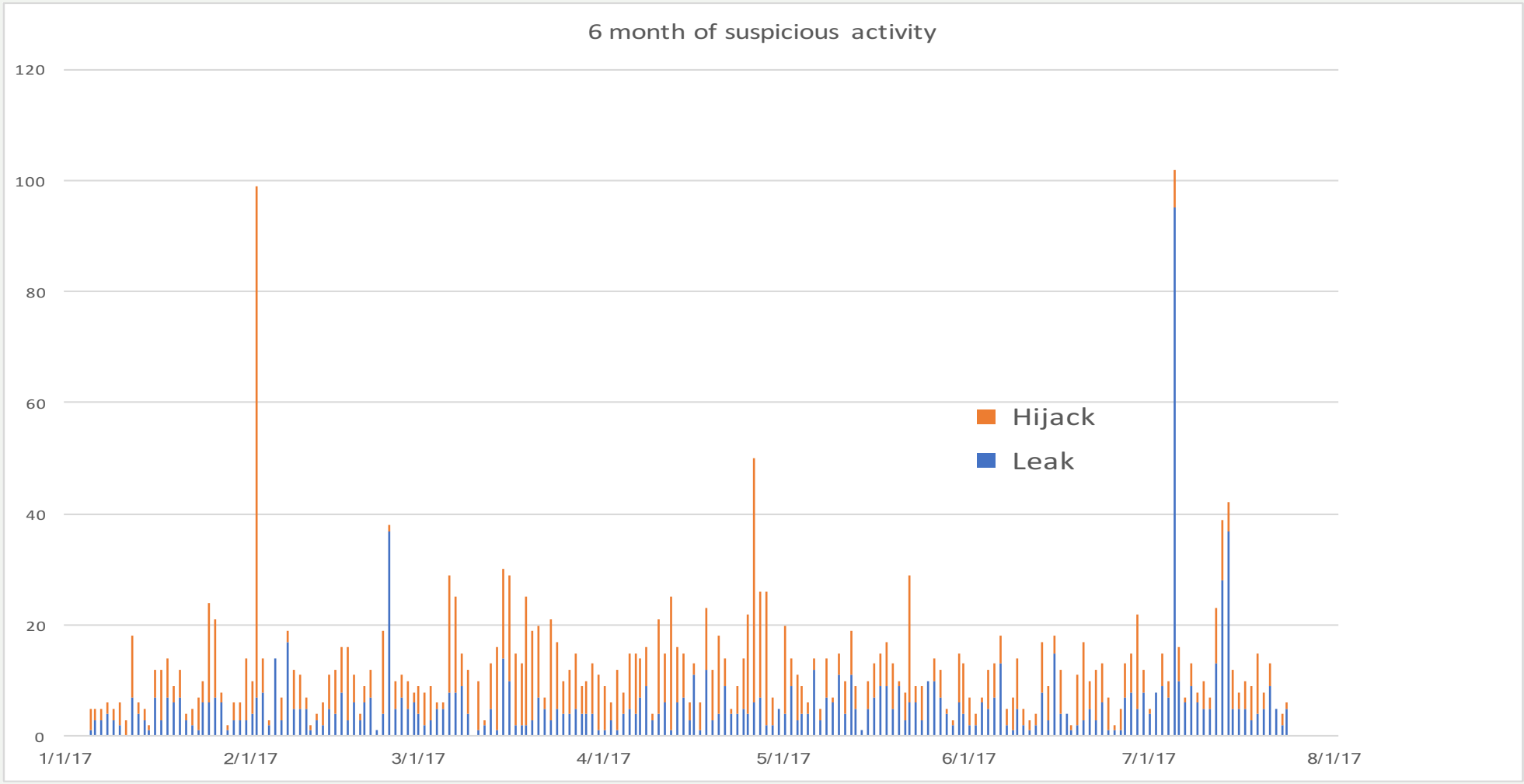
The Honor System: Routing Issues

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 ...

No Day Without an Incident



http://bgpstream.com/

The Problem:

Routing Incidents Cause Real World Problems

The Honor System: Routing Issues

No Day Without an Incident

The Threats: What's Happening?

