Internet Infrastructure Initiative

Triple I: a GFCE Capacity-building project

@LACIGF, La Paz, Bolivia, 5 August 2019

Global Risks Report 2018

"… this generation enjoys unprecedented technological, scientific, and financial resources, which we should use to chart a course towards a more sustainable, equitable and inclusive future.

At the same time, the risks are greater than ever, with an important role for disruptive technologies that may be used to affect societies in good and bad ways, and with cyberattacks amongst today's biggest threats to disrupt society."

WORLD ECONOMIC FORUM

Internet Infrastructure Initiative

- Aim: to help build a robust, transparent and resilient internet infrastructure.
- Rationale: A robust, open and resilient internet infrastructure is key to counter infringements and threats to the cyber domain, and:
  - diminishes the chances and impact of cyber-attacks (like DDoS) and cybercrime (hacking malware, phishing, botnets) and SPAM.
  - enables the public to maintain confidence and trust;
  - is a precondition for the use of the internet as a means to boosting innovative and economic activities.
- Offering: this Initiative seeks to deepen and broaden the know-how in locally applying, testing and monitoring compliance with widely agreed open internet standards.
  - Key elements include national internet infrastructure protection, internet exchange points, registries, open source software, email security and routing security.

Supported by global and regional stakeholders

- GFCE members
  - Governments
  - International Organisations
  - Businesses
- Regional Internet Registries
  - All regions
- Internet Society
  - Global office
  - Local chapters
- NL Ministry of Economic Affairs

Internet Society

lacnic

AFRINIC

APNIC

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

GFCE

AfricaCERT
United in promoting cyber security in Africa

ICANN

LACTLD
Latin American and Caribbean ccTLDs Organization

Ministerie van Economische Zaken

Aim of the Capacity building events

- Targeted at regions that are catching up
- Bringing together regional stakeholders
- Awareness raising on Open Internet Tools
- Inspiration through Good Practice Examples (mix local/global)
- Impact through joint commitment for action

GFCE

GFCE TRIPLE - I

From State-of-Practice to State-of-the-Art, together

Joint priority setting and action planning

La Paz, 5 August 2019

LACTLD Latin American and Caribbean ccTLDs Organization

lacnic

ICANN

Internet Society

Internet Society Capítulo Bolivia

Ministry of Economic Affairs and Climate Policy

“What to do to improve justified trust in using the Internet and email in the region”

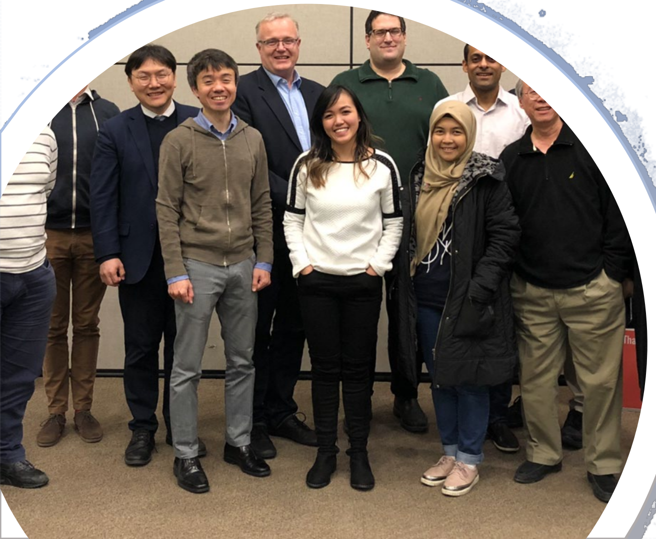
Purpose of the Day

GFCE Triple-I agenda for today

09:00	Opening, intent
09:30	Block I: Better Use of Today’s Open Internet Standards
11:30	Block II: Inspiration from Good Practice Actions - 1
12:30	Lunch
13:30	Block II: Inspiration from Good Practice Actions - 2
16:00	Block III: Action Planning for a More Trusted Internet
17:00	Conclusions and Closing Remarks

5 events so far

- Dakar, Senegal, hosted by the African Internet Summit, supported by AfricaCERT/AfriNIC/ISOC 2019, 7 May 2018
- Almaty, Kazachstan, hosted by RIPE NCC, supported by RIPE NCC/ISOC/Kazachstan Telecom, 25 September 2018
- Delhi, India, hosted by Indian Summerschool for Internet Governance, supported by ISOC/APNIC/Indian Govt, 12 October 2018
- Daejeon, Korea, hosted by APRICOT2019,supported by APNIC/ISOC/dotASIA, 23 February 2019
- Kampala, Uganda, hosted by the African Internet Summit, supported by AfricaCERT, AfriNIC, WACREN, ISOC, ICANN, 27 June 2019



Next events under preparation

GFCE TRIPLE - I

- Kolkata, India, hosted by Indian Summerschool for Internet Governance, supported by INSIG, ISOC, APNIC, Indian Gov, 14 November 2018

Triple I is a GFCE project

www.thegfce.com

For more information contact:

Maarten Botterman: maarten@gnksconsult.com
Arnold van Rhijn: A.C.F.vanRhijn@minez.nl

About Maarten Botterman

- More than 25 years experience with work “in the public interest”: where connected technologies touch society - internationally
- Independent analyst, strategic advisor, moderator and chairman, see for more: www.gnksconsult.com
- Currently chairing: IGF Dynamic Coalition on Internet of Things (www.iot-dynamic-coalition.org/); PICASSO Policy Expert Group (www.Picasso-project.eu), and Supervisory Board of NLnet Foundation (www.nlnet.nl.)
- ICANN Board Member (www.icann.org)
- Full CV: https://www.linkedin.com/in/botterman
- Email: maarten@gnksconsult.com

Mejor uso de los estandares abiertos de Internet

DMARC: DKIM / SPF

IPV6

GFCE

Global Forum on Cyber Expertise

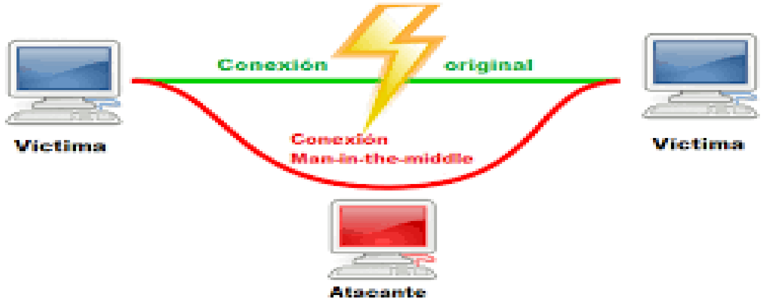
DMARC – DKIM - SPF

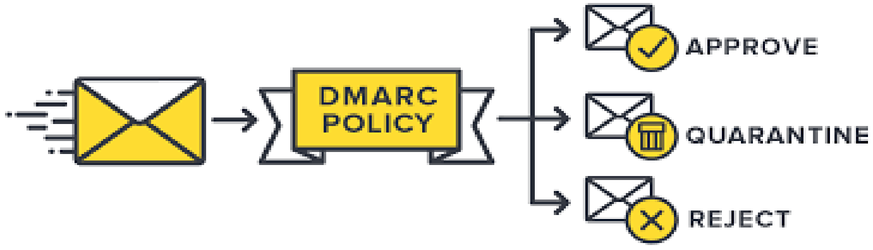
Tres protocolos basados en DNS del nombre de dominio

- **SPF** Certifica que el IP emisor esta permitido de hacer envios de e-mail. Evita el uso fraudulento del nombre de dominio.

- **DKIM** protocolo criptográfico basado en el uso de claves publicas registrados en su DNS. Firma el e-mail con el nombre de dominio y certifica que no haya habido alteración.

- **DMARC** permite tomar acciones y notificar basados en los dos protocolos anteriores en caso de ataques.





"spf=pass", "dkim=pass" y **"dmarc=pass"**

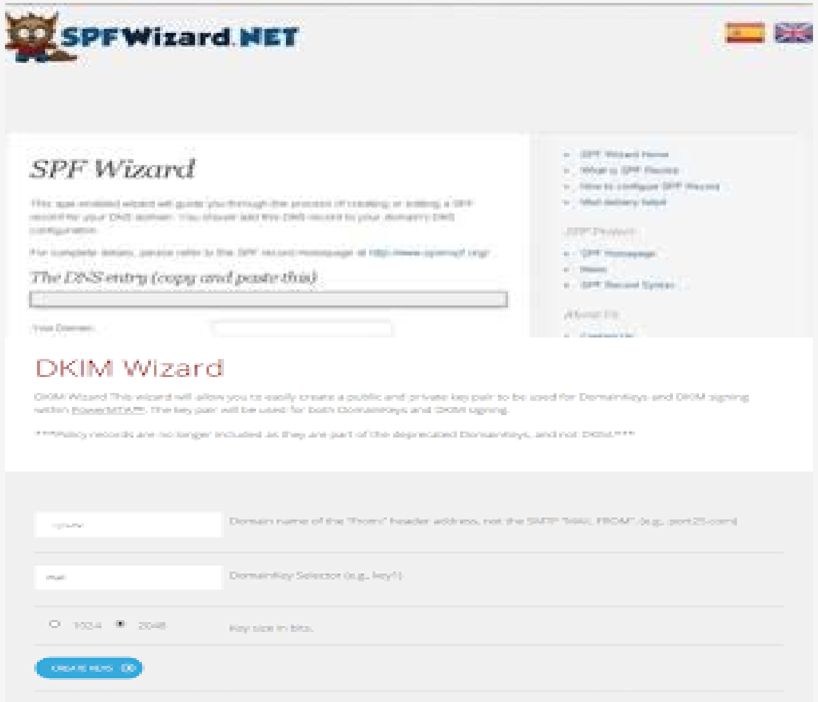
Retos en la adopción de los Estándares

Se identifica que:

1. Habilidades adecuadas para comprender, implementar y configurar adecuadamente.

2. Planificar – Hacer – verificar y actuar con la participación de las múltiples partes interesadas de la organización (monitoreo y ajuste de configuraciones.

3. Trust By Design.



SPFWizard.NET

SPF Wizard

This ajax enabled wizard will guide you through the process of creating or editing a SPF record for your DNS domain. You should add this DNS record to your domain's DNS configuration.

For complete details, please refer to the SPF record homepage at http://www.openspf.org/

The DNS entry (copy and paste this)

Your Domain:

- SPF Wizard Home
- What is SPF Record
- How to configure SPF Record
- Mail delivery Setup

SPF Project

- SPF Homepage
- News
- SPF Record Syntax

About Us

- Contact Us

DKIM Wizard

DKIM Wizard This wizard will allow you to easily create a public and private key pair to be used for DomainKeys and DKIM signing within PowerMTA™. The key pair will be used for both DomainKeys and DKIM signing.

Policy records are no longer included as they are part of the deprecated DomainKeys, and not DKIM.

Domain name of the "From:" header address, not the SMTP "MAIL FROM" (e.g. port25.com)

DomainKey Selector (e.g., key1)

○ 1024 ● 2048 Key size in bits.

CREATE KEYS

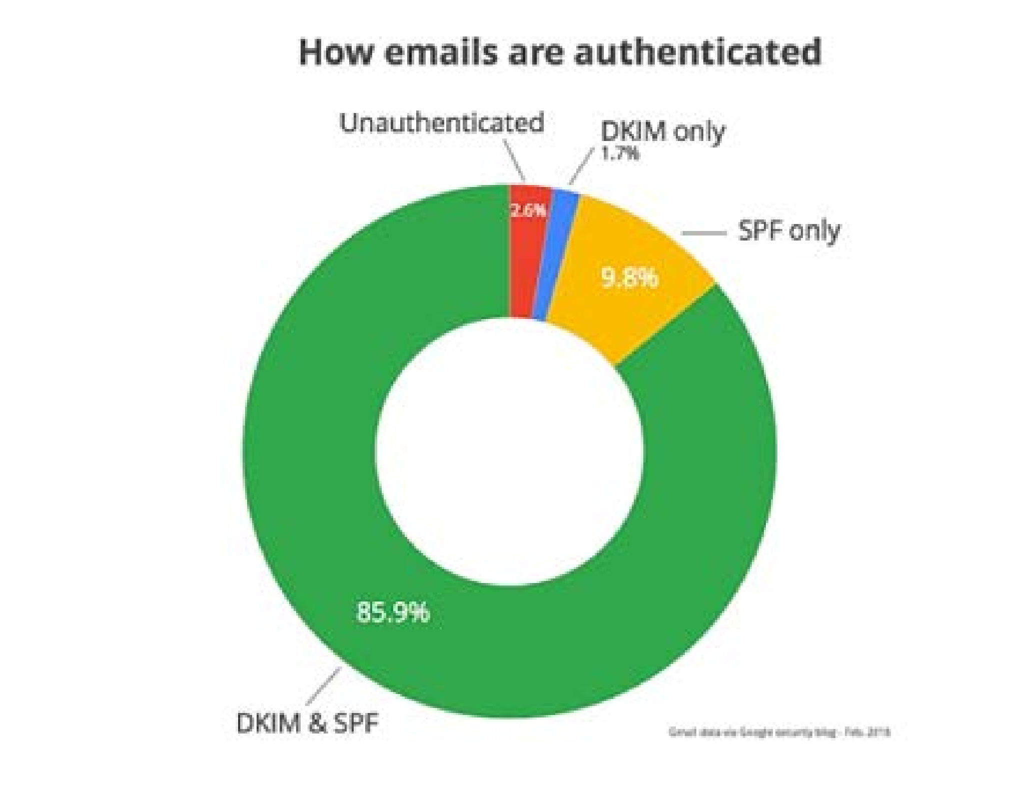
Reporte de Adopción

Gmail reporta al 2016 el siguiente porcentaje de adopción:

- El 86.8% de los correos que recibió están firmados de acuerdo al estándar DKIM.

- El 95.3% de los correos que recibió provenían desde servidores de correo (MTA) que usan el estándar SPF.

- El 85% de correos que recibió estaban protegidos por ambos estándares (SPF & DKIM)



How emails are authenticated

Gmail data via Google security blog - Feb. 2016

IPV6

IPv6, es una versión del Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol version 4 (IPv4) RFC 791, encargado de dirigir y encaminar los paquetes en la red, fue diseñado en los años 70 con el objetivo de interconectar redes.

IPv4 -> 4.294.967.296 direcciones IP posibles

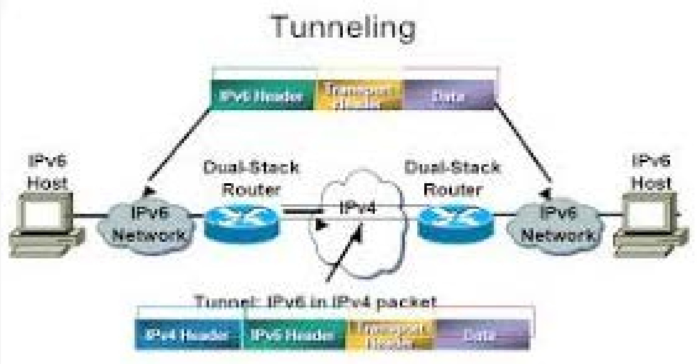
IPv6 -> 340 sextillones

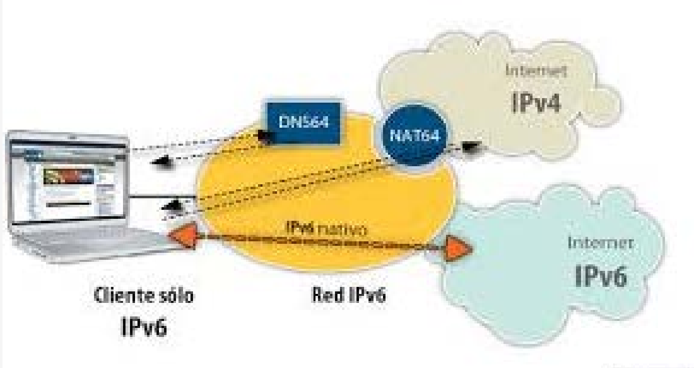
Clasificación general entre los mecanismos de transición de acuerdo al tipo de técnica que se utiliza:

Dual stack

Túneles

Traducción





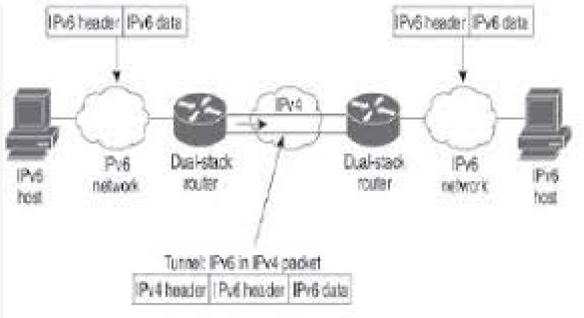
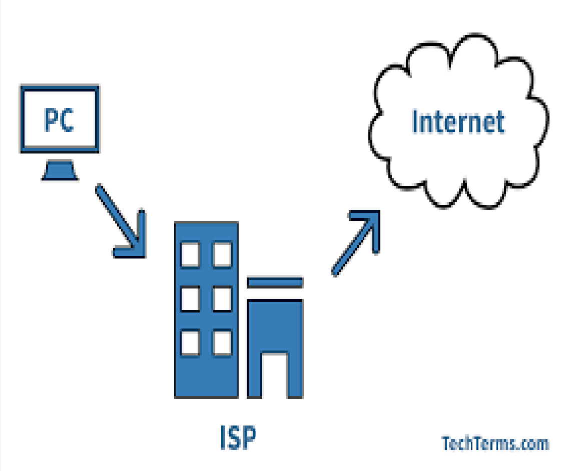


Figura 5. Modelo general del esquema túnel [8].

