MANRS

Normas Mutuamente Acordadas para el Enrutamiento Seguro en Internet:

Operadores de Red de Universidades

MANRS

Agenda Sesion 1

- Bienvenida y presentación. Internet Society, ANUIES y Red Clara
- Antecedentes. Juan Antonio Herrera
- MANRS. Christian O'Flaherty
- Preguntas y Respuestas.

MANRS

Normas Mutuamente Acordadas para Enrutamiento Seguro en Internet

Las Normas comúnmente acordadas para la seguridad del enrutamiento (MANRS) es una iniciativa comunitaria organizada por Internet Society, que tiene como objetivo mejorar la seguridad y la resiliencia del sistema de enrutamiento global.

Es una colaboración entre operadores implementando mejores prácticas que permiten un enrutamiento más seguro y confiable para todos.

ANUIES ANUIES - TIC cudi Corporación Universitaria para el Desarrollo de Internet A.C. Internet 2 - México Red CLARA Internet Society lacnic NIC MÉXICO

MANRS

Normas Mutuamente Acordadas para Enrutamiento Seguro en Internet

El taller consta de **5 sesiones virtuales**

Sesión 1: Jueves 25 de abril – Introducción a MANRS
Sesión 2: Jueves 23 de mayo – MANRS: Acción 1 – Filtrado
Sesión 3: Jueves 13 de junio – MANRS: Acción 2 – Anti-Spoofing
Sesión 4: Jueves 11 de julio – MANRS: Acción 3 – Coordinación
Sesión 5: Jueves 22 de agosto – MANRS: Acción 4 – Validación Global

La conclusión será con **una sesión presencial** en el marco de los eventos:

Encuentro TICAL 2019, 2 – 4 de septiembre de 2019 en Cancún, México.
Encuentro ANUIES-TIC 2019, 2 de octubre de 2019 en la UANL, Nuevo León, México.

ANUIES · ANUIES - TIC · cudi Corporación Universitaria para el Desarrollo de Internet A.C. Internet 2 - México · Red CLARA · Internet Society · lacnic · NIC MÉXICO

Christian O'Flaherty

Egresado de la Universidad Nacional del Sur (Bahía Blanca, Argentina) y Posgrado en gestión de empresas (Universidad Austral, Buenos Aires). Fue docente, director de operaciones de la red académica Argentina, gerente de planificación regional de Internet en Impsat y responsable del producto Internet en Global Crossing LAC. En el año 2009 se une a Internet Society para el desarrollo regional de Internet para America Latina y el Caribe.

Juan Antonio Herrera

Con 40 años de experiencia en Ciencias de la Computación. Pionero en el despliegue de Internet en la región sureste de México, y fundador de la red universitaria de la UADY, en donde colaboró hasta diciembre de 2018. Expositor en foros nacionales e internacionales de los casos de éxito en implementación de Tecnologías de Información en temas de Seguridad Informática, Servicios en la nube así como sobre Metodologías de Gestión y Gobierno de TI. Actualmente colabora en el proyecto MANRS para Operadores de Red de con asociaciones ANUIES, CUDI, ISOC, LACNIC y NICMX.

MANRS

Parte 1

ANTECEDENTES

MANRS

Antecedentes

La seguridad es vital para las empresas y organizaciones.

Las instituciones están dispuestas a exigir el cumplimiento de normas de seguridad de parte de sus proveedores de servicios.

MANRS

Incremento en los incidentes de enrutamiento

Solo en 2017, 14,000 interrupciones o ataques de enrutamiento, como secuestro, filtraciones y suplantación de identidad, llevaron a una serie de problemas que incluyen robo de datos, pérdida de ingresos, daños a la reputación y más.

Alrededor del 40% de todos los incidentes de la red son ataques, con una duración media de 19 horas por incidente.

Antecedentes

Todos los que operan una red son corresponsables de la estabilidad del ruteo global, es una responsabilidad compartida.

Los Operadores de Red de las Universidades no quedamos excentos de esa responsabilidad.

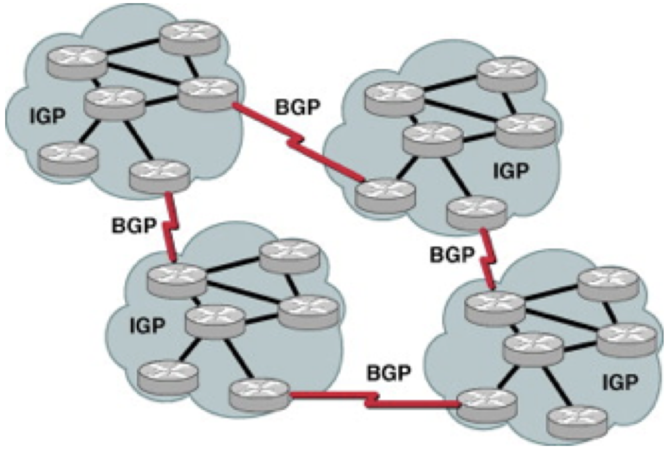
Una mala configuración de una red no solo afecta el servicio para sus usuarios, sino que puede afectar a otros operadores en cualquier parte del mundo.