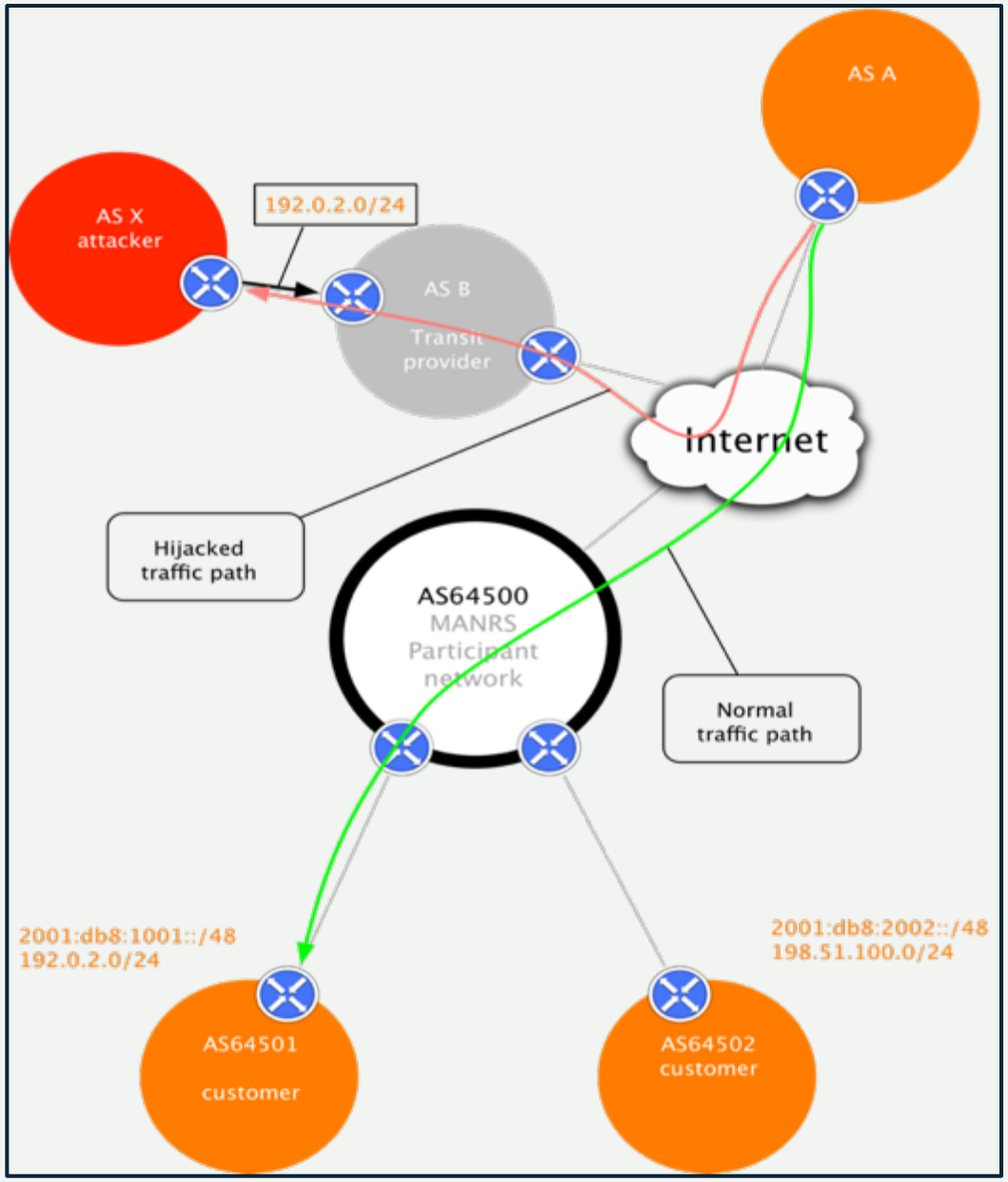
Event	Explanation	Repercussions	Solution
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	Stronger 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.

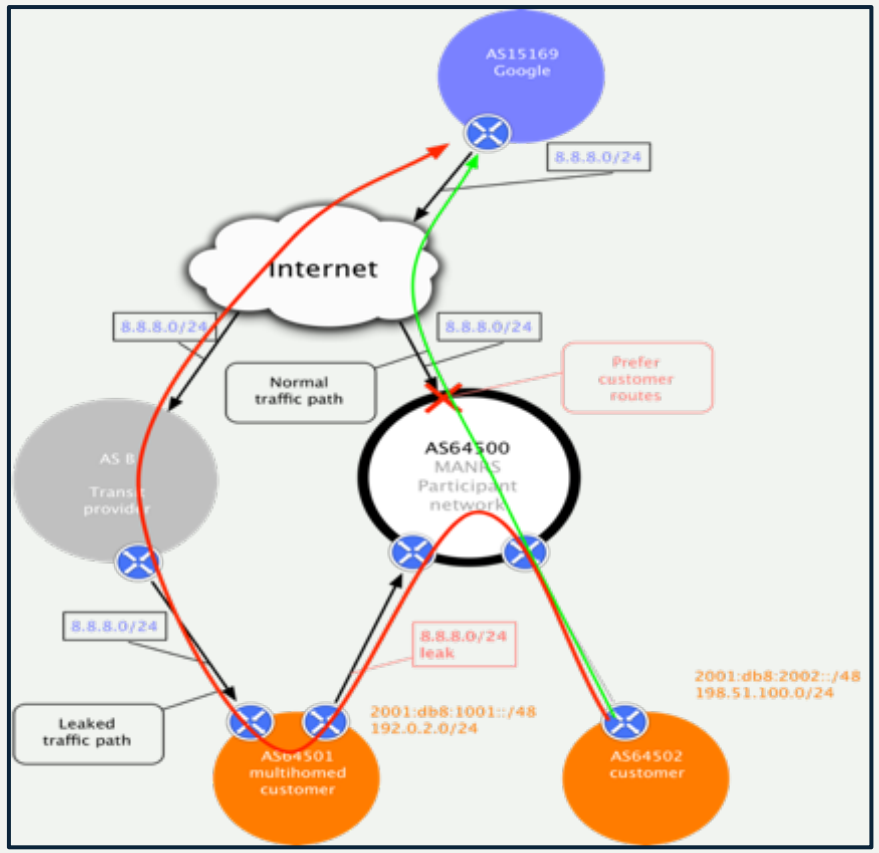
Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting false announcements).