Partes involucradas en la adopción IPv6

Existen cuatro grupos importantes en la adopción e implementación de IPv6:



1. Proveedores de Infraestructura de Red y Software.
   Modificacion de sus productos para incorporar capacidades

2. ISPs
   Actualización de sus redes para brindar acceso

3. Usuarios Finales
   Asegurando de que su red interna pueda manejar tráfico IPv6

4. Otros, ej.organizaciones, generadores de contenido, etc.

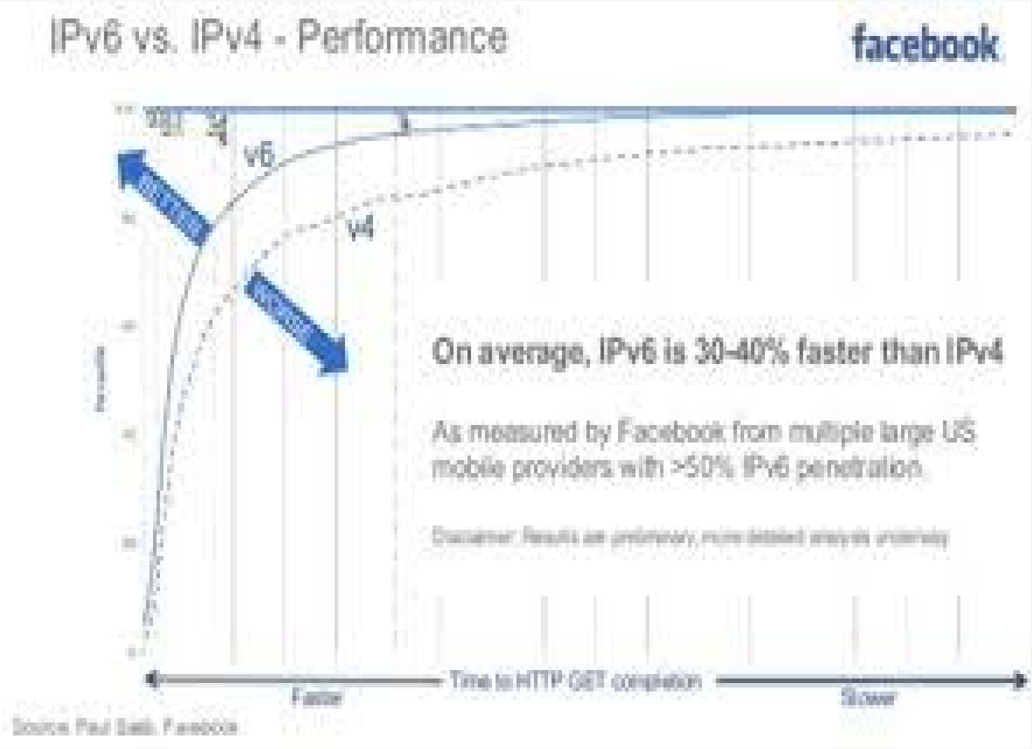
Beneficios de implementar IPv6

- ***Mejora en la conectividad***, un Internet más eficiente, seguridad integrada, autoconfiguracion y soporte mejorado para la movilidad.

- ***Continuidad empresarial e innovación***. despliegue de nuevas aplicaciones y servicios, como información en tiempo real (conectividad mejorada de extremo a extremo), servicios móviles personalizados, e Internet de las cosas (IoT). Las organizaciones que no hayan adoptado IPv6 no podrán conectarse a usuarios que solo tengan IPv6.

- ***Disminución de costos y menor complejidad***, A menudo se reduce a "ahorrar dinero y simplificar la red" (ISOC, 2017). Costo de obtener una dirección IPv4 está aumentando (mercado negro). IPv6 también simplifica la administración de la red (por ejemplo, elimina la necesidad de usar la traducción de direcciones de red - NAT) y tiene características que se pueden usar contra ataques cibernéticos.

- ***Crecimiento económico nacional***, direcciones IP son esenciales para el funcionamiento y la evolución de Internet. Las infraestructuras nacionales que utilizan IPv6 están mejor equipadas para aprovechar las oportunidades económicas que ofrecen los dominios innovadores, como las ciudades inteligentes y las redes inteligentes.



IPv6 vs. IPv4 - Performance

On average, IPv6 is 30-40% faster than IPv4

As measured by Facebook from multiple large US mobile providers with >50% IPv6 penetration.

Disclaimer: Results are preliminary, more detailed analysis underway

Source: Paul Saab, Facebook

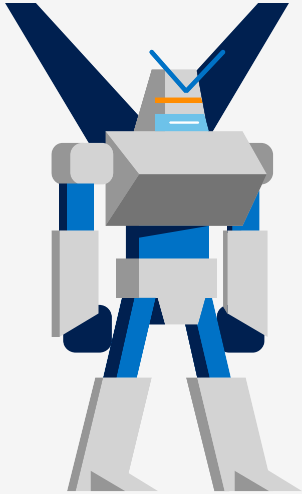
Retos en la implementación de IPv6

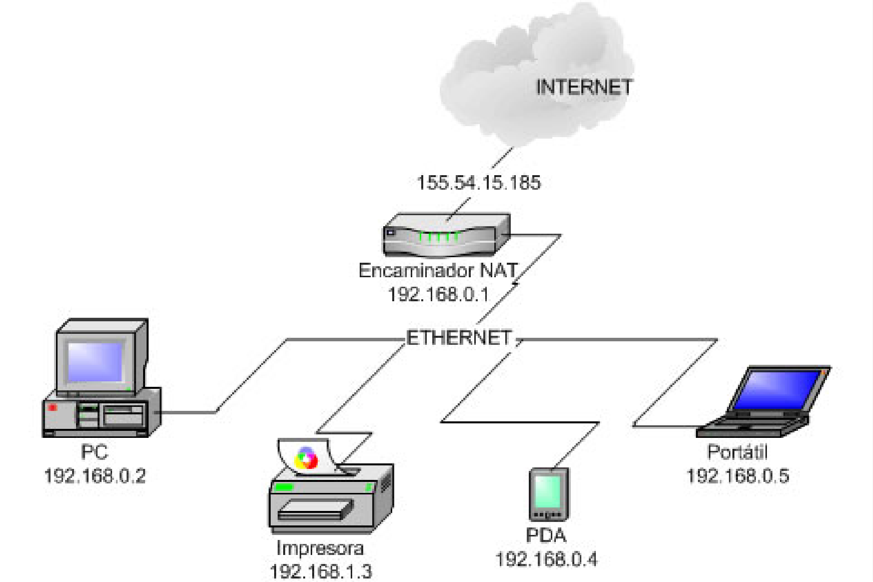
1. **Recursos**; esfuerzo, habilidad y recursos. Los desarrolladores de software y hardware, operadores de red, usuarios finales y otras partes interesadas, a menudo necesitan realizar cambios en sus sistemas y servicios para implementar IPv6.

2. **Percepción de falta de necesidad**. percepción de que IPv6 no tiene una "aplicación asesina" específica. Costos altos de IPv4 y las redes IPv4 aumentarán hasta el punto de que se volverán más grandes que los costos de adoptar IPv6.

3. **Desafíos técnicos**. problemas prácticos manejables: interacción con múltiples firewalls incompatibilidad de infraestructura.

4. **NAT**. Falsa sensación de resolución de problema de agotamiento: problemas en investigación forense, degradación en el uso de aplicaciones, VozIP, multicast, anycast, P2P, entre otros. Dependencia.



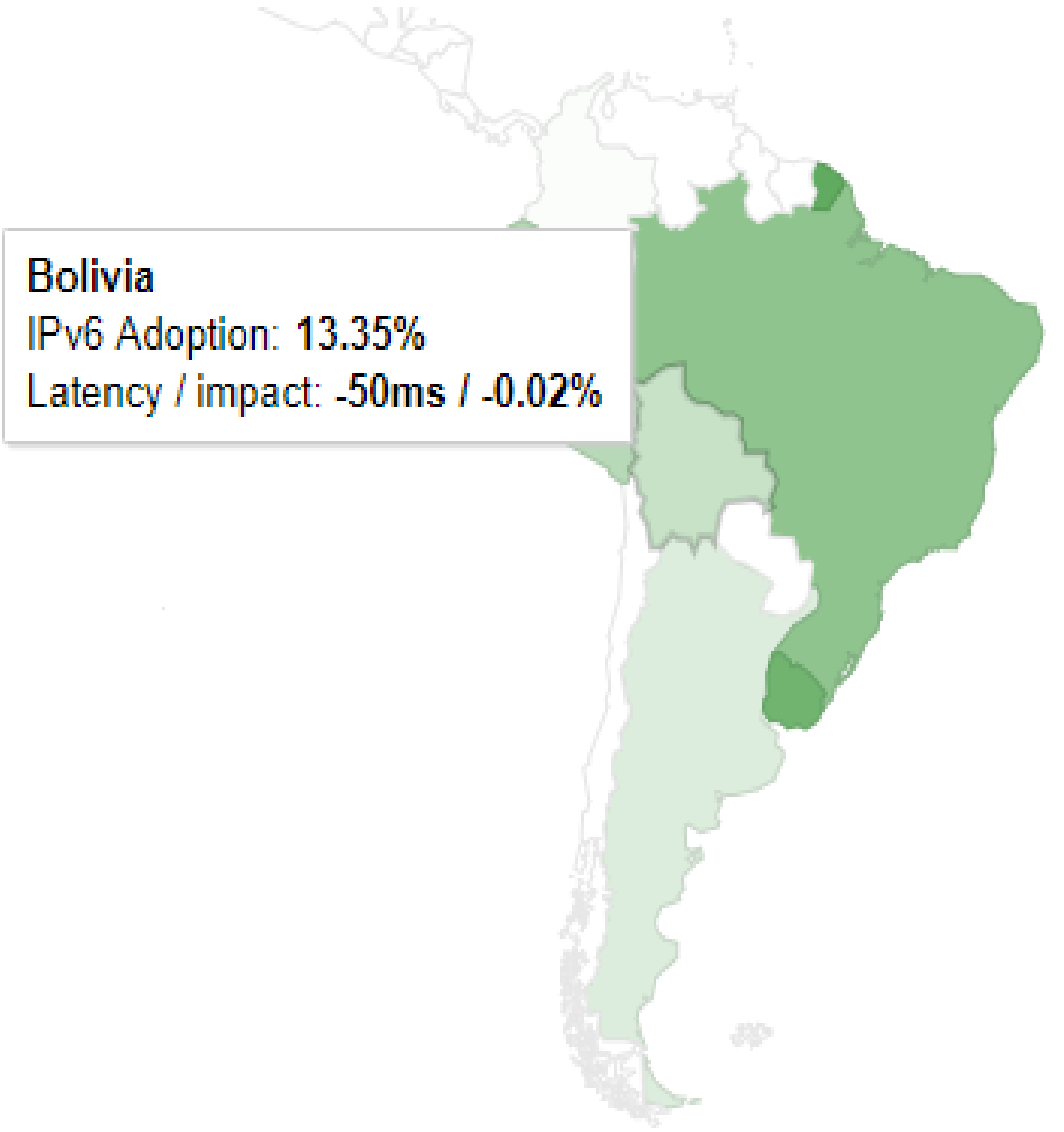


Estado Actual del despliegue de IPv6

Adopción ha sido moderada. las mediciones de IPv6 de Google, Akamai y APNIC muestran que IPv6 ahora ha surgido de las etapas de implementación "Innovadores" y "Adopción temprana" y se está moviendo a la "Mayoría temprana". Comienzo del declive del mercado de direcciones IPv4.

Los RIR en todo el mundo se han quedado sin direcciones IPv4 (solo se pueden asignar direcciones a los nuevos participantes en el mercado LATAM /22.

Además del agotamiento de las direcciones IPv4, hay cada vez más organizaciones individuales que dan el paso para promover el despliegue de IPv6. Por ejemplo, en Bélgica, dos ISP principales decidieron promover IPv6. limitar el uso de NAT (para permitir una informática forense más efectiva)



GRACIAS

La nube anycast de LACTLD

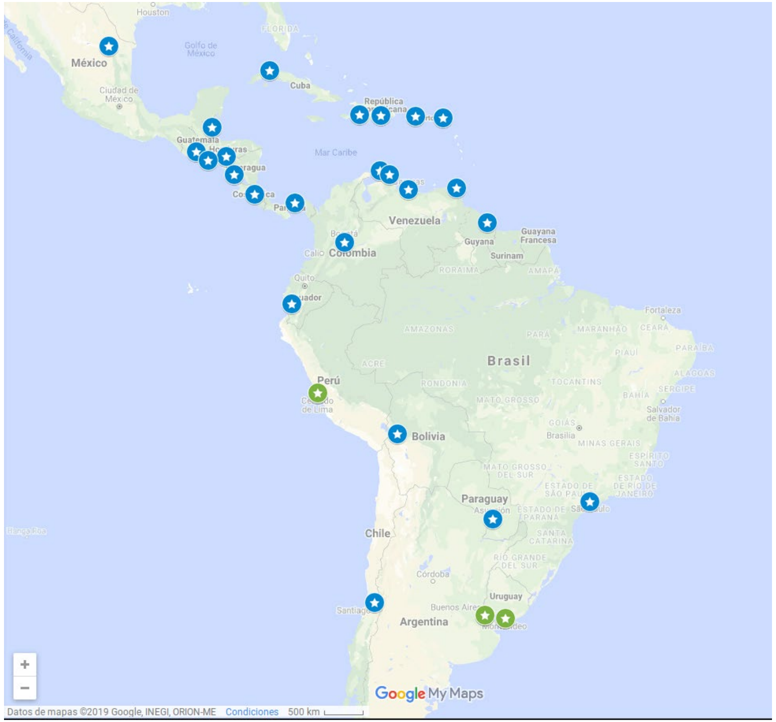
Workshop GFCE Triple-I
La Paz - agosto 2019

nic chile
SOMOS EL PUNTO CL

LACTLD
Latin American and Caribbean
ccTLDs Organization

¿Qué es LACTLD?

- organismo que agrupa a los ccTLDs de Latinoamérica y el Caribe
- fundado en 1998
- 27 asociados



Datos de mapas ©2019 Google, INEGI, ORION-ME Condiciones 500 km

Cómo funciona el DNS en un ccTLD

- múltiples “servidores autoritativos”
- generalmente 1 es primario y el resto secundarios
- permite
    - distribuir la carga
    - acercarse a los clientes
    - robustez y resiliencia

Cooperación en DNS desde los inicios

- “Intercambio” de secundarios
- De buena fe, informal
- Poco escalable
- Ejemplo:
    - CL entrega secundario a CR, ES, PA y VE
    - BR a BO, CU, GH, GT, PA, PT, SV y UY
    - etc.

Upgrade: servicio anycast

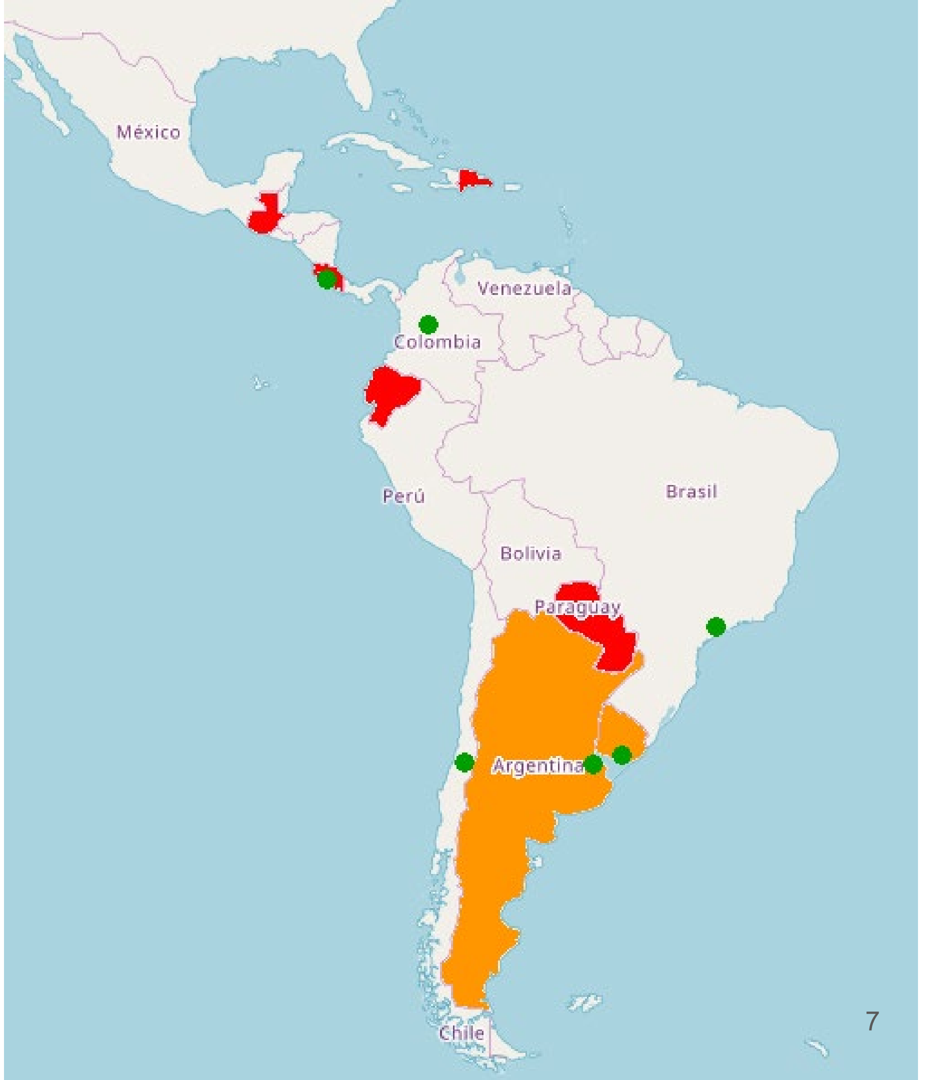
- la tecnología “anycast” es la evolución del servicio de secundarios
- 1 servidor “esconde” múltiples nodos dentro de una “nube”
- altamente escalable
    - raíz F tiene más de 230 nodos
- más eficiente ante caída de nodos
- mejor comportamiento ante ataques DoS