Los fundamentos: cómo funciona el enrutamiento

Hay alrededor de 60,000 redes con Sistemas Autónomos en Internet, cada una de las cuales utiliza un Número de sistema autónomo (ASN) único para identificarse en otras redes.

Los enrutadores utilizan Border Gateway Protocol (BGP) para intercambiar "información de accesibilidad", redes a las que saben cómo llegar.

Los enrutadores construyen una "tabla de enrutamiento" y eligen la mejor ruta al enviar un paquete, generalmente en base a la ruta más corta.

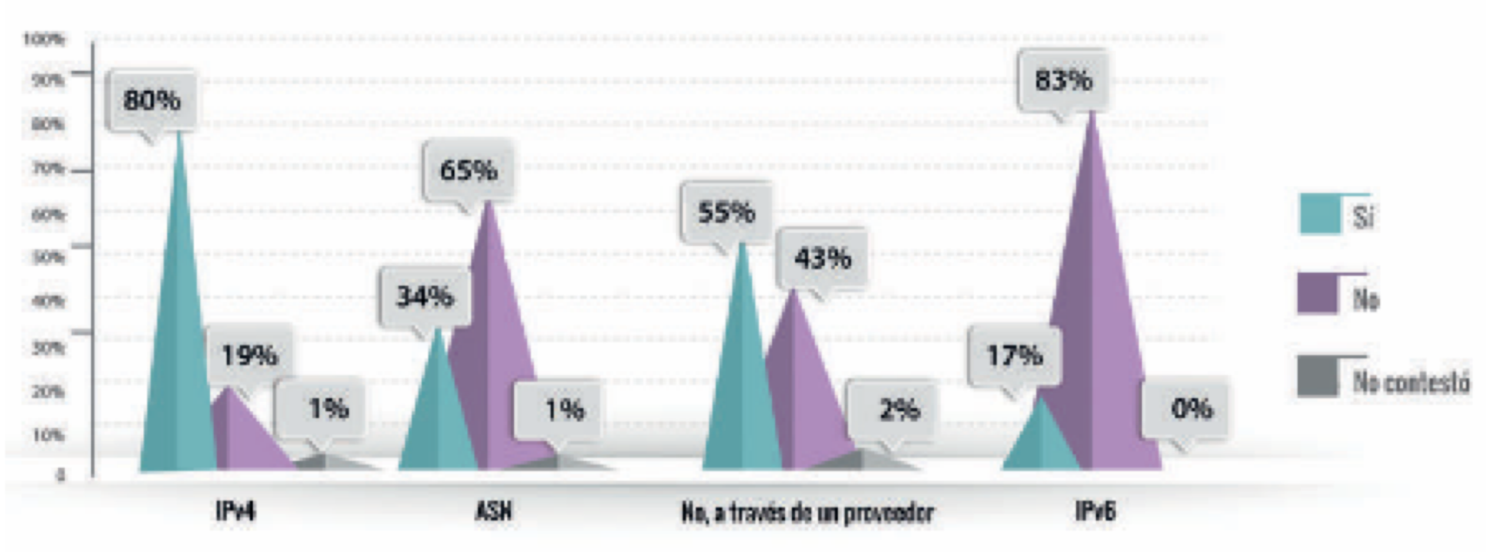


MANRS

Estado de Recursos de Internet Universidades de México

IES que cuentan con servicios propios o públicos de Internet

Figura 2.9.12 IES que cuentan con servicios propios/públicos de Internet



"4 de cada 5 IES entrevistadas cuentan con redes IPv4 públicas".