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 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 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.

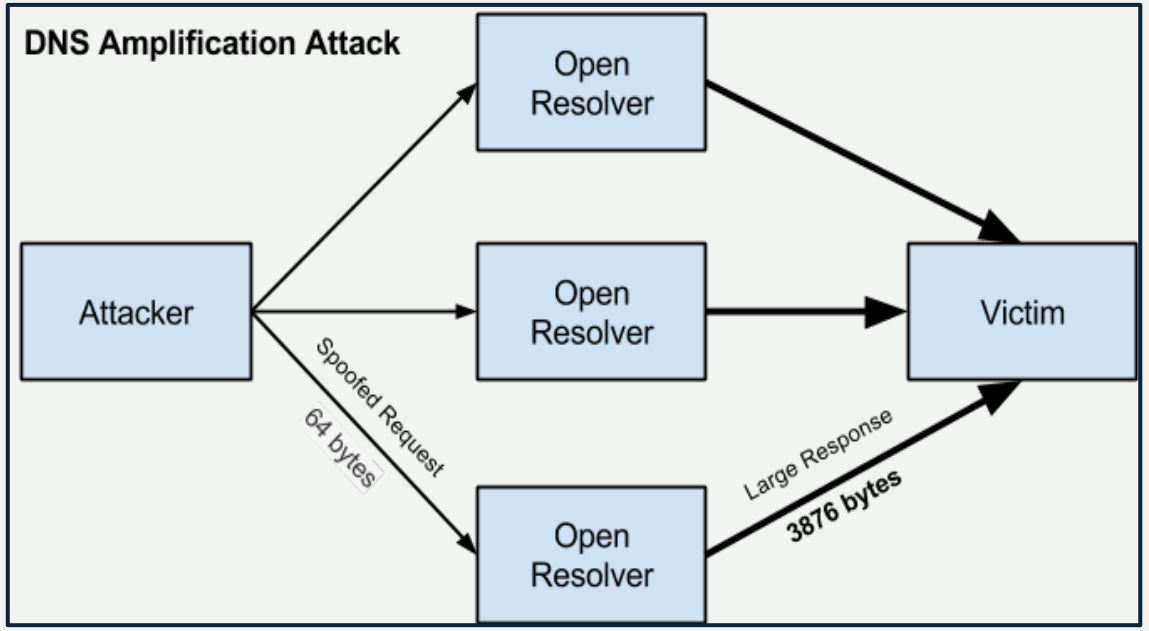


Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting announcements that don't make sense).

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).

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.

Collaboration and Consensus

Your security is in someone else's hands. The actions of others directly impact you and your network security (and vice versa).

Why should they help you? You can start by helping them.

Where is the line between good and bad routing security?

We need globally recognized security expectations for all network operators to raise the bar on 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 Proposal: 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