Nube anycast de LACTLD

- servicio para miembros de LACTLD
    - e infraestructura crítica
- cada ccTLD puede cooperar con uno o varios nodos
    - también pueden alojar nodos organismos externos (IXP)
- cada ccTLD puede utilizar la nube con su ccTLD como cliente
- la administración de la nube es compartida entre ccTLDs miembros
    - se aprovecha la experiencia de cada organización
- acuerdos de cooperación con LACTLD

Proyecto exitoso

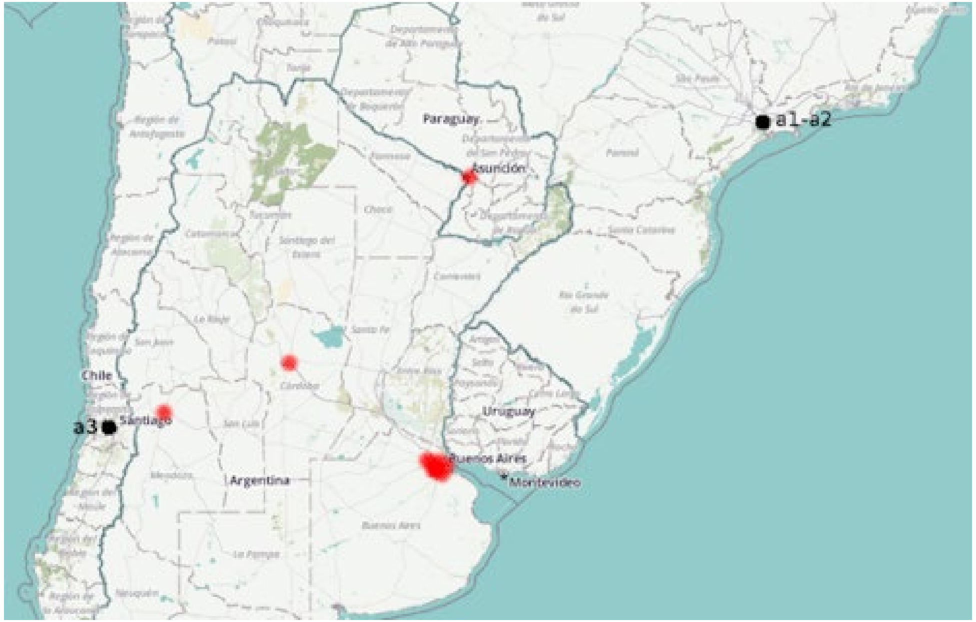
- en operación desde el 2015
- administradores: .BR, .CL y LACNIC
- 8 ccTLDs
  - 124 zonas
  - 6 ya delegados en full producción (.cr, .py, .ec, .do, .gt, .pr)
- 7 nodos en producción:
  - Brasil, Chile, Argentina, Uruguay, Colombia y Costa Rica



Mejoras continuas

- Instalación de un nuevo nodo mejora el tiempo de respuesta en la vecindad del nodo para todos los ccTLDs que son clientes de la nube

- Ejemplo: estudio de instalación de nodo en Buenos Aires
    - entre 16% y 80% de RTT



Fuente: https://labs.ripe.net/Members/hugo_salgado/visualisation-of-a-new-node-in-lactld-anycast-service

Pronto

- 1 nuevo ccTLD (El Salvador .sv)
- 3 nuevos nodos: NIC.MX (México, USA), NIC.CZ (Praga)
- Acuerdo con LAC-IX para instalación de nuevos nodos

Conclusiones

- Ejemplo de colaboración regional
- Juntos podemos compartir recursos
- Tecnología desarrollada y mantenida en la región
- Robustez y resiliencia de la Internet en Latinoamérica

Gracias

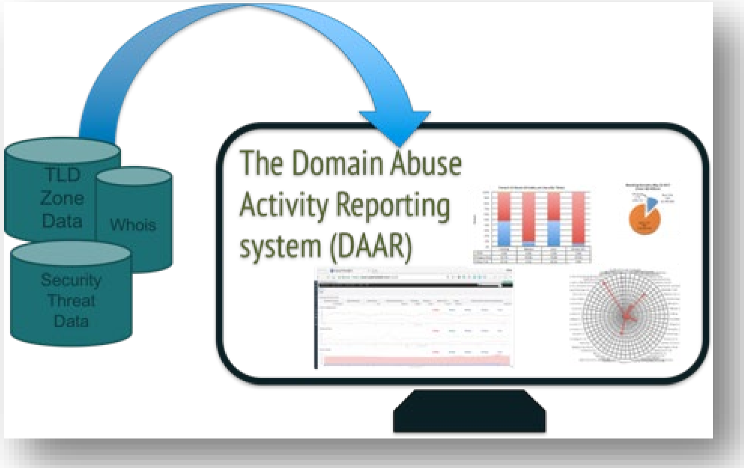
anycast.lactld.org

Hugo Salgado - hugo@nic.cl

nic chile
SOMOS EL PUNTO CL

LACTLD
Latin American and Caribbean
ccTLDs Organization

The Domain Abuse Activity Reporting System (DAAR)



Daniel Fink, ICANN
LACIGF, La Paz

August 2019

The Domain Abuse Activity Reporting System

What is the Domain Abuse Activity Reporting system?

A system for reporting on domain name registration and abuse data across TLD registries and registrars

Domain abuse

DAAR identifies and tracks domain names associated with four kinds of abuse:

I. Phishing.
II. Malware.
III. Botnet command-and-control.
IV. Spam.

The Domain Abuse Activity Reporting System

How does DAAR differ from other reporting systems?

- Studies all gTLD registries and registrars for which we can collect zone and registration data
- Employs a large set of abuse feeds (e.g., blocklists)
- Accommodates historical studies
- Takes a scientific approach: transparent, reproducible

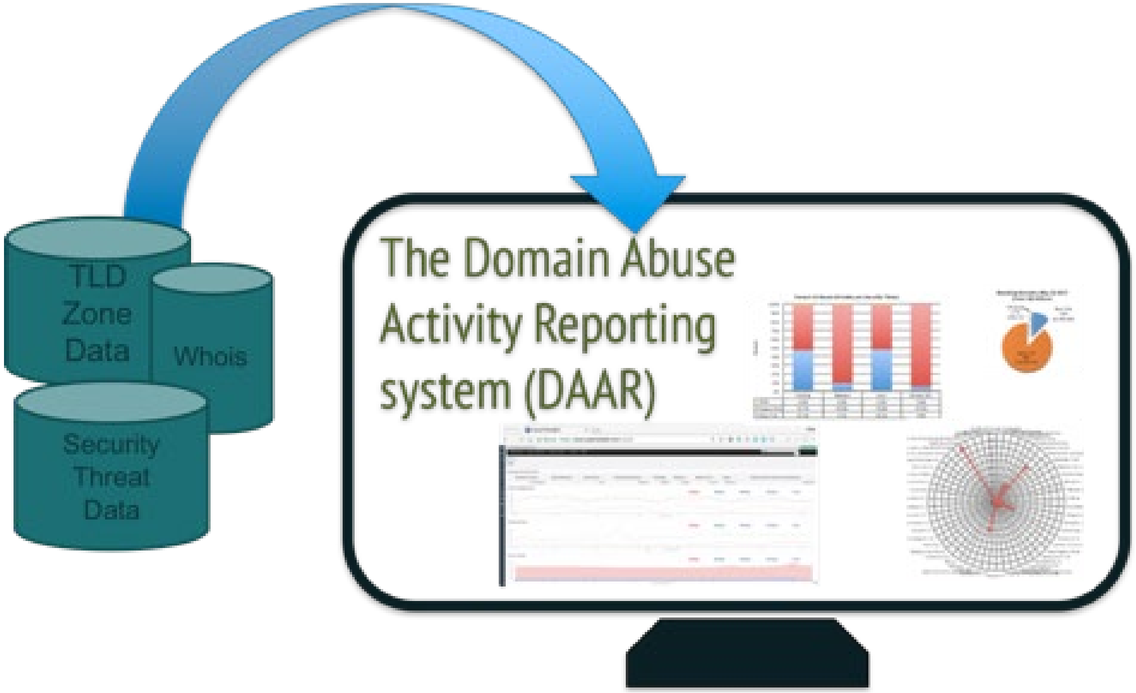
Project Goals

DAAR data can be used to

- Report on threat activity at TLD or registrar level
- Study historical security threats or domain registration activity
- Help operators understand or consider how to manage their reputations, their anti-abuse programs, or terms of service
- Study malicious registration behaviors
- Assist operational security communities

The purpose of DAAR is to provide data to support community, academic, or sponsored research and analysis for informed policy consideration

DAAR Methodology & Domain Data



TLD Zone Data

Whois

Security Threat Data

The Domain Abuse Activity Reporting system (DAAR)

DAAR Uses TLD Zone Data

DAAR system uses data from public, open, and commercial sources

I. DNS zone data

II. WHOIS data

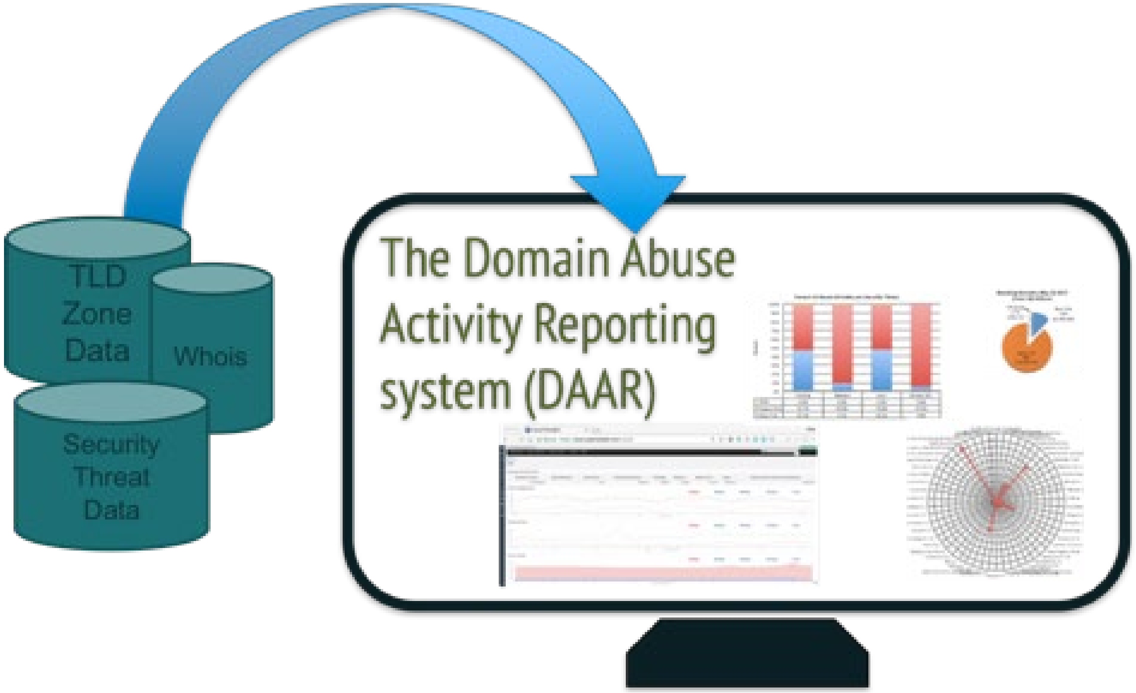
III. Open source or commercial abuse threat (Reputation Blocklist) data*

*Certain data feeds require a license or subscription

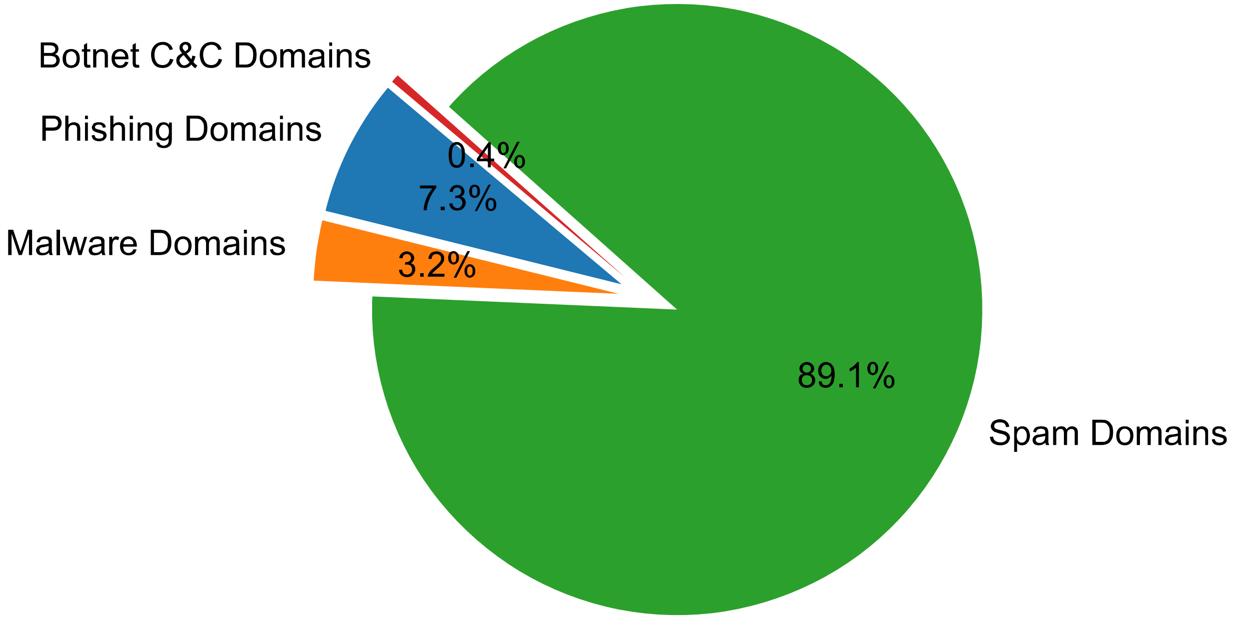
Current Reputation Datasets

- SURBL lists (domains only)
- Spamhaus Domain Block List
- Anti-Phishing Working Group
- Malware Patrol (Composite list)
- Phishtank
- Ransomware Tracker
- Feodotracker

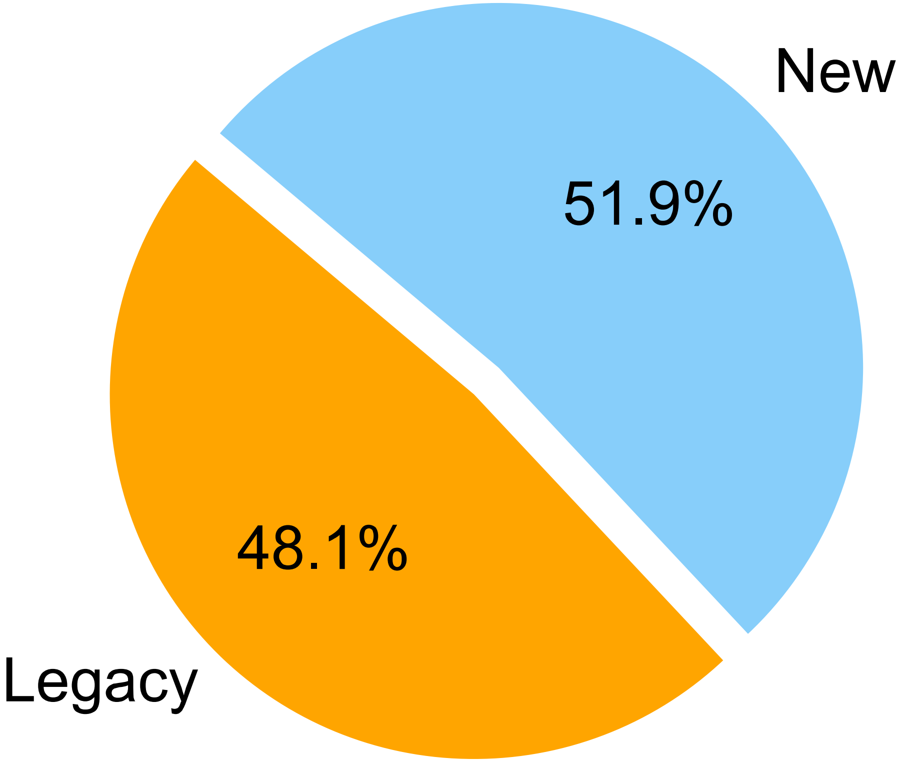
Visualizing DAAR Data



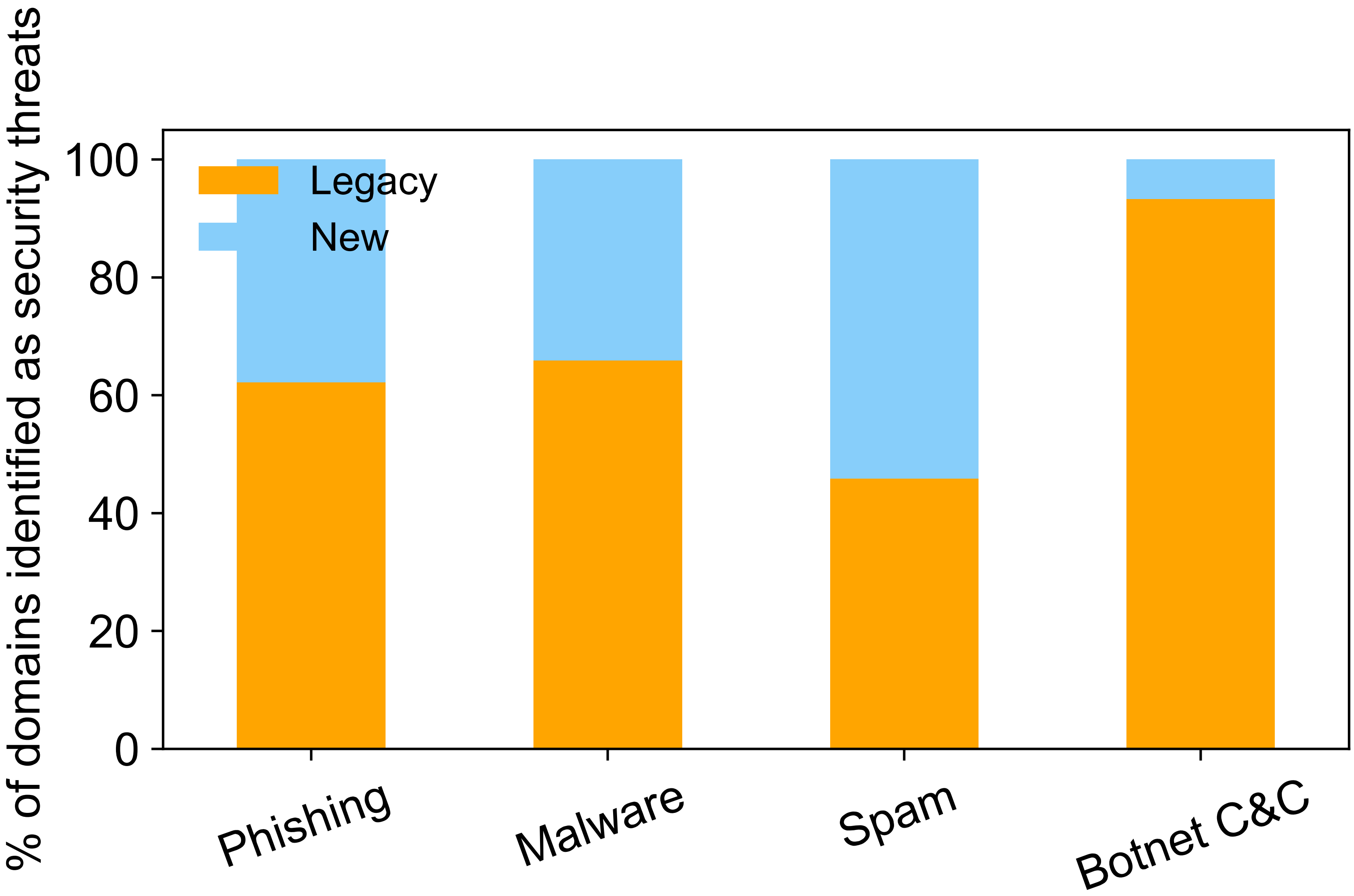
Overall Abuse Distribution in DAAR Data (Jan. 2019)