Estado actual de las Tecnologías de la Información y Comunicaciones en las Instituciones de Educación Superior en México Estudio 2018.

http://publicaciones.anuies.mx/libros/240/estado-actual-de-las-tecnologias-de-la-informacion-y-comunicaciones

MANRS

Análisis de Indicadores: Encuesta ANUIES-TIC 2018

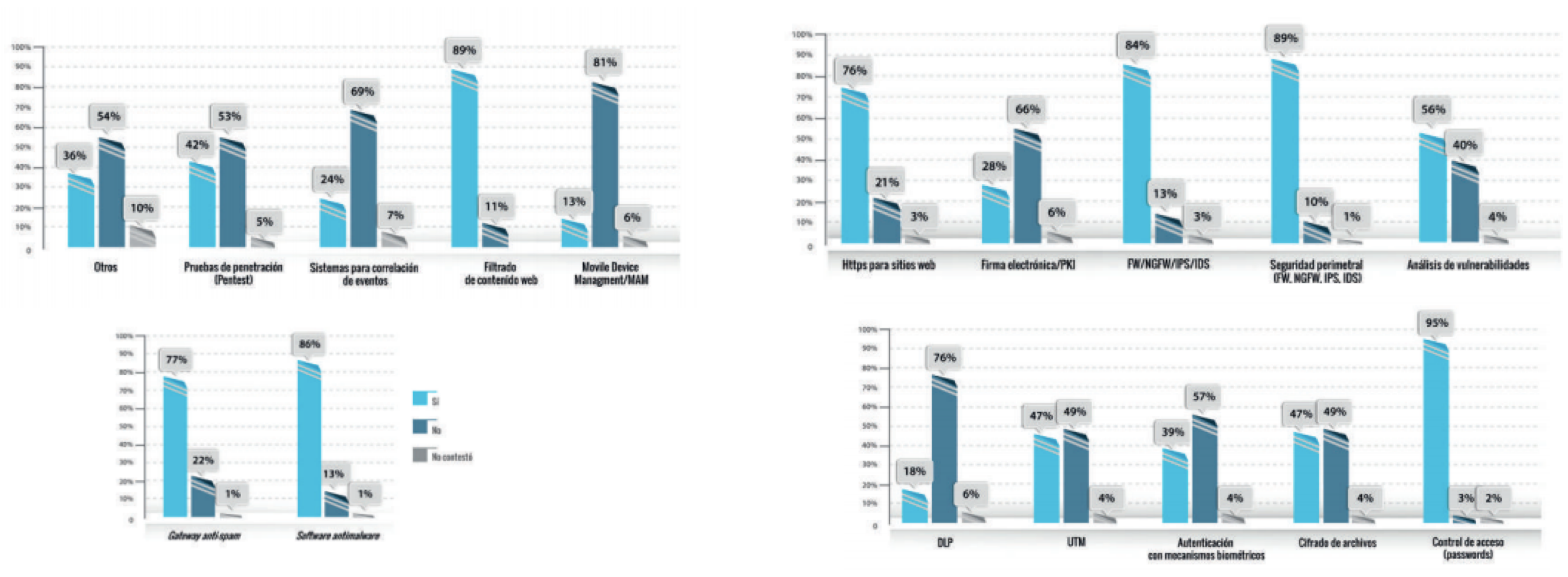
¿Qué mecanismos utiliza para proteger la infraestructura y los sistemas de información?

- Pruebas de penetración (Pentest)
- Sistemas para correlación de eventos
- Filtrado de contenido web
- Mobile Device Management/MAM
- DLP
- UTM
- Autenticación con mecanismos biométricos
- Cifrado de archivos
- Control de acceso (passwords)
- Buenas prácticas para desarrollo de software
- Https para sitios web
- Firma electrónica/pki
- Seguridad perimetral (fw, ngfw, ips, ids)
- Análisis de vulnerabilidades
- Gateway Anti-spam
- Software Antimalware
- Otros

http://estudio-tic.anuies.mx/Estudio_ANUIES_TIC_2018.pdf

Indicadores: Mecanismos para proteger la infraestructura y los sistemas de información

Figura 2.5.12 Mecanismos para proteger la infraestructura y los sistemas de información



http://estudio-tic.anuies.mx/Estudio_ANUIES_TIC_2018.pdf

MANRS

Reactivos para la encuesta ANUIES-TIC 2019: Seguridad en el Ruteo

Su Universidad aplica alguno de los siguientes mecanismos para la seguridad en el ruteo BGP?

- Filtrado BGP: Prefix-list, AS-PATH
- Prefijos definidos en el RFC1918
- Anti-spoofing BCP38 (RFC 2827)
- Buenas prácticas para la configuración del plano de control del ruteador perimetral - RFC6192
- Información de contacto actualizada a nivel mundial en bases de datos de enrutamiento comunes: Whois
- Recursos de Internet Certificado: RPKI (Resource Public Key Infraestructure)
- ROAs (Route Origination Authorizations)
- Registro en un IRR (Internet Routing Registry

Indique qué tipo de incidentes de enrutamiento se han presentado en los últimos 12 meses:

- Route Hijacking (secuestro de rutas
- Route Leak (fuga de rutas)
- IP Address Spoofing (Falsificación de direccionamiento ip)

Incluisión en la pregunta 5.9 "Indique cuáles son las necesidades de sus administradores en cuanto a TI y seguridad":

- Seguridad de Ruteadores
- Configuración BGP/RPKI

MANRS

Enfrentemos en conjunto …

- Los operadores de red tienen la responsabilidad de garantizar una infraestructura de enrutamiento segura y robusta a nivel mundial.
- La seguridad de la red depende de una infraestructura de enrutamiento que elimine a los malos actores: configuraciones erróneas y accidentales que puedan causar estragos en Internet.
- Cuantos más operadores de red trabajen juntos, menos incidentes habrá y menos daño podrán hacer.