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

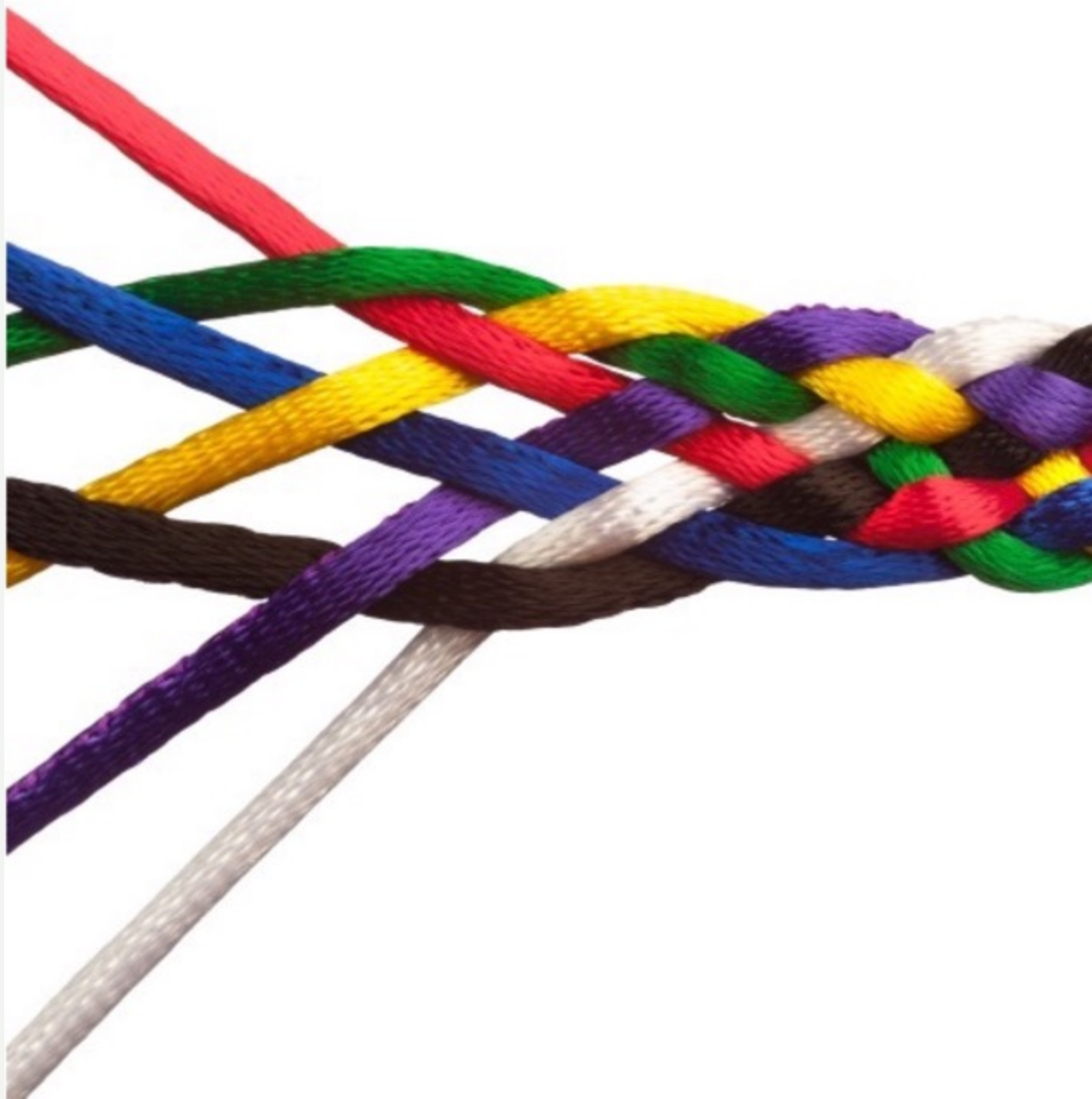
Join Us

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

MANRS

Version 1.0, BCOP series
Publication Date: 25 January 2017

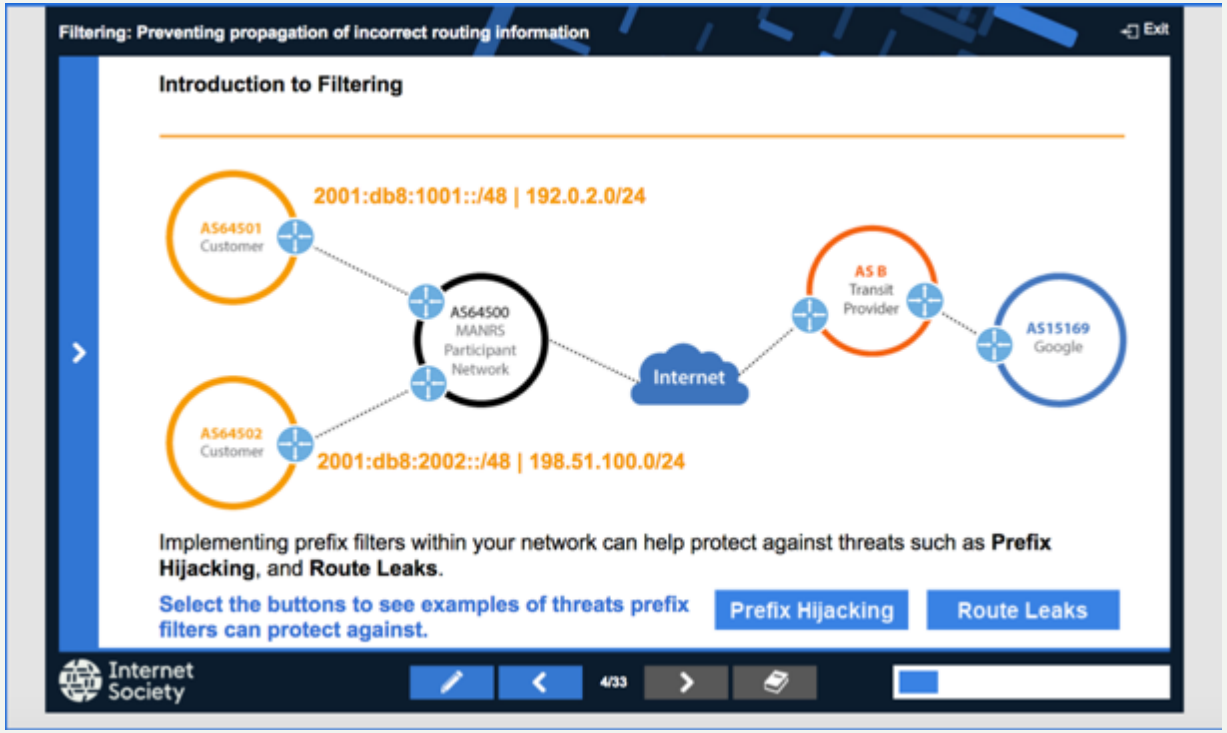
MANRS Training Modules

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



CONFIGURACIONES

(Slides Hans)

COORDINATION

Coordination

MILACNIC

- https://milacnic.lacnic.net/

- https://www.peeringdb.com/

¿Qué es RPKI?

RPKI (Resource Public Key Infrastructure) permite la validación del derecho de una organización a usar un recurso determinado (IPv4, IPv6, ASN)

RPKI combina la jerarquía del modelo de asignación de recursos de Internet a través de los RIRs con el uso de certificados digitales basados en el estándar X.509

RPKI es estandarizado en el IETF a través del grupo de trabajo SIDR, el cual ha producido los RFCs 6480 – 6492

Global Validation

Discusión

RPKI

Todos los objetos firmados de RPKI se listan en repositorios públicos

Luego de ser verificados, estos objetos pueden ser usados para configurar filtros en los routers

Proceso de validación

- Los objetos firmados tienen referencias al certificado usado para firmarlos
- Cada certificado tiene un puntero a un certificado de un nivel superior