Distribution of Abused Domains in gTLDs



Distribution of Domains with Different Abuse Types in gTLDs



Thank You

- [@icann](#)
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann

Contact Info:
DAAR@icann.org
https://www.icann.org/octo-ssr/daar

BLOCK I
Better Use of Today’s Open Internet Standards

GFCE Triple-I Day @LACIGF2019

Daniel Fink

5 Ago 2019 – LACIGF, La Paz, Bolivia

ICANN

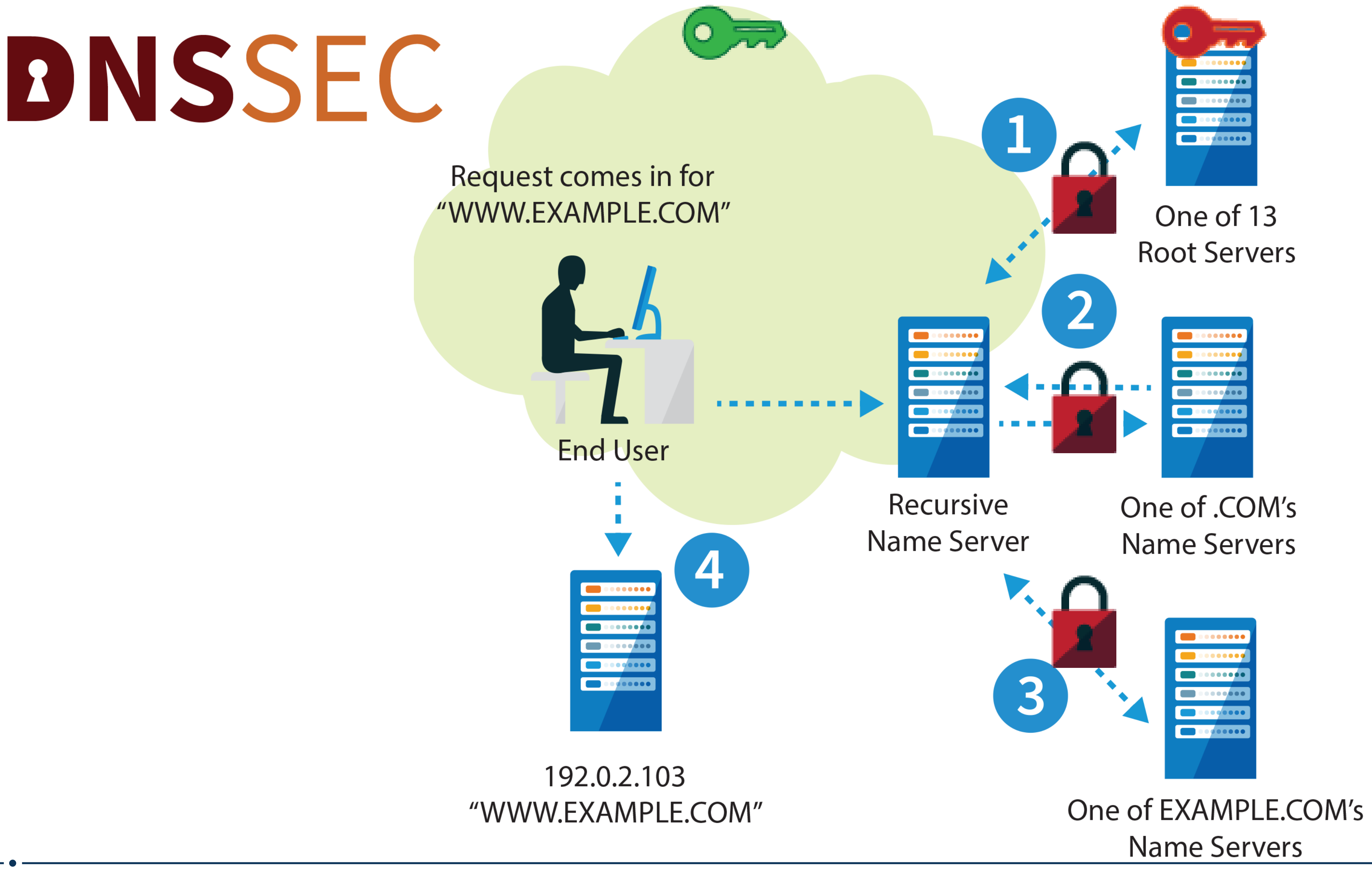
DNSSEC

What is DNSSEC?

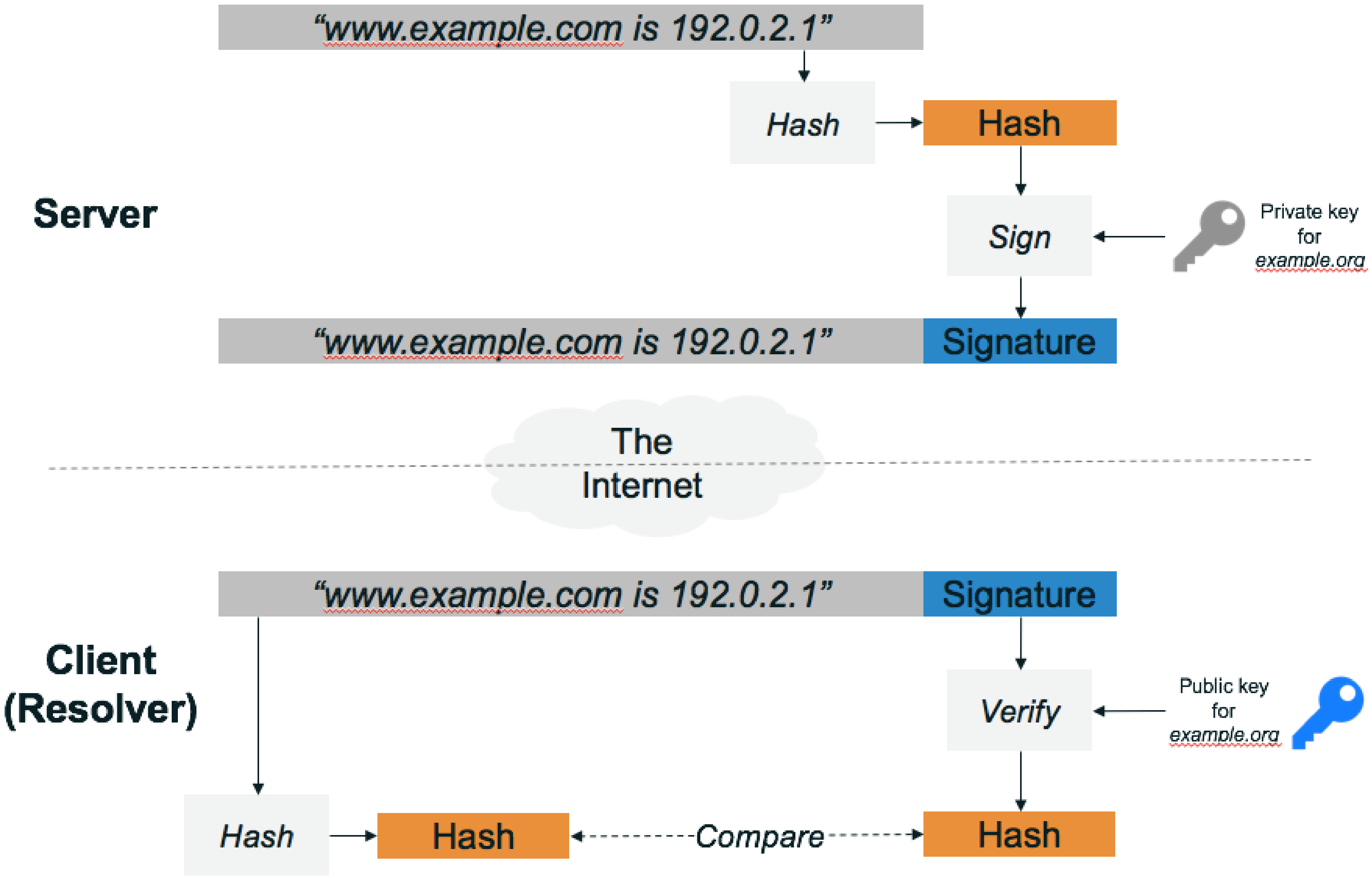
Domain Name System Security Extensions (DNSSEC)

- To help prevent DNS abuse, DNSSEC introduces cryptography that provides assurances to users that DNS data they are seeing is valid and true
- Domain name registrants **SIGN** their DNS data
- DNS operators **VALIDATE** all DNS data passing through DNS resolvers

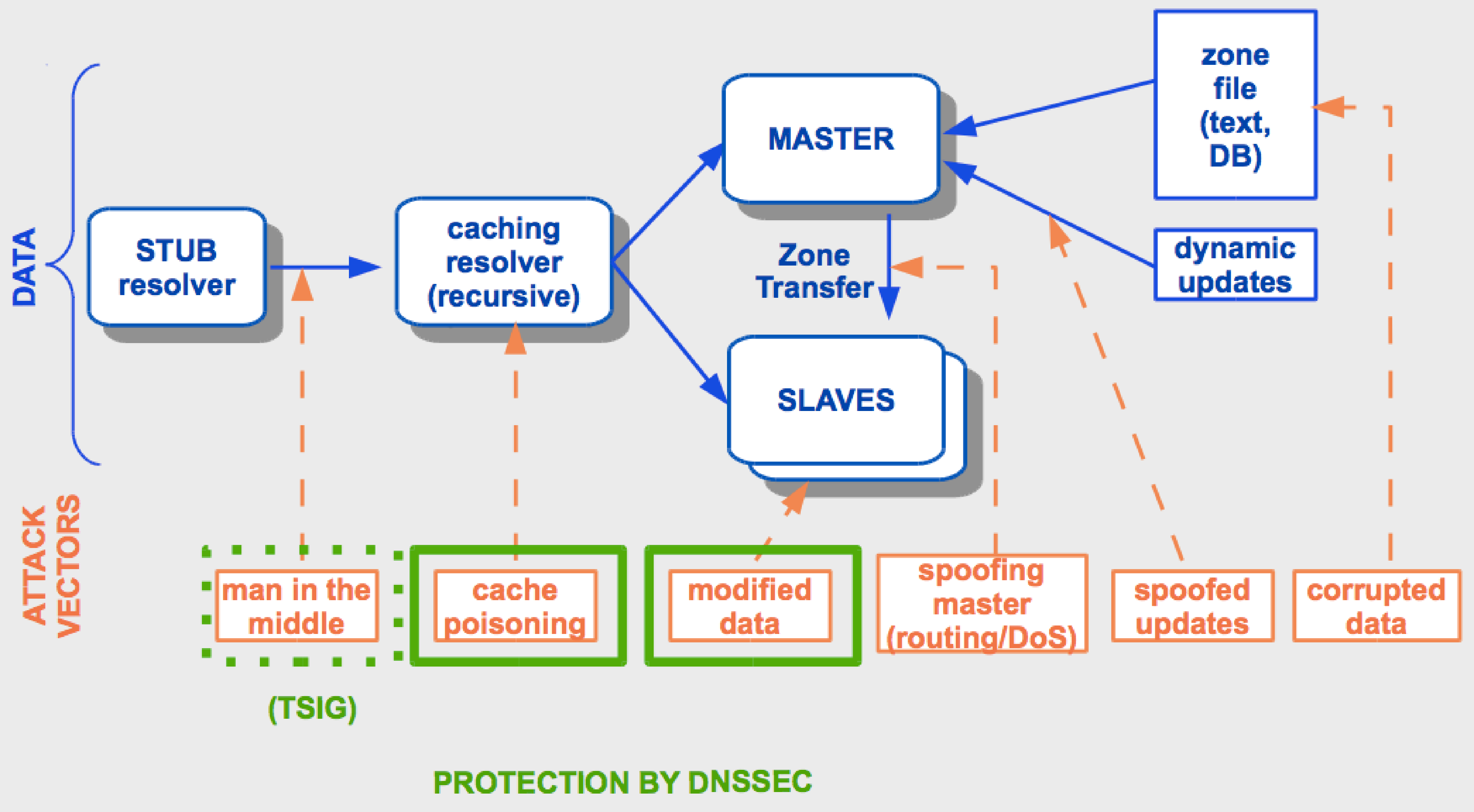
How DNSSEC Works



How DNSSEC Works



What does DNSSEC protect?



DNSSEC

Benefits

- End User – gain confidence of reaching intended website
- Registrant – fraud mitigation & greater brand protection
- Registrar – Comply with industry standards & meet registrant demands for increased security
- Registry – Meet industry best practices & registrar demands for increased domain security

State of DNSSEC Deployment

Over 90% of top-level domains are signed with DNSSEC

- 1530 TLDs in the root, 1399 are signed (as of 13 July 2019)
- About 50% of ccTLDs are signed
- Recent adoption in Kuwait, Moldova, Algeria, Bhutan
- 2nd level DNSSEC deployment growing slow & steady

TLS

What is TLS?

Transport Level Security protocol (TLS)

- TLS provides protection of all data transmitted between two end-points (user and service) on the internet by encrypting the data stream.
- The most common use of TLS is creating a secure environment for **web browsing**.
- **HTTPS** is the secure version of HTTP and uses TLS to encrypt the transmitted data.

TLS

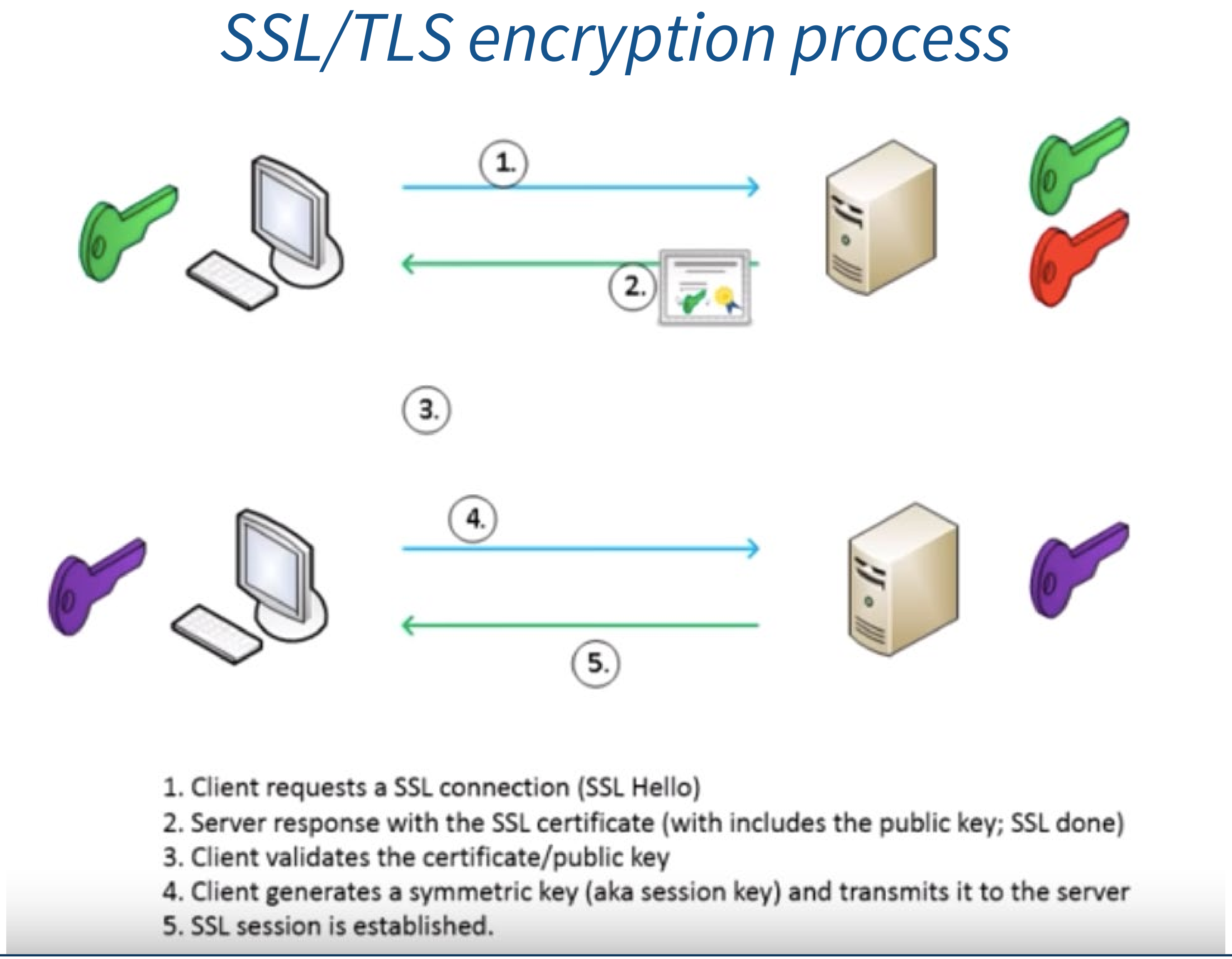
Benefits

- Privacy: prevent eavesdrop on messages (e.g. passwords)
- Integrity: manipulation of the message (Man-in-the-middle)
- Identification: the place you are visiting is the one you think it is

Goal

- Trusted end-to-end communication

How TLS Works



SSL/TLS encryption process

1. Client requests a SSL connection (SSL Hello)
2. Server response with the SSL certificate (with includes the public key; SSL done)
3. Client validates the certificate/public key
4. Client generates a symmetric key (aka session key) and transmits it to the server
5. SSL session is established.