¿Porqué MANRS? Redes de Educación e Investigación

MANRS

- Mostrar liderazgo técnico y diferenciarse de los ISPs comerciales.
- Promover el cumplimiento de MANRS a clientes y proveedores centrados en la seguridad.
- Para ayudar a resolver los problemas de la red global. Las Redes Nacionales de Educación e Investigación (RNEI) son a menudo los primeros en adoptar nuevos desarrollos.
- Liderar con el ejemplo y mejorar la seguridad de enrutamiento para todos.

MANRS

Why Universidad Autónoma de Yucatán Supports MANRS

The Autonomous University of Yucatan (UADY) considers it essential to provide reliable and secure computer services to its users, and as part of the adoption of standards of good practices for the management of information security to counteract attacks and the problems they generate. The adoption of MANS is of great importance for UADY to collaborate in strengthening the security of routing on the Internet.

Juan Antonio Herrera Correa, CIO, UADY.

https://www.manrs.org/isps/participants/entry/483/

Network Operator Participants

Network operators across the globe have already committed to the MANRS initiative and implemented the Actions defined in the MANRS document.

← Go back

Universidad Autónoma de Yucatán

UADY
UNIVERSIDAD AUTÓNOMA DE YUCATÁN

Universidad Autónoma de Yucatán Website

https://www.riuady.uady.mx

Areas Served: Mexico

ASNs

22122

Implementation of MANRS Actions

- ✓ **Action 1: Prevent propagation of incorrect routing information**
- ✓ **Action 2: Prevent traffic with spoofed source IP addresses**

  Is very important apply BCOP for harden configuration in routers.
- ✓ **Action 3: Facilitate global operational communication and coordination between network operators**
- ✓ **Action 4: Facilitate validation of routing information on a global scale**

Why Universidad Autónoma de Yucatán Supports MANRS

The Autonomous University of Yucatan (UADY) considers it essential to provide reliable and secure computer services to its users, and as part of the adoption of standards of good practices for the management of information security to counteract attacks and the problems they generate. The adoption of MANS is of great importance for UADY to collaborate in strengthening the security of routing on the Internet.

Juan Antonio Herrera Correa, CIO, UADY.