- Los recursos listados en un certificado DEBEN ser subconjuntos válidos de los recursos listados en el certificado padre
- De esta forma se puede seguir una cadena de confianza hasta un "trust anchor” tanto criptográficamente como en términos de CIDR

ROAs

Usando certificados podemos crear objetos que describan el origen de un prefijo

ROAs: Routing Origin Authorization

- Los ROAs contienen información sobre el AS de origen permitido para un conjunto de prefijos
- Los ROAs son firmados usando los certificados generados por RPKI
- Los ROAs firmados son copiados al repositorio

ROAs (ii)

Un ROA simplificado contiene la siguiente información:

Prefix	MaxLen	Origin AS	Valid Since	Valid Until
200.40.0.0/17	20	6057	2013-01-02	2013-12-31
200.3.12.0/22	24	28000	2013-01-02	2014-12-31

Este ROA establece que:

- ”El prefijo 200.40.0.0/17 será originado por el ASN 6057 y podría ser desagregado hasta un /20" ”Esto es válido desde el 2 de Enero de 2013 hasta el 31 de Diciembre de 2013"

Otro contenido del ROA:

- Los ROAs contienen material criptográfico que permite la validación del contenido del ROA

Validación de Origen

Los routers arman una base de datos con la información que reciben de los caches

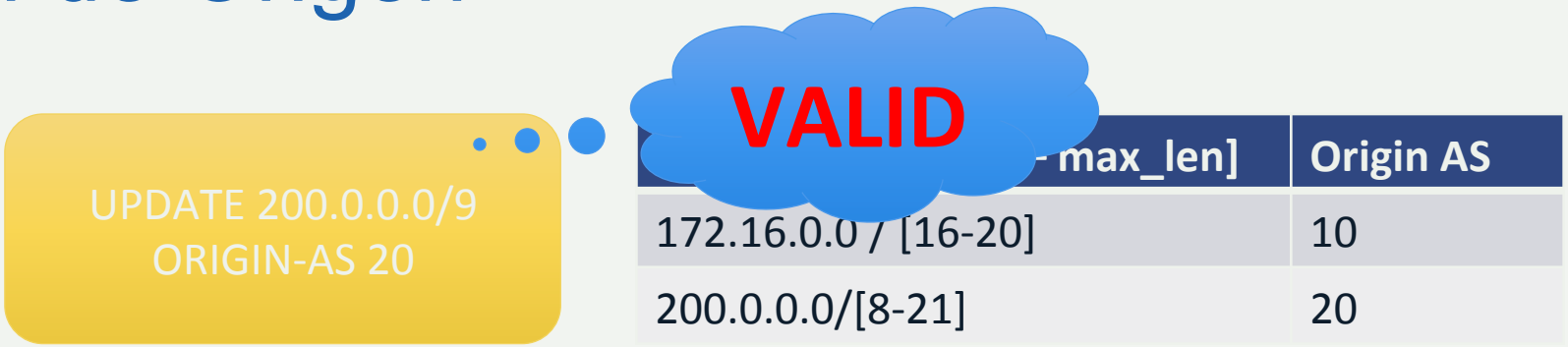
Esta tabla contiene

- Prefix, Min length, Max length, Origin-AS

Aplicando un conjunto de reglas, se asigna un estado de validez a cada UPDATE de BGP