TLS

HTTPS Weakness

- Limited means to verify that user is using the correct certificate
- Third parties (CAs) are able to issue certificates for any domain

Solution

- DNS-based Authentication of Named Entities (DANE)

DANE - DNS-based Authentication of Named Entities

- Enables a domain owner to specify which certificate a user should use to connect to the site.
- Information is digitally signed with DNSSEC.
- Also gaining momentum in securing e-mail communication and instant messaging applications.

Engage with ICANN – Thank You and Questions

ICANN

One World, One Internet

Visit us at **icann.org**

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann

Implementación DNSSEC

Entidad pública de Servicios Tecnológicos

adsib
agencia para el desarrollo de la
sociedad de la información en Bolivia

Firma digital

de Certificación Digital, como Entidad Certificadora Pública

www.firmadigital.bo

NIC .bo Bolivia

Administrar el Registro y Delegación de Dominios .bo

https://nic.bo

Administrar el Repositorio Estatal de Software Libr

Brindar la conformidad técnica para la adquisición o donación, ampliación y/o renovación de Lice

https://softwarelibre.gob.bo

1

Servicio de envío de notificaciones ADS
SMS, Push, Correo

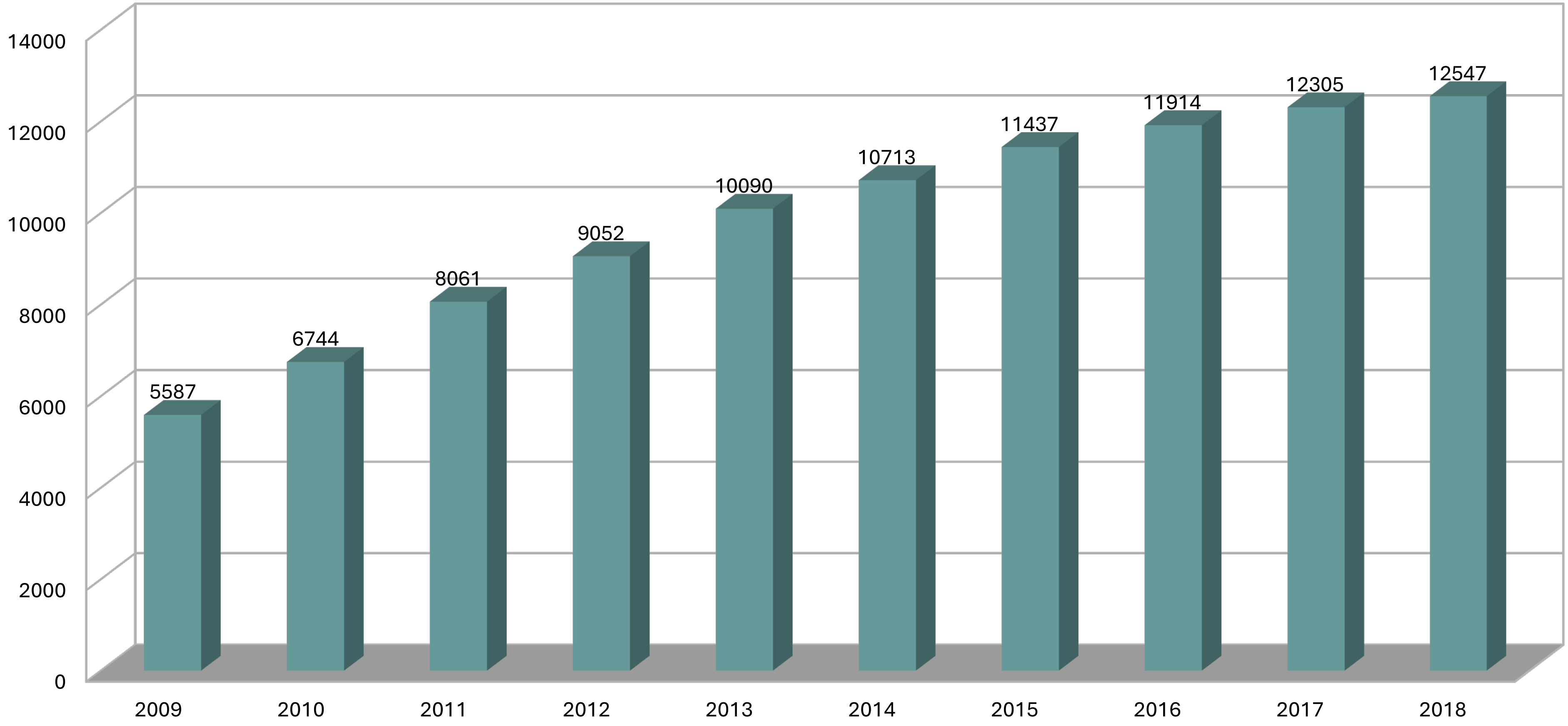
tidades

https://notificaciones.bo

“Desarrollar políticas, estrategias y acciones para brindar servicios fiables, in

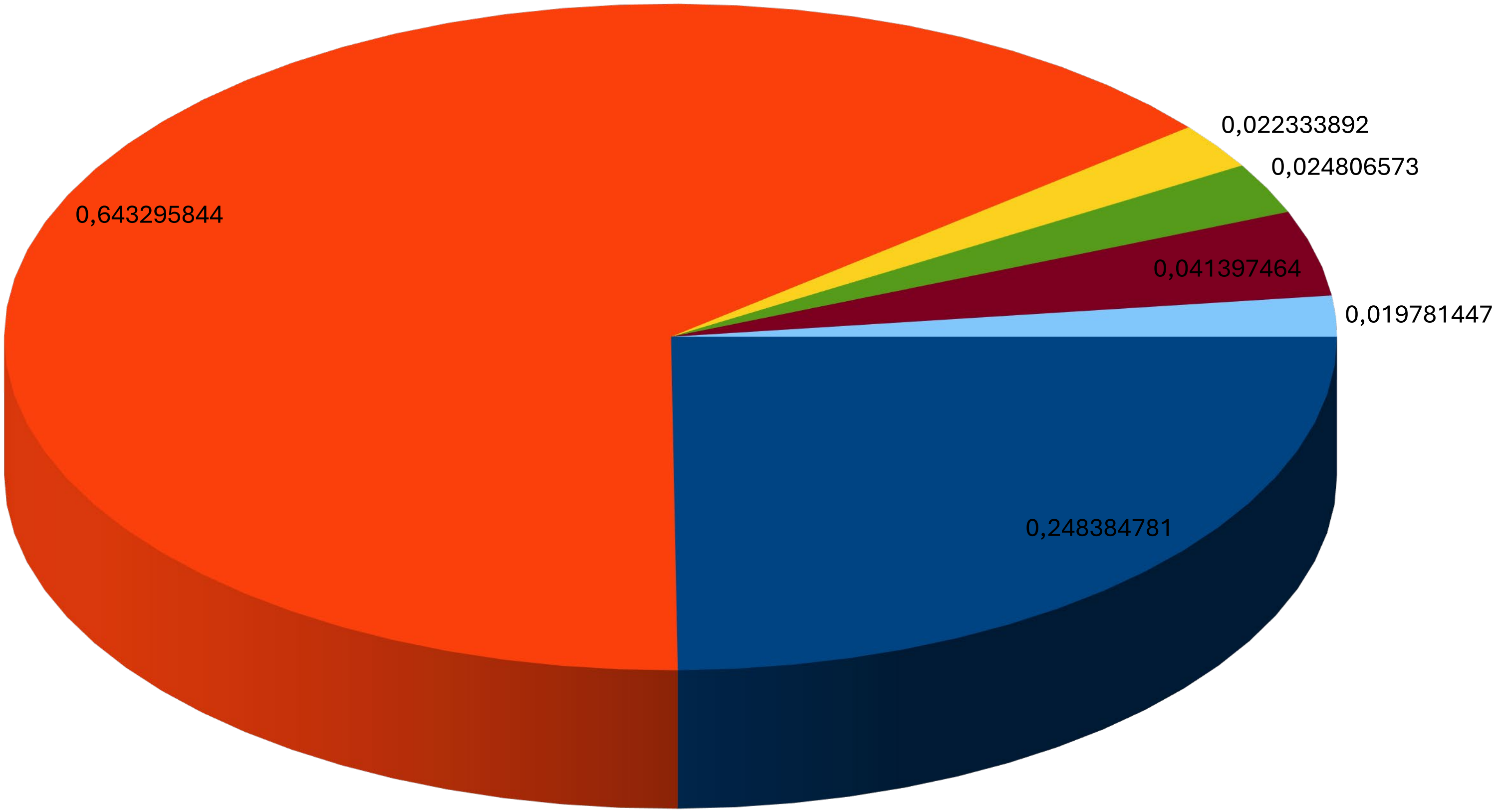
Servicio: Registro y renovación de dominios .bo

agencia para el desarrollo de la sociedad de la información en Bolivia



Número de dominios por gestión

Servicio: Registro y renovación de dominios .bo



.bo 25%

.com.bo 64%

edu.bo 2%

gob.bo 2,5%

org.bo 4%

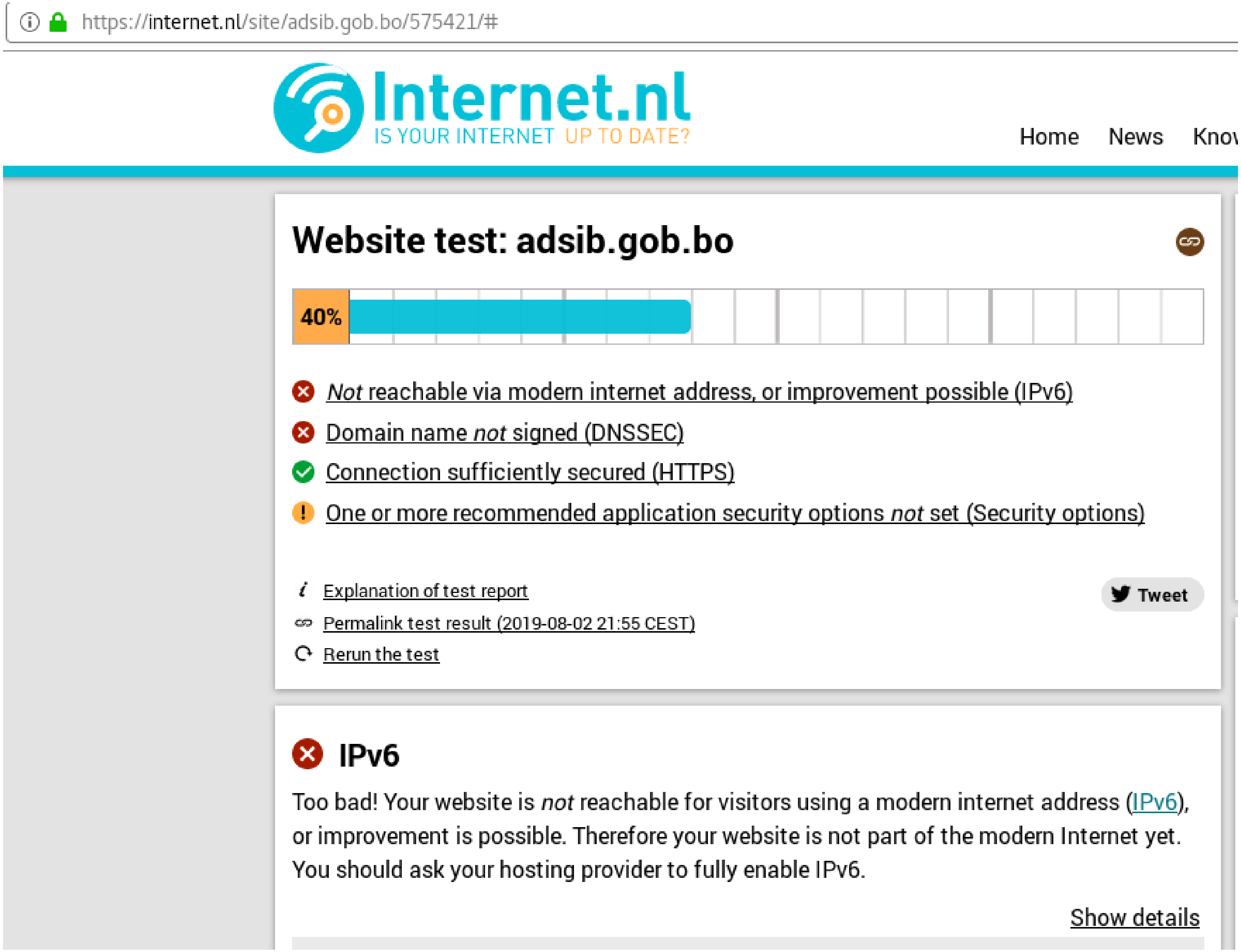
otros 2%

Composición dominios – gestión 2018

brindar servicios … SEGURIDAD

adsib
agencia para el desarrollo de la sociedad de la información en Bolivia

- DNSSEC



https://internet.nl/site/adsib.gob.bo/575421/#
Internet.nl
IS YOUR INTERNET UP TO DATE?
Home
News
Knov

Website test: adsib.gob.bo

40%

✗ *Not* reachable via modern internet address, or improvement possible (IPv6)

✗ Domain name *not* signed (DNSSEC)

✓ Connection sufficiently secured (HTTPS)

! One or more recommended application security options *not* set (Security options)

i Explanation of test report

Permalink test result (2019-08-02 21:55 CEST)

Rerun the test

✗ IPv6

Too bad! Your website is *not* reachable for visitors using a modern internet address (IPv6), or improvement is possible. Therefore your website is not part of the modern Internet yet. You should ask your hosting provider to fully enable IPv6.

QUE ES DNSSEC

DNSSEC es un conjunto de extensiones de seguridad que utiliza ***criptografía asimétrica*** para el servicio de DNS, que aporta los siguientes beneficios:

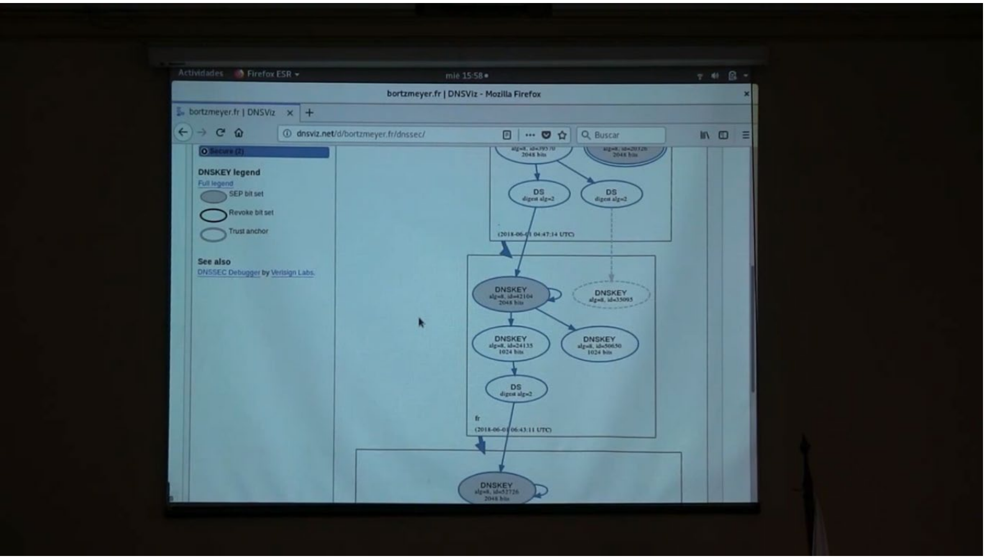
- Autentificar el origen de los datos de un servidor DNS.
- Mantener la integridad de los datos entre servidores DNS

Tiene como objetivo principal el *"impedir cualquier tipo de redireccionamiento no autorizado hacia un sitio malicioso basándose en la seguridad que brinda una cadena de confianza establecida desde la root zone (.)".*

Buenas prácticas: Establecer una cooperación de múltiples partes interesadas

“La cooperación contribuye al desarrollo de un entorno propicio a nivel nacional

Stéphane Bortzmeyer
AFNIC
Octubre 2018



Talleres DNSSEC

adsib
agencia para el desarrollo de la
sociedad de la información en Bolivia

Jose Machicado
ADSIB
Mayo y julio 2019

Talleres DNSSEC

Entidades
Vicepresidencia
Aduana Nacional
Ministerio de Obras Públicas, Servicios y Vivienda
Banco Central de Bolivia
Entel S.A
Contraloría General del Estado
SENASAG
Fondo Nacional de Desarrollo Regional
DATACOM
Administración de Servicios Portuarios
AGETIC
Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes ATT