MANRS

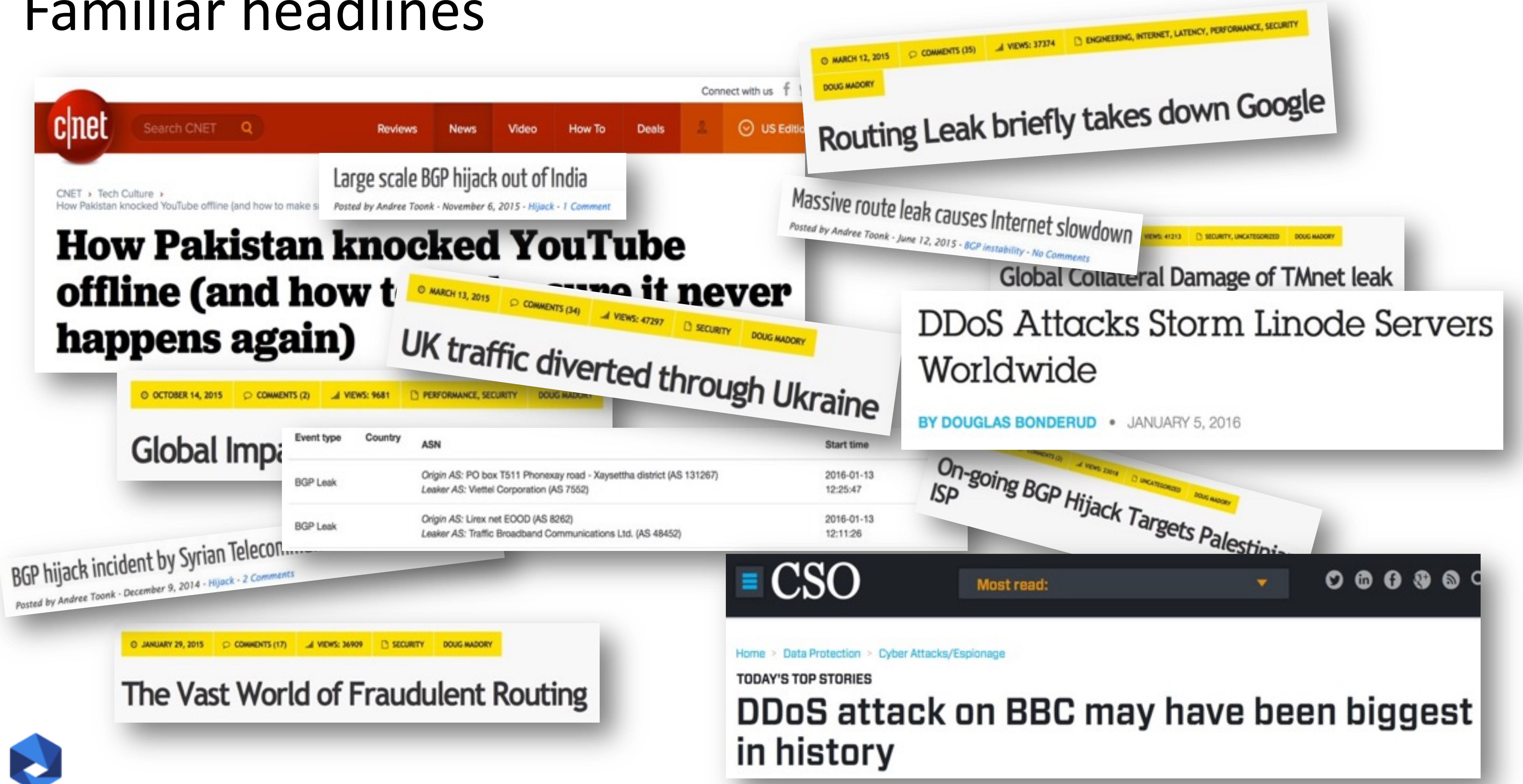
Parte 2

INTRODUCCIÓN A MANRS

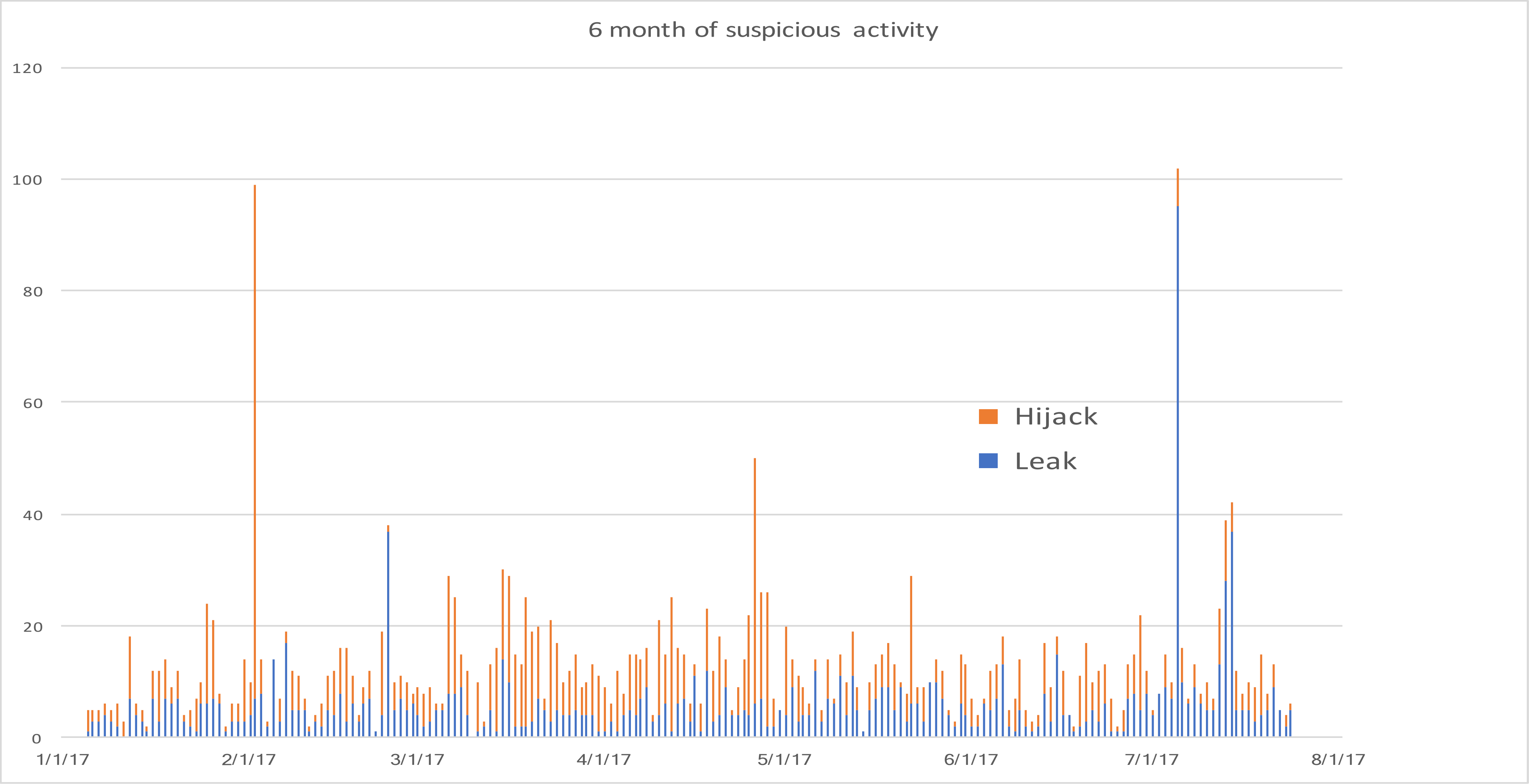
Insecurity by Design

- When the Internet was developed, they didn’t build in security by design.
- The objective was resilience, simplicity and ease of deployment
- That created the Internet as the best effort, interdependent, general purpose network of networks supporting permission-less innovation.
- **While these qualities have made the Internet so successful, they also contribute to many of its security issues.**

Familiar headlines



No Day Without an Incident



http://bgpstream.com/

The routing system is constantly under attack

- 13,935 total incidents (either outages or attacks like route leaks and hijacks)
- Over 10% of all Autonomous Systems on the Internet were affected
- 3,106 Autonomous Systems were a victim of at least one routing incident
- 1,546 networks caused at least one incident

Source: https://www.bgpstream.com/

Routing Incidents Cause Real World Problems

Event	Explanation	Repercussions	Example
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.	*The 2008 YouTube hijack*
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.	*September 2014. VolumeDrive began announcing to Atrato nearly all the BGP routes it learned from Cogent causing disruptions to traffic in places as far-flung from the USA as Pakistan and Bulgaria.*
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	*March 1, 2018. Memcached 1.3Tb/s reflection-amplificationattack reported by Akamai*

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.