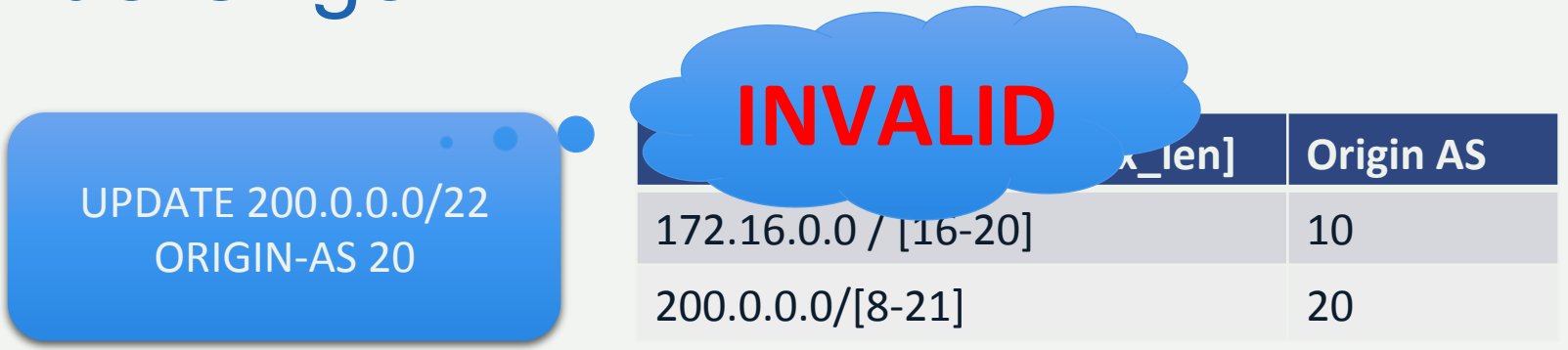
Los operadores de red pueden usar el atributo “validez” para construir políticas de ruteo

Validación de Origen



- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide -> "**invalid**"

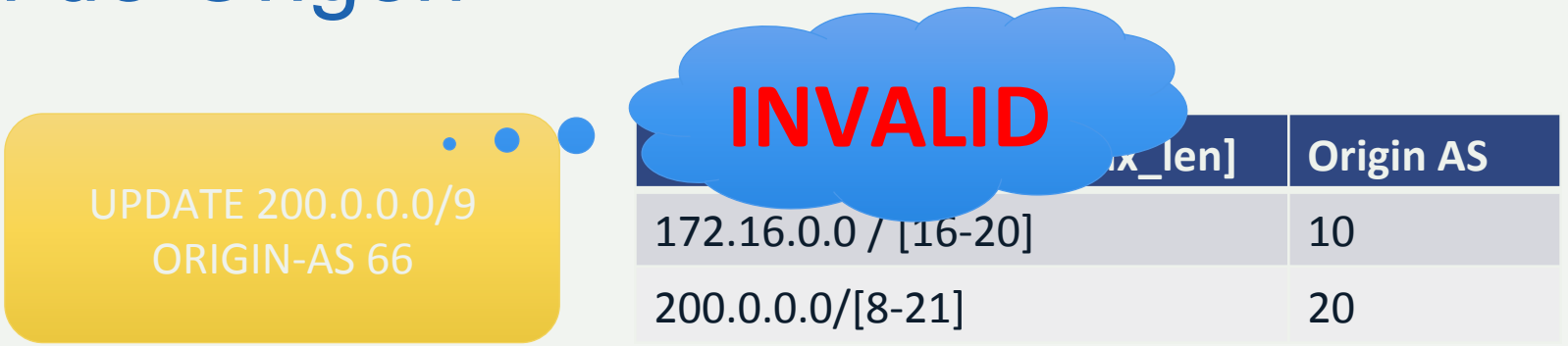
Validación de Origen



[x_len]	Origin AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide -> "**invalid**"