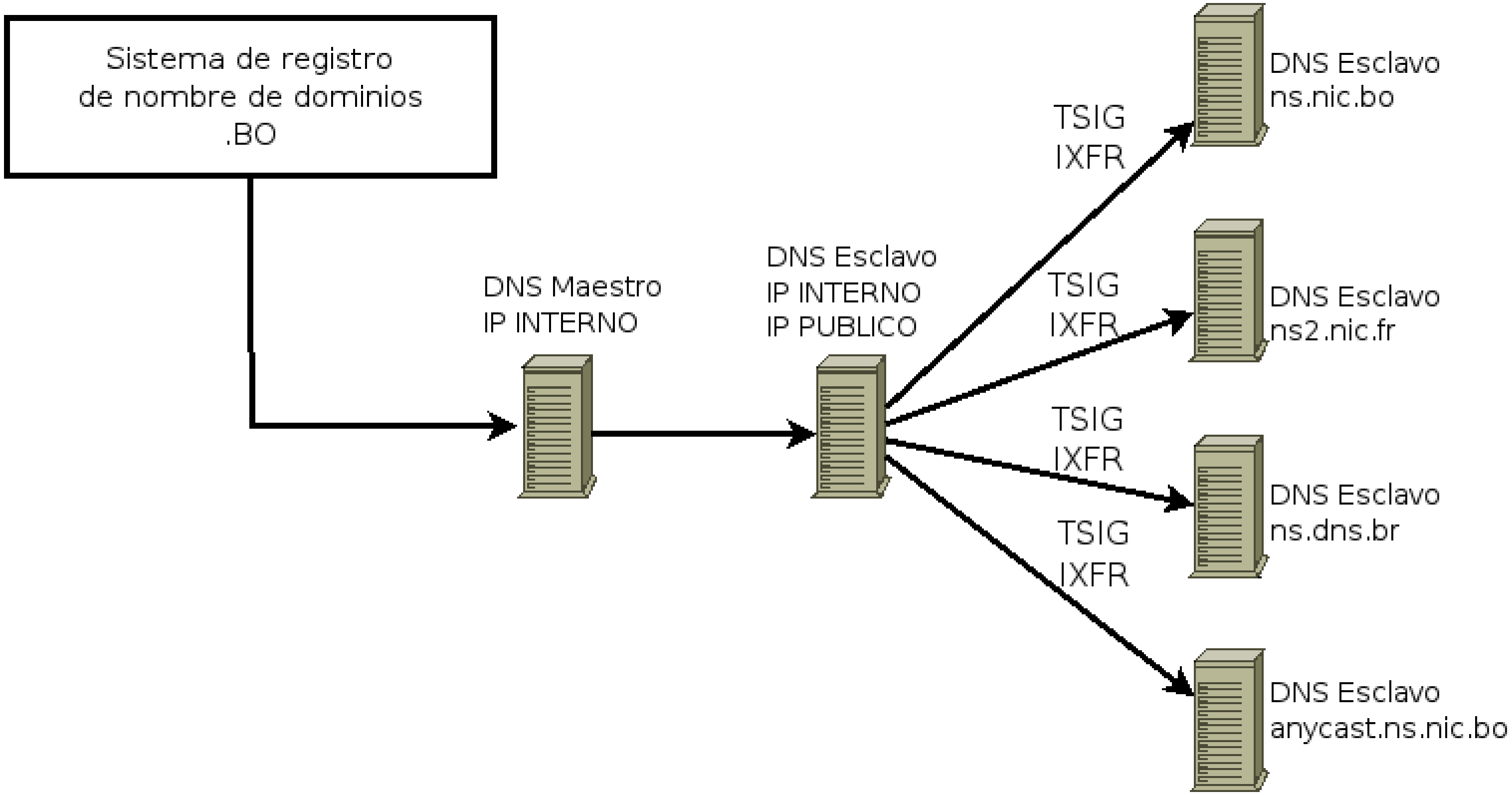
Despliegue DNSSEC en .bo

- Capacitación, investigación y comprensión de DNSSEC (**Realizado**)
- Pruebas Internas de DNSSEC (**Realizado**)
- Registro dnssec.bo y prueba de la Infraestructura. (**Realizado**)
- Capacitación final a entidades publicas (**Agosto**)
- Presentación de las políticas y procedimientos para DNSSEC (**Octubre**)
- Firmar la zona .BO (**Noviembre**)
- Enviar el registro DS a IANA (**Diciembre**)
- Registrar los DS de los usuarios (**Diciembre**)

INFRAESTRUCTURA

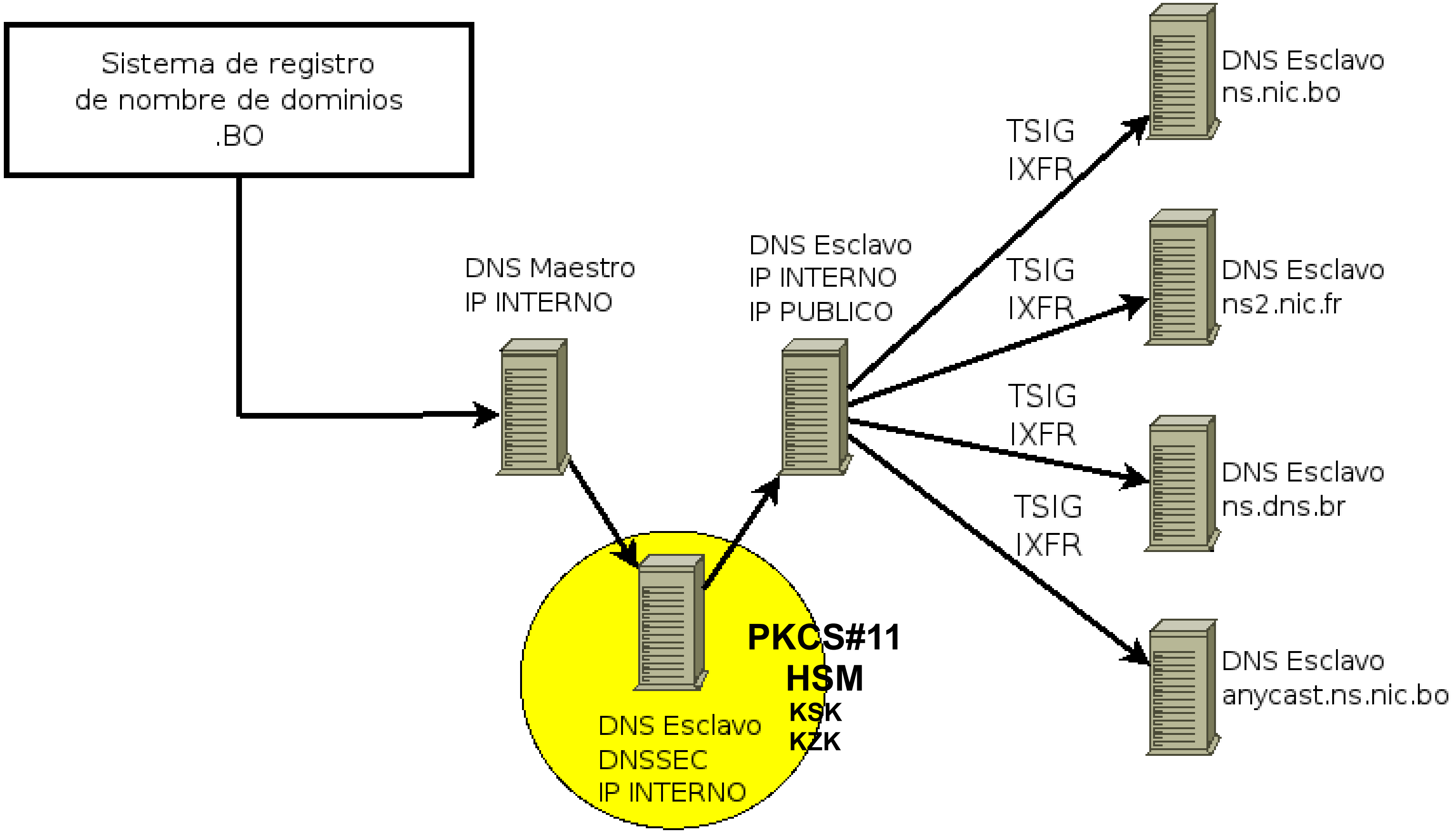
adsib
agencia para el desarrollo de la sociedad de la información en Bolivia

INFRAESTRUCTURA DNS ACTUAL



INFRAESTRUCTURA

INFRAESTRUCTURA DNS PARA DNSSEC



Firmado y renovación de claves

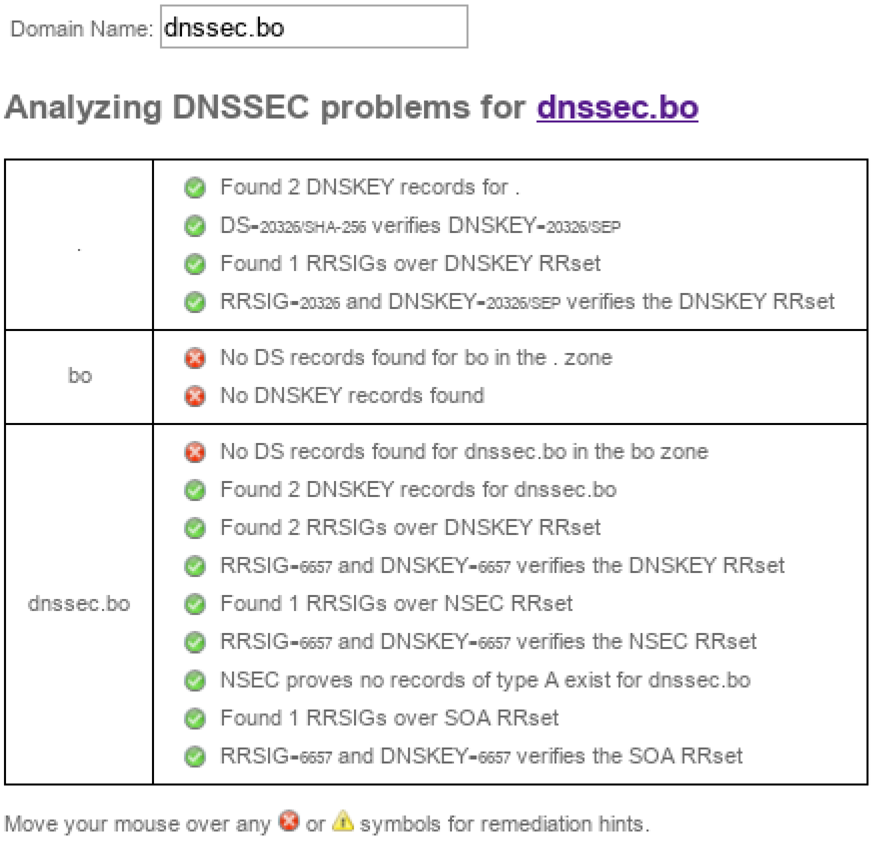
KSK (Key Signing Key):

- Tamaño de clave: 2048
- Reemplazo de la Clave: 2 años
- Esquema de reemplazo: Pre-publicación (una clave activa y una pasiva)
- Algoritmo: RSA/SHA256

ZSK (Zone Signing Key):

- Tamaño de clave: 1024
- Reemplazo de la Clave: 3 Meses
- Esquema de reemplazo: Generación de dos claves (Envío del registro DS a)
- Algoritmo: RSA/SHA256

Pruebas de validación

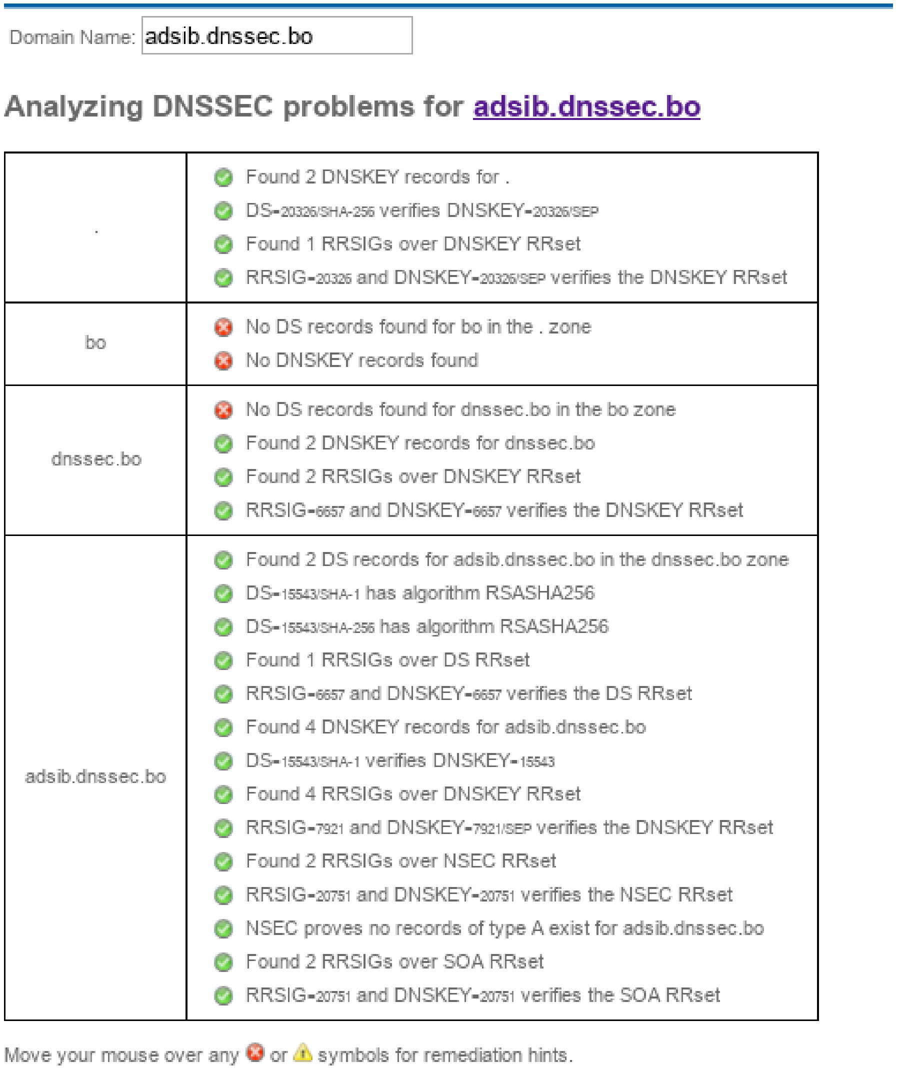


Domain Name: dnssec.bo

Analyzing DNSSEC problems for dnssec.bo

.	✓ Found 2 DNSKEY records for . ✓ DS-20326/SHA-256 verifies DNSKEY-20326/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG-20326 and DNSKEY-20326/SEP verifies the DNSKEY RRset
bo	✗ No DS records found for bo in the . zone ✗ No DNSKEY records found
dnssec.bo	✗ No DS records found for dnssec.bo in the bo zone ✓ Found 2 DNSKEY records for dnssec.bo ✓ Found 2 RRSIGs over DNSKEY RRset ✓ RRSIG-6657 and DNSKEY-6657 verifies the DNSKEY RRset ✓ Found 1 RRSIGs over NSEC RRset ✓ RRSIG-6657 and DNSKEY-6657 verifies the NSEC RRset ✓ NSEC proves no records of type A exist for dnssec.bo ✓ Found 1 RRSIGs over SOA RRset ✓ RRSIG-6657 and DNSKEY-6657 verifies the SOA RRset

Move your mouse over any ✗ or ⚠ symbols for remediation hints.



Domain Name: adsib.dnssec.bo

Analyzing DNSSEC problems for adsib.dnssec.bo

.	✓ Found 2 DNSKEY records for . ✓ DS-20326/SHA-256 verifies DNSKEY-20326/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG-20326 and DNSKEY-20326/SEP verifies the DNSKEY RRset
bo	✗ No DS records found for bo in the . zone ✗ No DNSKEY records found
dnssec.bo	✗ No DS records found for dnssec.bo in the bo zone ✓ Found 2 DNSKEY records for dnssec.bo ✓ Found 2 RRSIGs over DNSKEY RRset ✓ RRSIG-6657 and DNSKEY-6657 verifies the DNSKEY RRset
adsib.dnssec.bo	✓ Found 2 DS records for adsib.dnssec.bo in the dnssec.bo zone ✓ DS-15543/SHA-1 has algorithm RSASHA256 ✓ DS-15543/SHA-256 has algorithm RSASHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG-6657 and DNSKEY-6657 verifies the DS RRset ✓ Found 4 DNSKEY records for adsib.dnssec.bo ✓ DS-15543/SHA-1 verifies DNSKEY-15543 ✓ Found 4 RRSIGs over DNSKEY RRset ✓ RRSIG-7921 and DNSKEY-7921/SEP verifies the DNSKEY RRset ✓ Found 2 RRSIGs over NSEC RRset ✓ RRSIG-20751 and DNSKEY-20751 verifies the NSEC RRset ✓ NSEC proves no records of type A exist for adsib.dnssec.bo ✓ Found 2 RRSIGs over SOA RRset ✓ RRSIG-20751 and DNSKEY-20751 verifies the SOA RRset

Move your mouse over any ✗ or ⚠ symbols for remediation hints.

Gracias

Jannett Ibañez Flores

mibanez@adsib.gob.bo
@IbaezJannett

Internet Governance Forum

IoT Global Good Practice

www.iot-dynamic-coalition.org

GFCE Triple-I @LACIGF2019, La Paz, Bolivia, 5 August 2019

Building Global Trust in the Internet of Things

THE IGF DYNAMIC COALITION ON IOT BRINGS TOGETHER STAKEHOLDERS FROM ALL OVER THE WORLD TO ENGAGE IN A DIALOGUE ON "GOOD PRACTICE" IN IOT, WITH THE INTENT TO FIND A REALISTIC AND ETHICAL WAY FORWARD

Benefits … and challenges

- New technologies bring us ways to respond to todays' challenges that never existed before … and come with new challenges
- Technologies are not good or bad in themselves – it is how we use them.