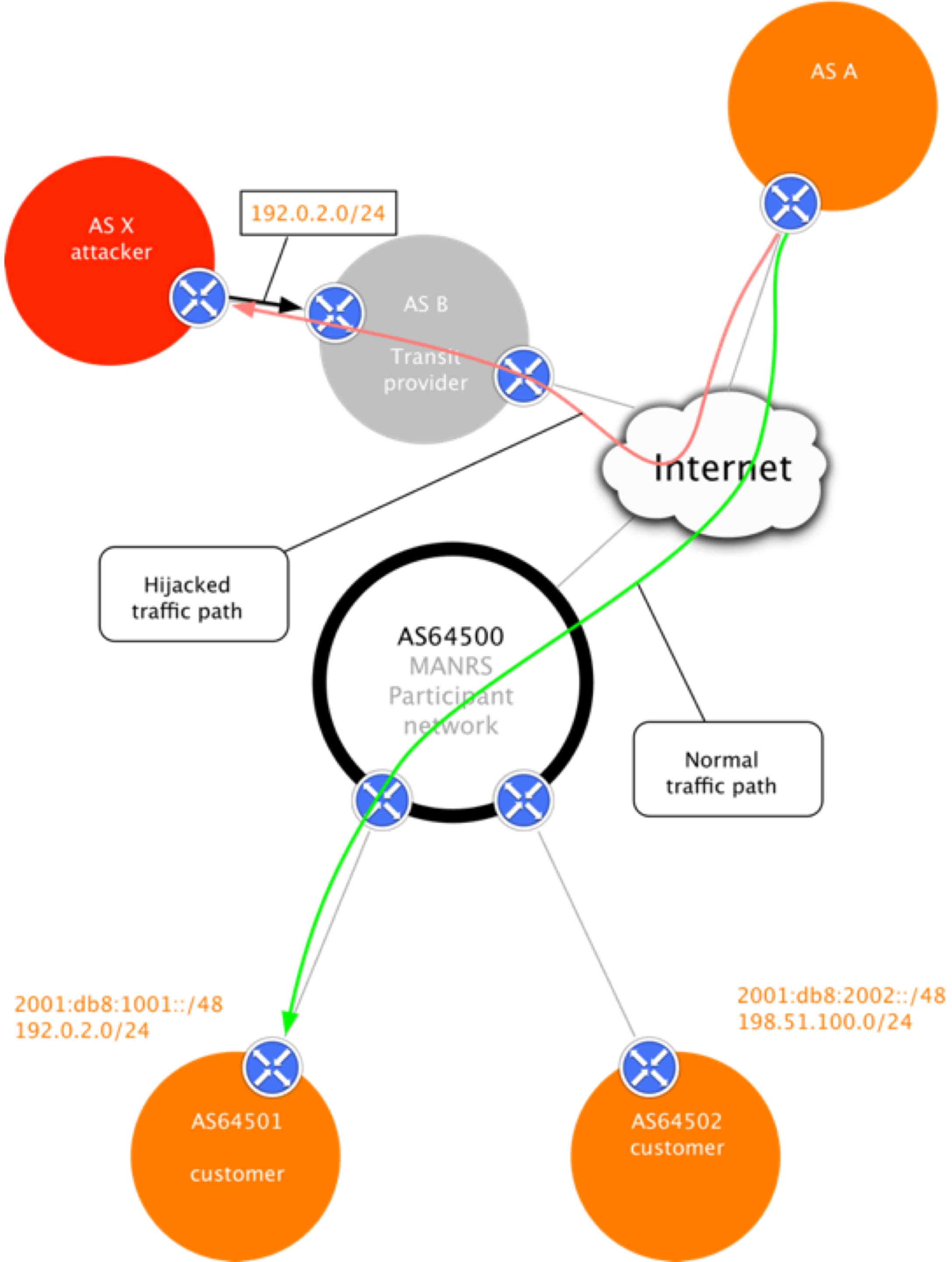
The Honor System: Routing Issues

- 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

Route Hijacking

- **Route hijacking,** also known as "BGP hijacking" when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretends that the network is their client. This routes traffic to the attacker, while the victim suffers an outage.

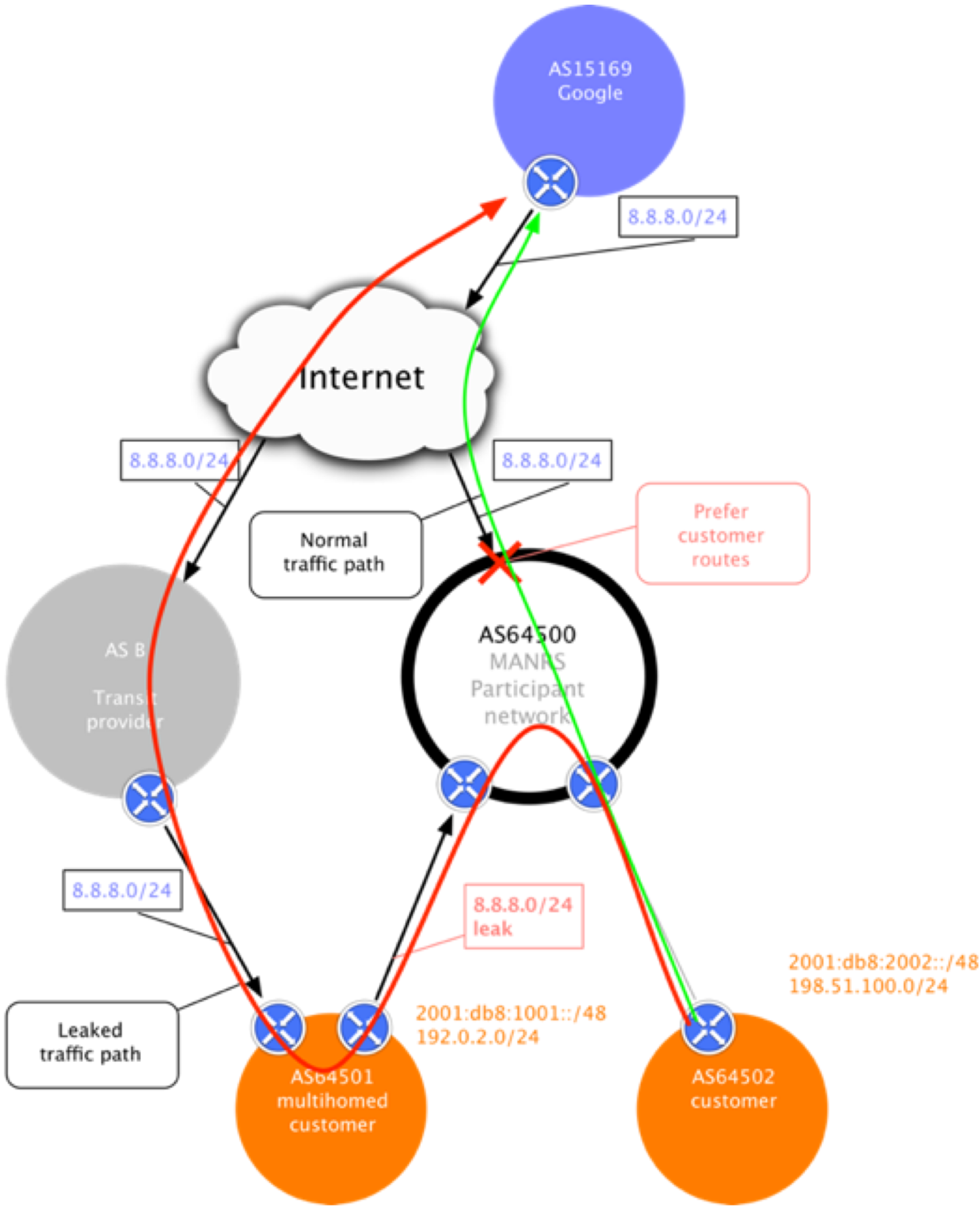
- ***Example:*** *The 2008 YouTube hijack; an attempt to block Youtube through route hijacking led to much of the traffic to Youtube being dropped around the world (*[*https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study*](https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study)*)*