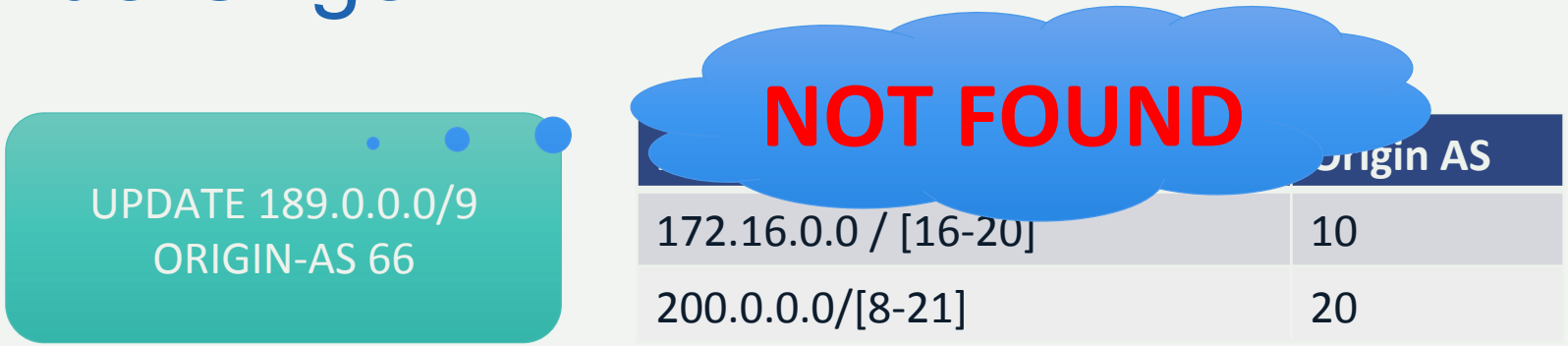
Validación de Origen



[max_len]	Origin AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide -> "**invalid**"

Validación de Origen



- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide -> "**invalid**"

Políticas de Ruteo con Validación de Origen

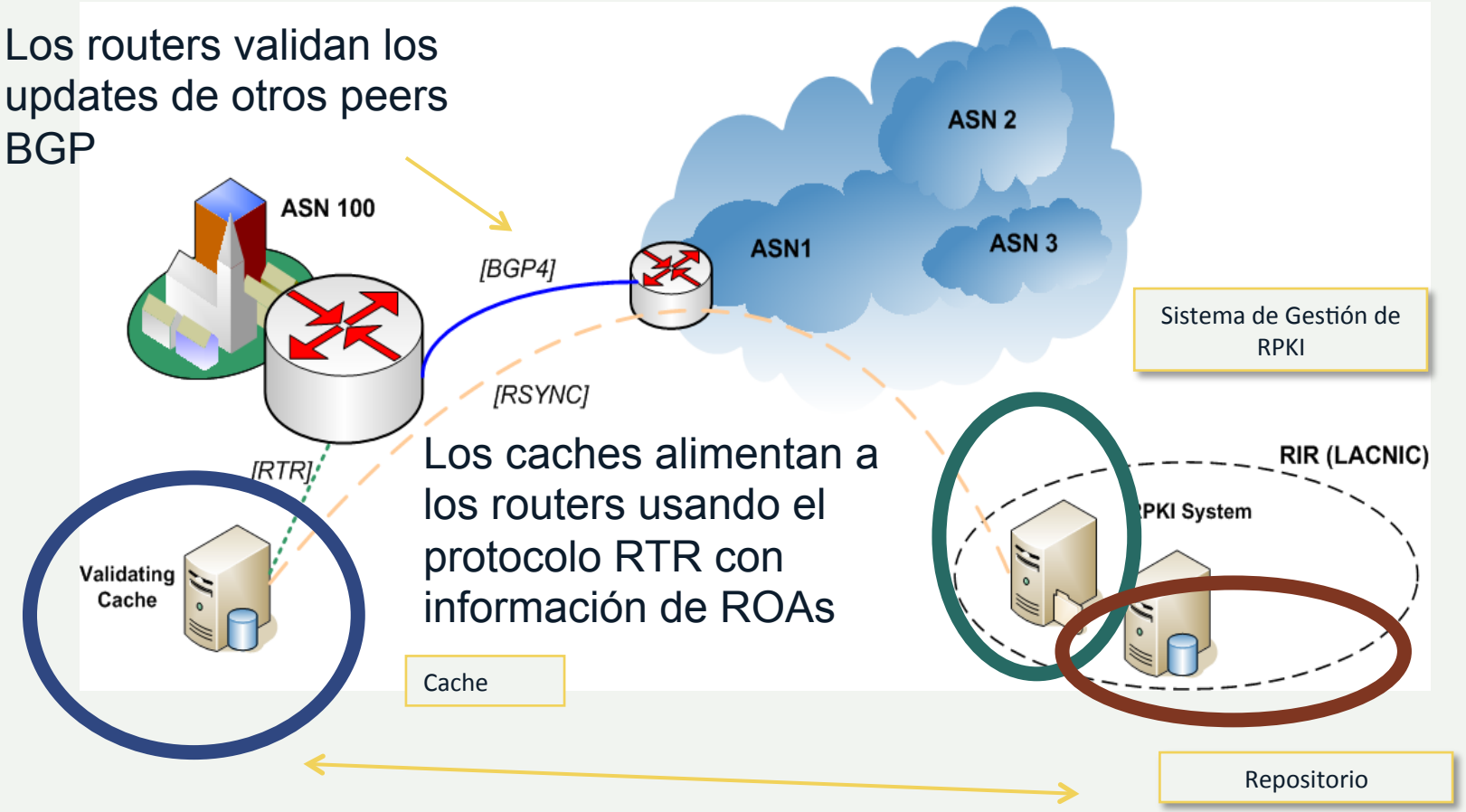
Usando el atributo de validez de BGP los operadores de red pueden construir políticas de ruteo