Societal challenges

Healthcare; Independent living; Secure society; Sustainable society

Economic challenges

Innovation; growth; profit

Environmental challenges

Scarce resources; waste reduction; environmental monitoring

Governance

Global standards, open standards, multistakeholder involvement, ethical IoT

Privacy and data collection

Big data issues, cloud issues (location, jurisdiction, accountability), digital literacy

Security

Access,Autonomous systems, cyber attacks on new end points

Source: GNKS 2014

www.iot-dynamic-coalition.org/

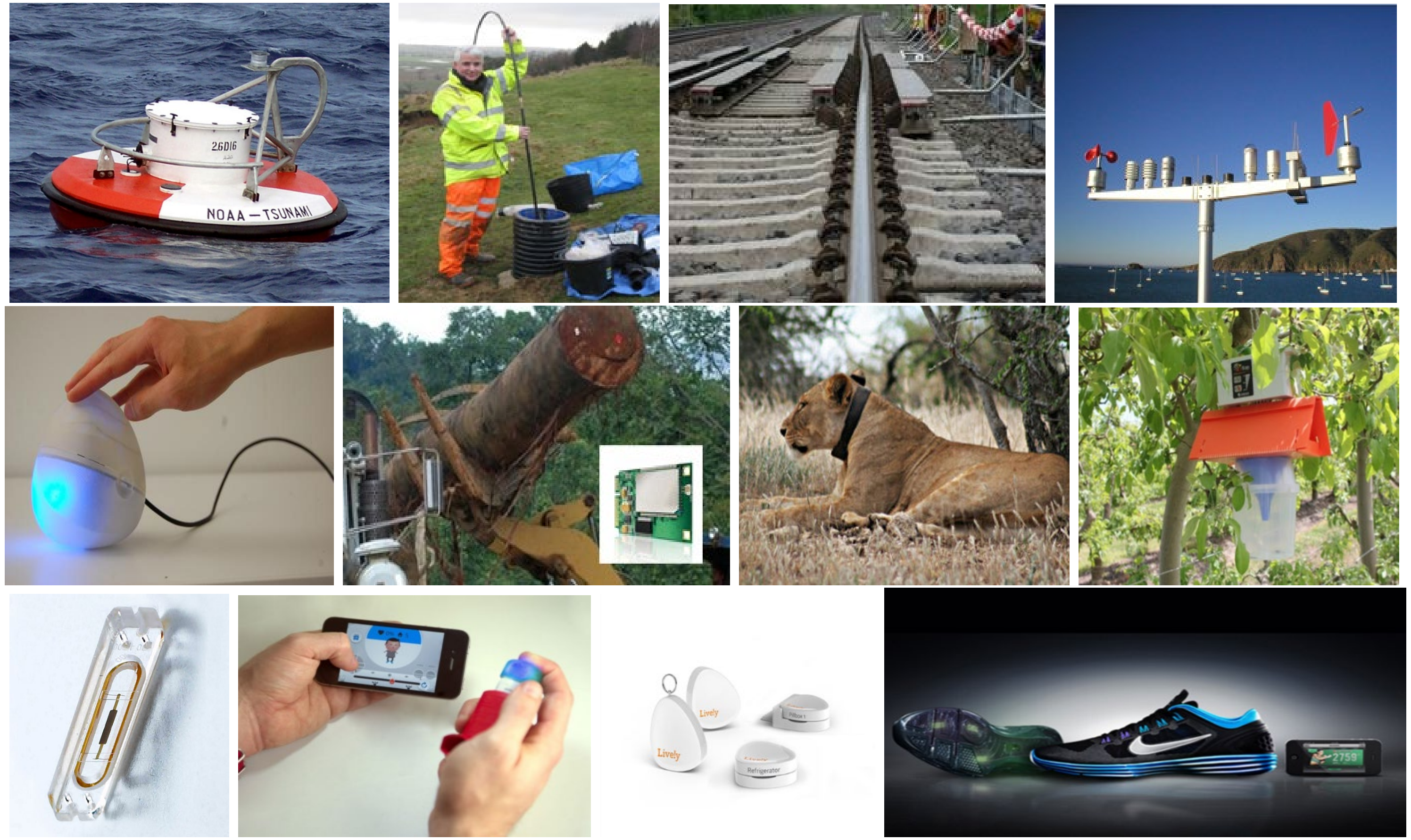
Address specific societal issues

- Connected technologies are a necessity to addressing multiple societal challenges in a doable way.
- It requires sharing global knowledge about solutions, and local knowledge and action to make things happen.

1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS
INTERNET OF THINGS AND THE SUSTAINABLE DEVELOPMENT GOALS

Many applications…

- Ranging from:
  - industrial IoT to Consumer IoT;
  - connected emergency warning systems to traffic management systems;
  - Health monitoring and enhancing systems to agriculture applications;
  - Wildlife tracking to security enhacing;
  - Autonomous systems to tools that enhance our human abilities;
  - and much more ….



Internet of Things **Good Practice Principle**

- *Internet of Things Good Practice aims at developing IoT systems, products, and services* ***taking ethical considerations into account from the outset****, both in the development, deployment and use phases of the life cycle,* ***thus to find an ethical, sustainable way ahead*** *using IoT to help to* ***create a free, secure and enabling rights-based*** *environment: a future we want.*

(IGF Dynamic Coalition on IoT: "IoT Good Practice policies")

IGF DC IoT thinking in summary

Embrace IoT to address societal challenges in an ethical way

- We need IoT to keep this world manageable

Create an IoT environment that encourages investments

- Involve all stakeholders
- Create ecosystem
- Stimulate awareness and feedback
- Provide legal clarity and review the legal mechanisms

Ensure emergence of a trusted IoT environment

- Meaningful transparency
- Clear accountability
- Real choice

Examples from other countries

- Canada
- Netherlands
- United Kingdom

CANADIAN MULTISTAKEHOLDER PROCESS

ENHANCING IOT SECURITY

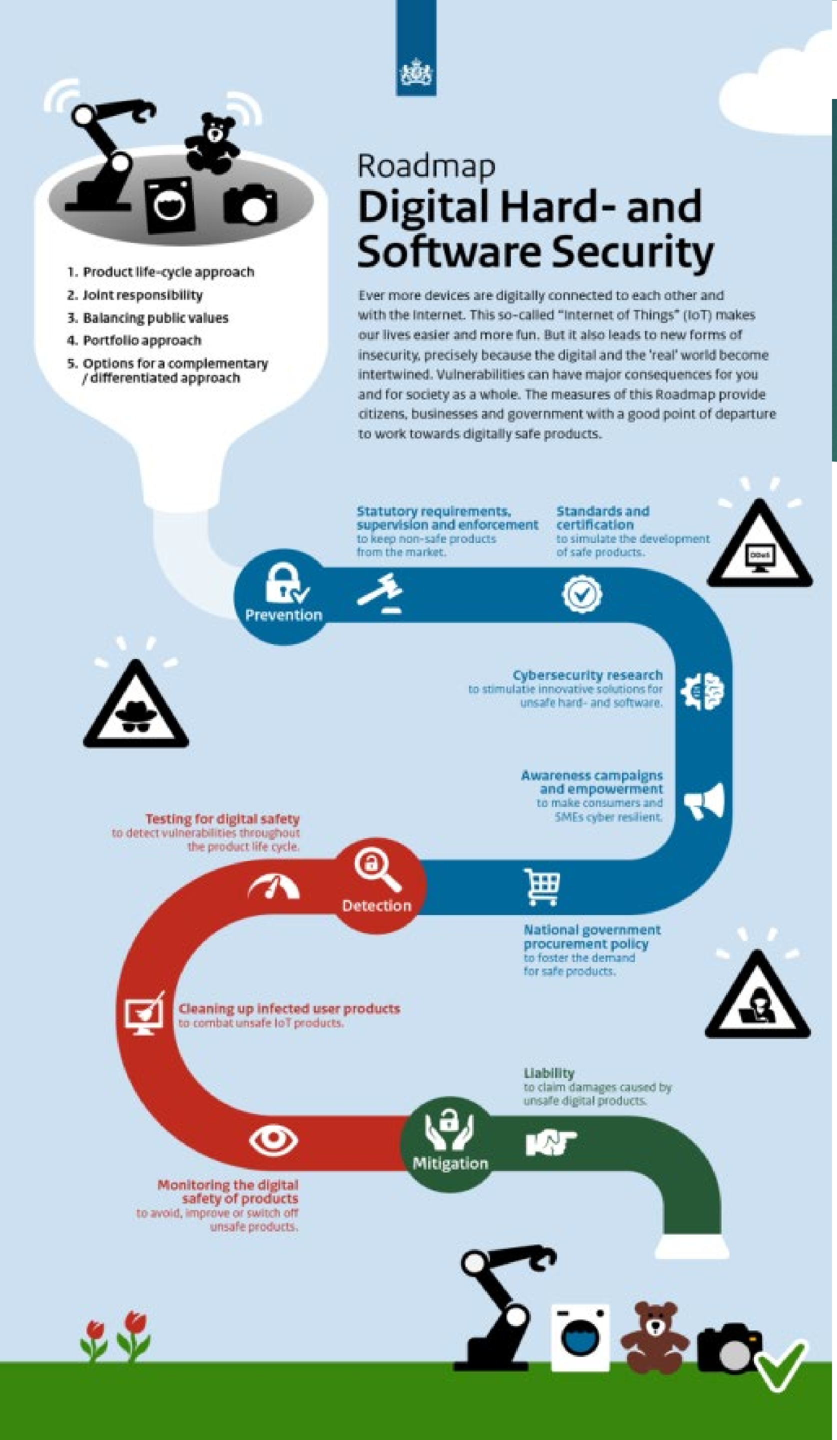
The Canadian approach

- All stakeholders bear a responsibility and opportunity for the safety and resiliency of the Internet.
- We need urgent and collective action now if we are to make an increasingly-connected world a safe place for users and society-at-large.
- No single stakeholder can solve this alone, and users need to be at the center of solutions. An inclusive and collaborative approach is needed for long-lasting, efficient and flexible solutions.
- The complexity of IoT security necessitates such a bottom-up, organic process to ensure the outcomes address all existing and potential challenges and issues.
- Informed by global experiences.

Initiative focus

- The following three thematic areas have been identified and working groups created for each:

1. **Consumer Education:** the aim of this working group is to establish an education and awareness framework to create a more security-conscious public.
2. **Labelling:** the goal of this group is to scope out possible labelling regimes that could be applied and/or enhanced in the Canadian landscape.
3. **Network Resiliency:** the purpose of this group is to develop a set of recommendations to protect the Internet from things and protect things from the Internet. Thus far, this has coalesced in the form of a secure home gateway which leverages Manufacturers Use Description (MUD).



Roadmap

Digital Hard- and Software Security

1. Product life-cycle approach
2. Joint responsibility
3. Balancing public values
4. Portfolio approach
5. Options for a complementary / differentiated approach

Ever more devices are digitally connected to each other and with the Internet. This so-called "Internet of Things" (IoT) makes our lives easier and more fun. But it also leads to new forms of insecurity, precisely because the digital and the 'real' world become intertwined. Vulnerabilities can have major consequences for you and for society as a whole. The measures of this Roadmap provide citizens, businesses and government with a good point of departure to work towards digitally safe products.

Prevention

Statutory requirements, supervision and enforcement to keep non-safe products from the market.

Standards and certification to simulate the development of safe products.

Cybersecurity research to stimulatie innovative solutions for unsafe hard- and software.

Awareness campaigns and empowerment to make consumers and SMEs cyber resilient.

National government procurement policy to foster the demand for safe products.

Detection

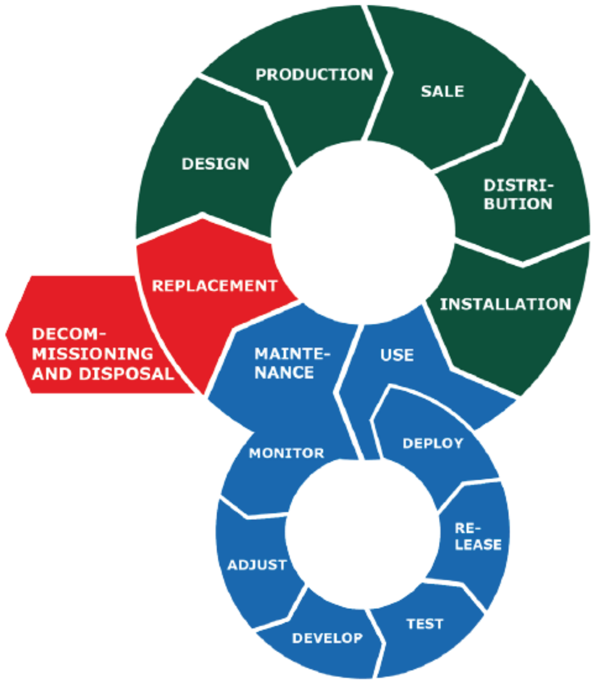
Testing for digital safety to detect vulnerabilities throughout the product life cycle.

Cleaning up infected user products to combat unsafe IoT products.

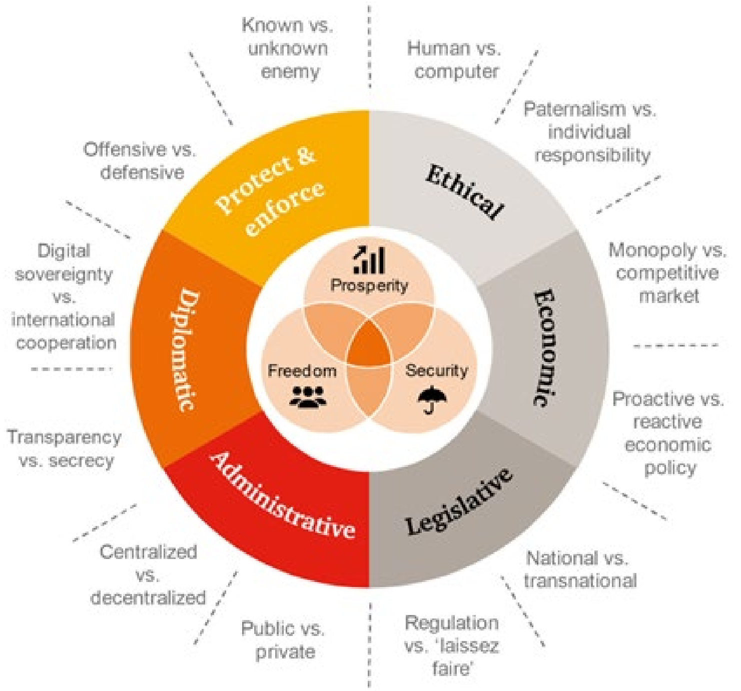
Monitoring the digital safety of products to avoid, improve or switch off unsafe products.

Mitigation

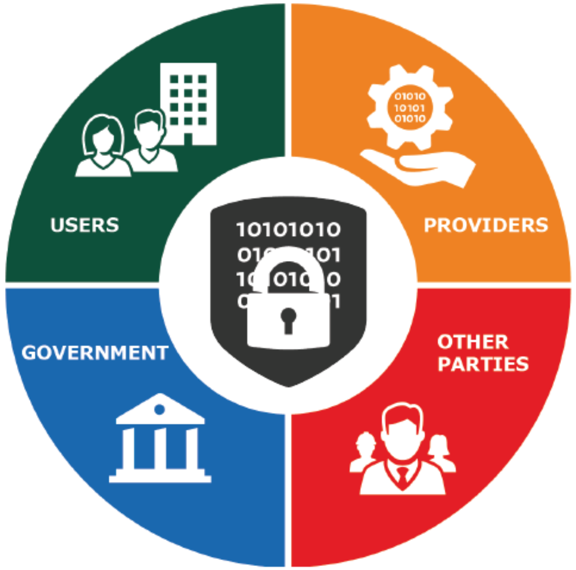
Liability to claim damages caused by unsafe digital products.