Route Leak

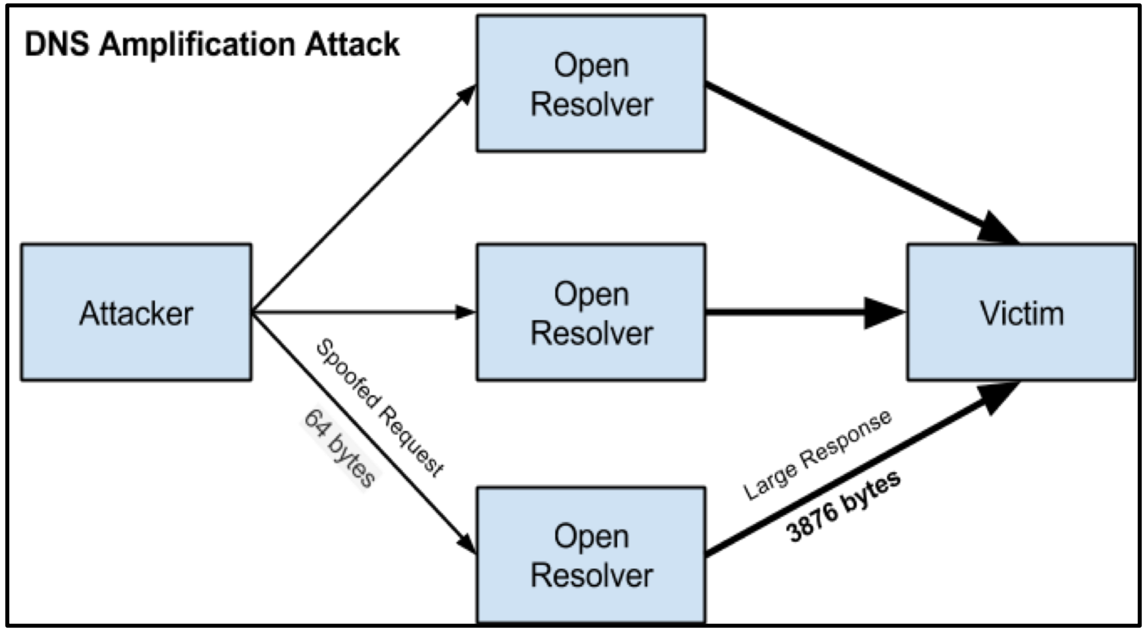
- **A Route leak** is a problem where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that is has a route to a destination through the other upstream provider. This makes the network an intermediary network between the two upstream providers.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

- ***Example:*** *September 2014. VolumeDrive (AS46664) is a Pennsylvania-based hosting company that uses Cogent (AS174) and Atrato (AS5580) for Internet transit. VolumeDrive began announcing to Atrato nearly all the BGP routes it learned from Cogent causing disruptions to traffic in places as far-flung from the USA as Pakistan and Bulgaria. (https://dyn.com/blog/why-the-internet-broke-today/)*



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 systemic 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.

- Mutually Agreed Norms for Routing Security (MANRS)

- Provides crucial fixes to reduce 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.

- MANRS sets a new norm in routing hygiene

Mutually Agreed Norms for Routing Security

MANRS defines four simple but concrete actions that network operators must implement to 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 builds a visible community of security minded network operators and IXPs

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

Implementing MANRS Actions:

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.

Addresses many 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.

- 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

Preguntas

Gracias