Por ejemplo:

- A las rutas con estado “valid” asignarles mayor preferencia que a las rutas con estado “unknown”
- Descartar rutas con estado “invalid”

MUY IMPORTANTE: RPKI es una fuente de información! Los operadores son libres de usarla como les parezca mejor

RPKI en acción



Los caches traen y validan criptográficamente los certificados y ROAs de los repositorios

Conclusiones

El sistema de ruteo es una de las operaciones principales de Internet

Aún es vulnerable a ataques y a configuraciones erróneas

Se ha hecho algo de trabajo (RPKI, Origin Validation)

Pero es necesario seguir trabajando

- Especificación del protocolo
- Despliegue (Filtrado, RPKI, Origin Validation)

Links / Referencias

LACNIC’s RPKI System

- http://rpki.lacnic.net

LACNIC’s RPKI Repository

- rsync://repository.lacnic.net/rpki/

To see the repository

- rsync --list-only rsync://repository.lacnic.net/rpki/lacnic/

RPKI Statistics

- http://www.labs.lacnic.net/~rpki

Beneficios

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

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

What We Learned from the Study

Security is Vital to Enterprises

- MANRS knowledge is low, but the desire for security is high
- Enterprises are willing to require MANRS compliance of their service providers

MANRS Adds Value for Service Providers

- Security can help service providers differentiate from their competitors; Identifiable value in a vague market
- Service providers may be able to add additional revenue streams based on information security feeds and other add-on services

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

MANRS IXPP

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

Acciones para el IXPP

Acción 1. Facilitar la prevención de la propagación de información de enrutamiento incorrecta. (Obligatorio)

- El IXP implementa el filtrado de anuncios de ruta en el route server usando IRR y / o RPKI. Los anuncios no válidos se filtran de acuerdo con la política publicada de IXP.

Acción 2. Promover MANRS entre los miembros del IXP. (Obligatorio)

- El IXP promueve o prove asistencia para que los miembros implementen las acciones de MANRS. (Hay 4 casillas de verificación separadas para diferentes niveles de incentivos, se debe verificar una o más).

Acciones para el IXPP

Acción 3. Proteger la plataforma de peering.

- El IXP tiene una política publicada de tráfico no permitido en el switch de peering y realiza el filtrado de dicho tráfico. (higiene de capa 2)

Acción 4. Facilitar la comunicación y coordinación operativa global entre los operadores de red.

- El IXP y cada uno de sus miembros tienen al menos una dirección de correo electrónico válida y activa y un número de teléfono que otros miembros pueden usar para casos de abuso, seguridad e incidentes operacionales.

Acción 5. Proporcionar herramientas de monitoreo y depuración a los miembros.

- El IXP proporciona un looking glass para sus miembros.

AUTOEVALUACION

Autoevaluación - Filtering:

- Check that the ASN does not announce bogons
  - Use CIDR Report https://www.cidr-report.org/as2.0/

- Check that the ASN was not implicated in recent incidents https://bgpstream.com/

Autoevaluación - Anti-Spoofing

- Check that ASN does not show up in CAIDA spoofer database

  https://spoofer.caida.org/provider.php?asn=[ASN],
  https://spoofer.caida.org/as.php?asn=[ASN]

- If there are no, or no recent tests, run Spoofer
  https://spoofer.caida.org/as.php?asn=[ASN]

Autoevaluación - Coordination

Los contactos en whois / rdap estan actiualizados?

- https://rdap.rfegistro.br

- Esta registrado en PeeringDB:
  - https://www.peeringdb.com/asn/[ASN]

Autoevaluación - Global Validation

- Check that routing information is public (IRR, ROA, etc.)
- http://localcert.ripe.net:8088/bgp-preview
- Presentación Carlos Martinez + Fred Neves

HERRAMIENTAS

MANRS Implementation Guide

MANRS Training LAB

MANRS Observatory

MANS Tutorials

Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

MANRS

Version 1.0, BCOP series
Publication Date: 25 January 2017

LEARN MORE:
https://www.manrs.org

Preguntas, Sugerencias, Pedidos?

Thank you.

Christian O’Flaherty

oflaherty@isoc.org

manrs.org