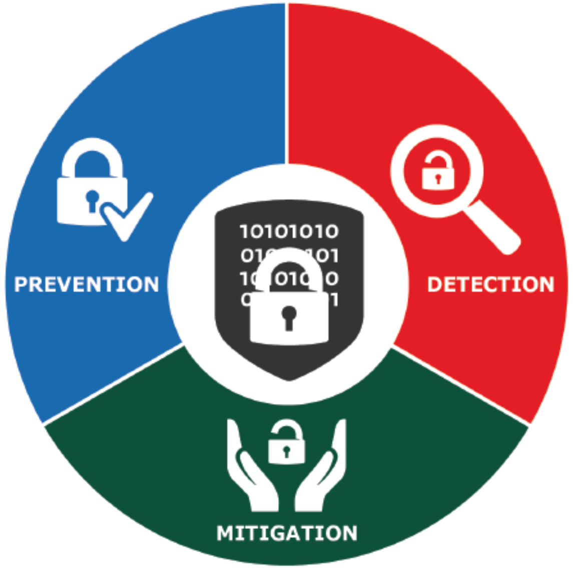
Product life cycle approach


Protect & enforce
Ethical
Economic
Legislative
Administrative
Diplomatic
Prosperity
Freedom
Security
Known vs. unknown enemy
Human vs. computer
Paternalism vs. individual responsibility
Monopoly vs. competitive market
Proactive vs. reactive economic policy
National vs. transnational
Regulation vs. 'laissez faire'
Public vs. private
Centralized vs. decentralized
Transparency vs. secrecy
Digital sovereignty vs. international cooperation
Offensive vs. defensive

Balancing public interest



Joint responsibility



Portfolio approach

Dutch Roadmap Digital Hardware and Software Security:
a complementary approach

Standards and certification

Monitoring digital security

Cleaning up infected products

Testing digital security

Cybersecurity research

Liability

Statutory requirements, supervision and enforcement

Awareness campaigns and empowerment

National goverment procurement policy

UK Government approach

2017 -2018: Cooperation with industry, academia, consumer associations and international partners

March 2018: Policy report

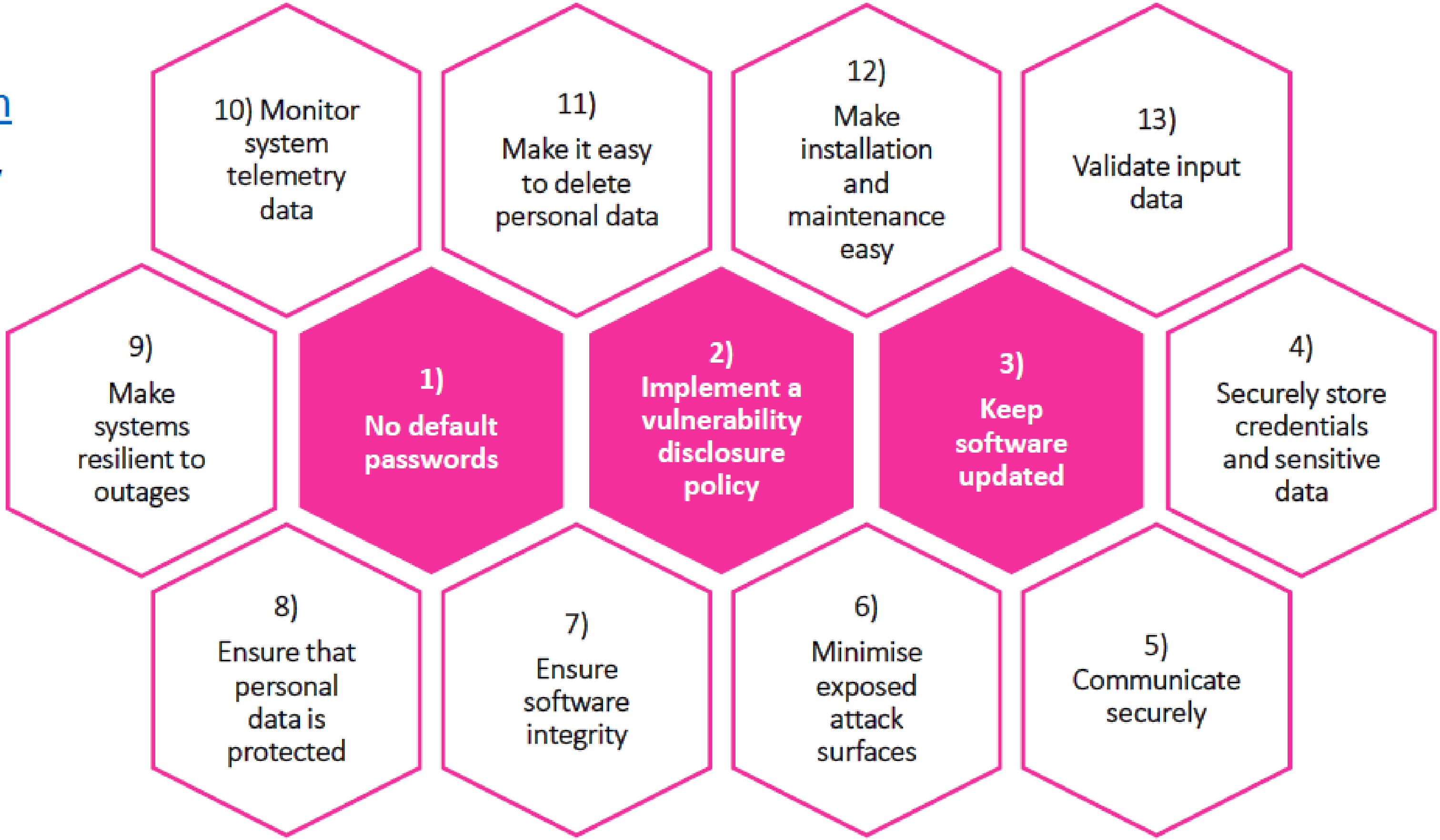
October 2018: Code of Practice for Consumer IoT Security

Mapping of the Code to existing recommendations https://iotsecuritymapping.uk

Consumer guidance https://www.gov.uk/government/publications/secure-by-design

Code of Practice for Consumer IoT Security

- Published in October 2018 in 8 languages: gov.uk/government/publications/secure-by-design
- To help manufacturers protect consumers' privacy and online security.
- Brings together what is widely considered good practice in 13 high-level guidelines.
- Focuses on what matters most.
- Mapped against existing standards and recommendations from 50+ organisations: iotsecuritymapping.uk.



1) No default passwords

2) Implement a vulnerability disclosure policy

3) Keep software updated

4) Securely store credentials and sensitive data

5) Communicate securely

6) Minimise exposed attack surfaces

7) Ensure software integrity

8) Ensure that personal data is protected

9) Make systems resilient to outages

10) Monitor system telemetry data

11) Make it easy to delete personal data

12) Make installation and maintenance easy

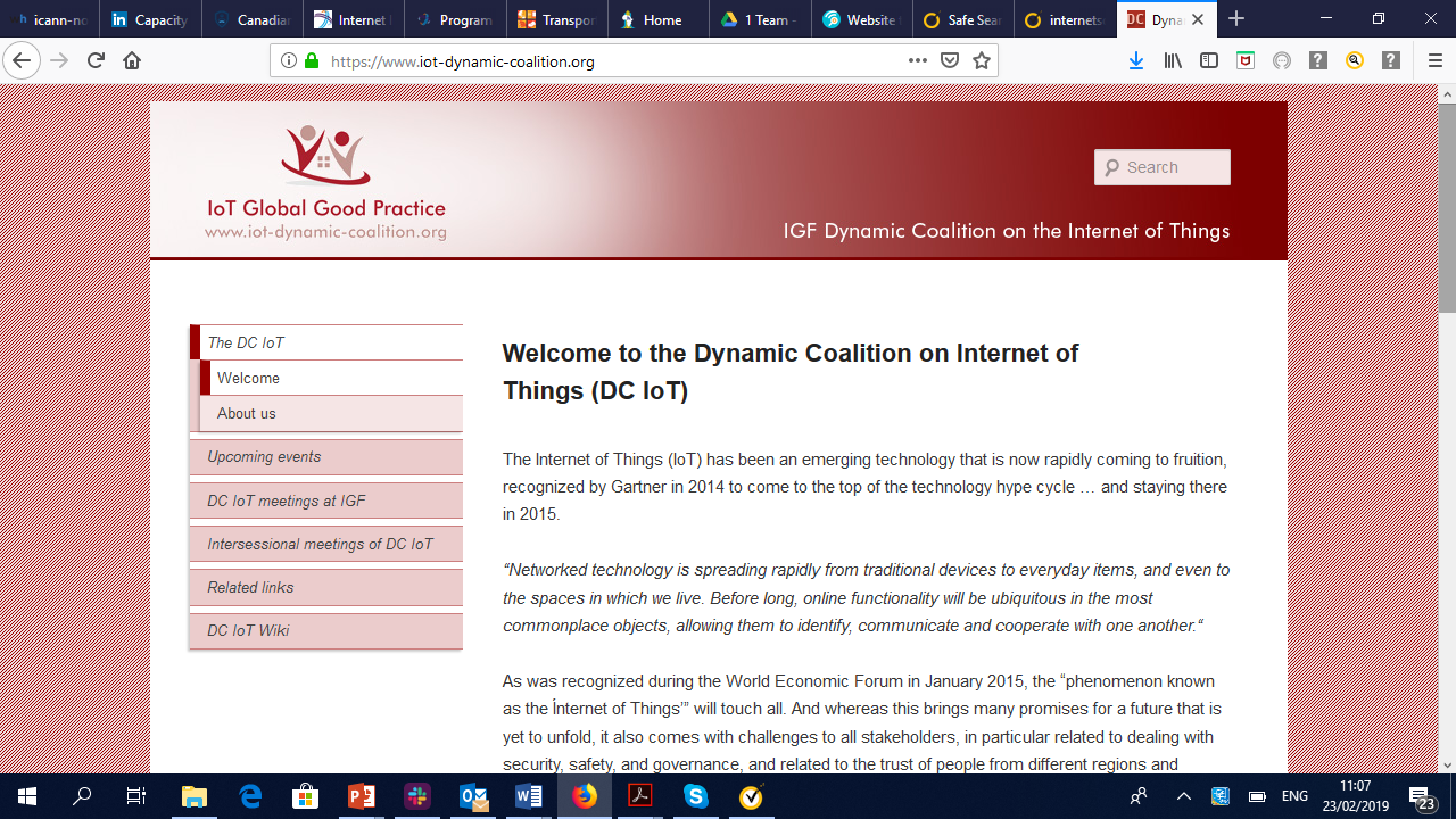
13) Validate input data

Considerations

- What can we learn from the Canadian approach
  - Use a multistakeholder approach to kick off a flywheel of action
    - Action both in technical community; government units; consumer organisations; kick-off joint position
- What can we learn from the Dutch approach?
  - Complementary measures:
    - Liability (stick behind the door); Government procurement (backing up development of standards); Reviewing legislation (statutory requirements supervision and enforcement); Cleaning up infected products (joint LEA – industry action?)
- What can we learn from the British approach?
  - Working towards a Code of Practice for industry?
    - Adopting the British one – or at least use it for discussion with industry and other stakeholders
- ***Keep an eye on global developments! To learn, and to tack on as IoT goes across borders, as well***

Global Action

IN SUPPORT OF LOCAL ACTION

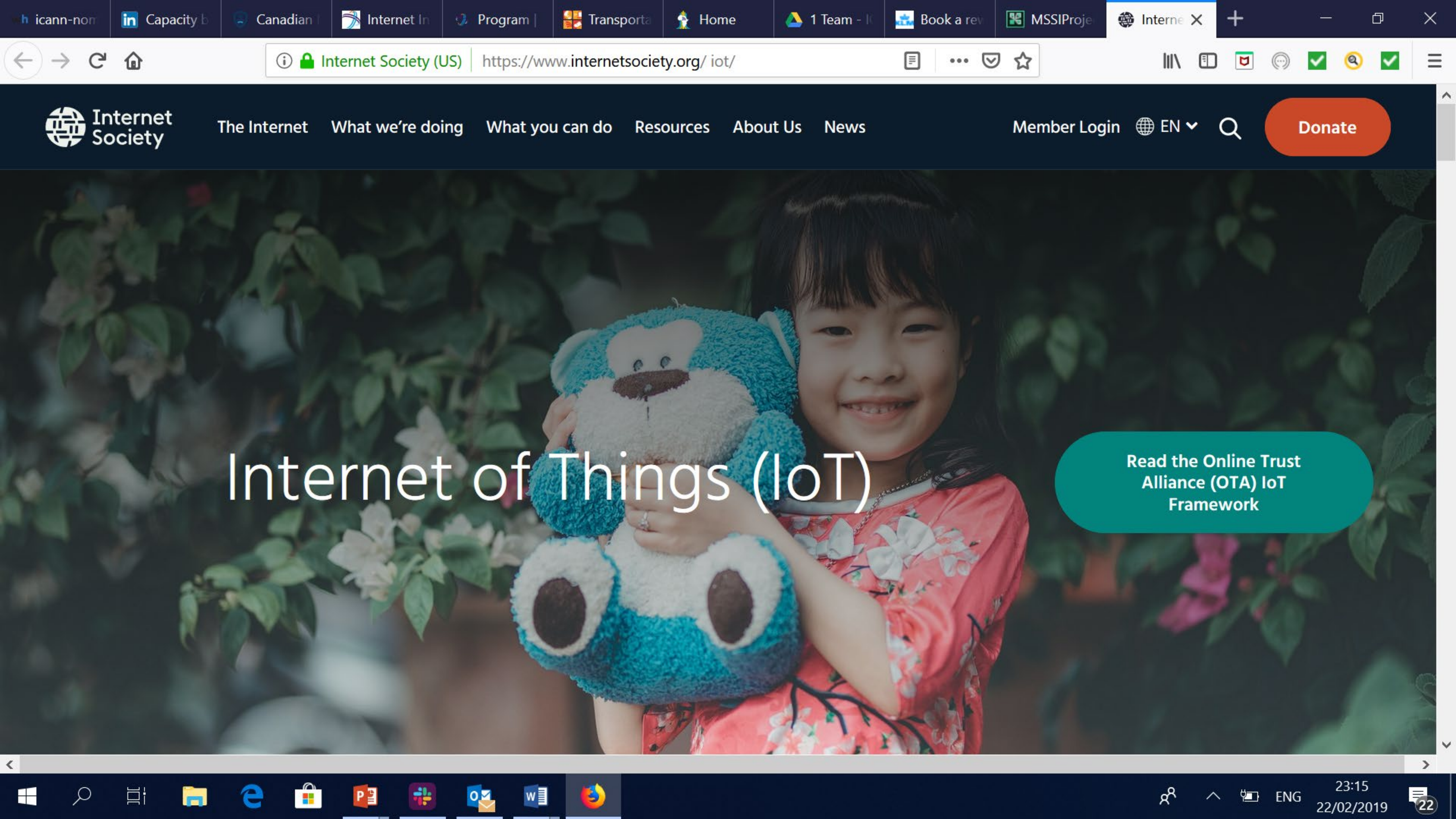


Welcome to the Dynamic Coalition on Internet of Things (DC IoT)

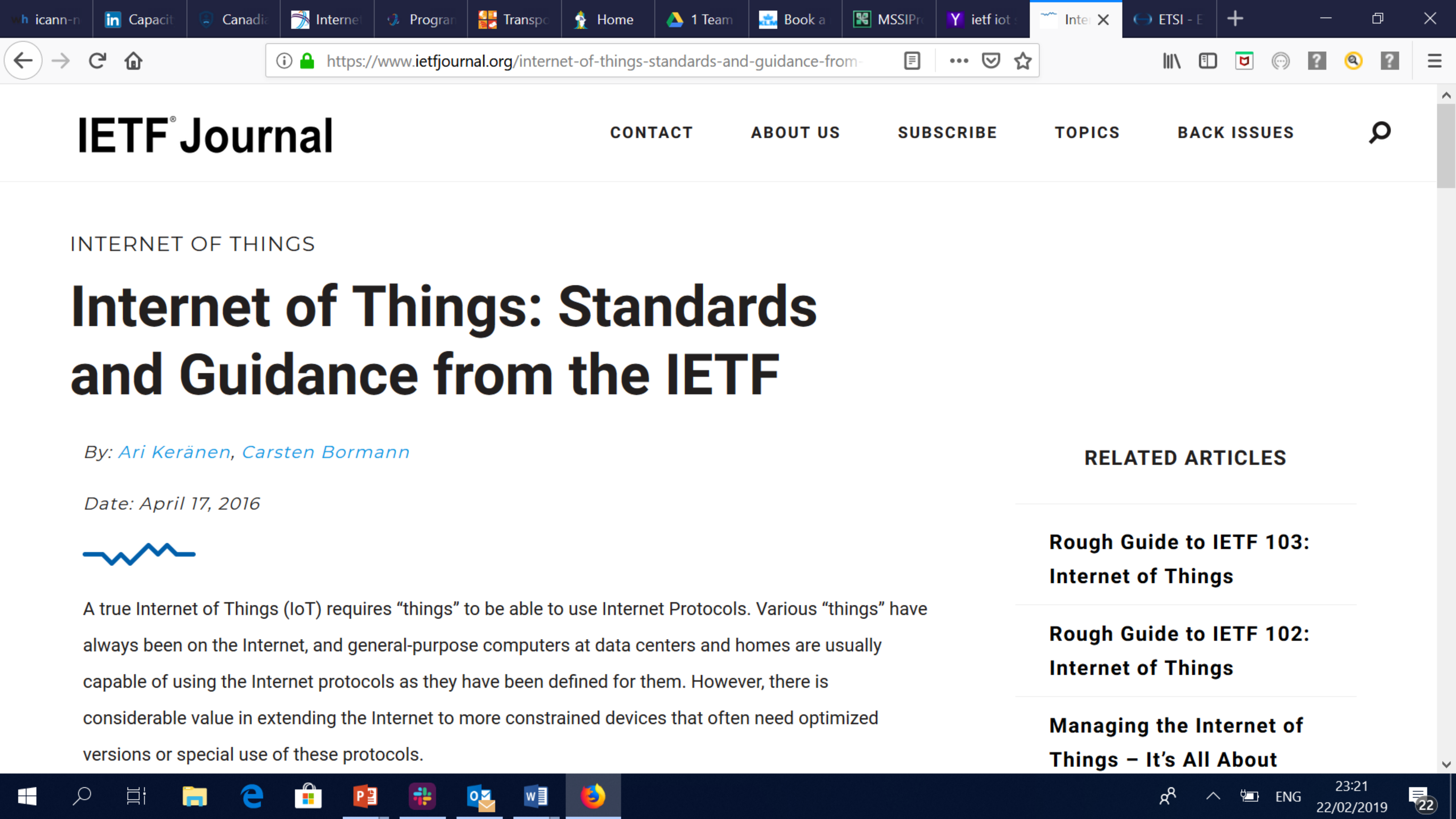
The Internet of Things (IoT) has been an emerging technology that is now rapidly coming to fruition, recognized by Gartner in 2014 to come to the top of the technology hype cycle … and staying there in 2015.

"Networked technology is spreading rapidly from traditional devices to everyday items, and even to the spaces in which we live. Before long, online functionality will be ubiquitous in the most commonplace objects, allowing them to identify, communicate and cooperate with one another."

As was recognized during the World Economic Forum in January 2015, the "phenomenon known as the Internet of Things'" will touch all. And whereas this brings many promises for a future that is yet to unfold, it also comes with challenges to all stakeholders, in particular related to dealing with security, safety, and governance, and related to the trust of people from different regions and



Internet of Things (IoT)



IETF® Journal

CONTACT ABOUT US SUBSCRIBE TOPICS BACK ISSUES

INTERNET OF THINGS

Internet of Things: Standards and Guidance from the IETF

By: Ari Keränen, Carsten Bormann

Date: April 17, 2016

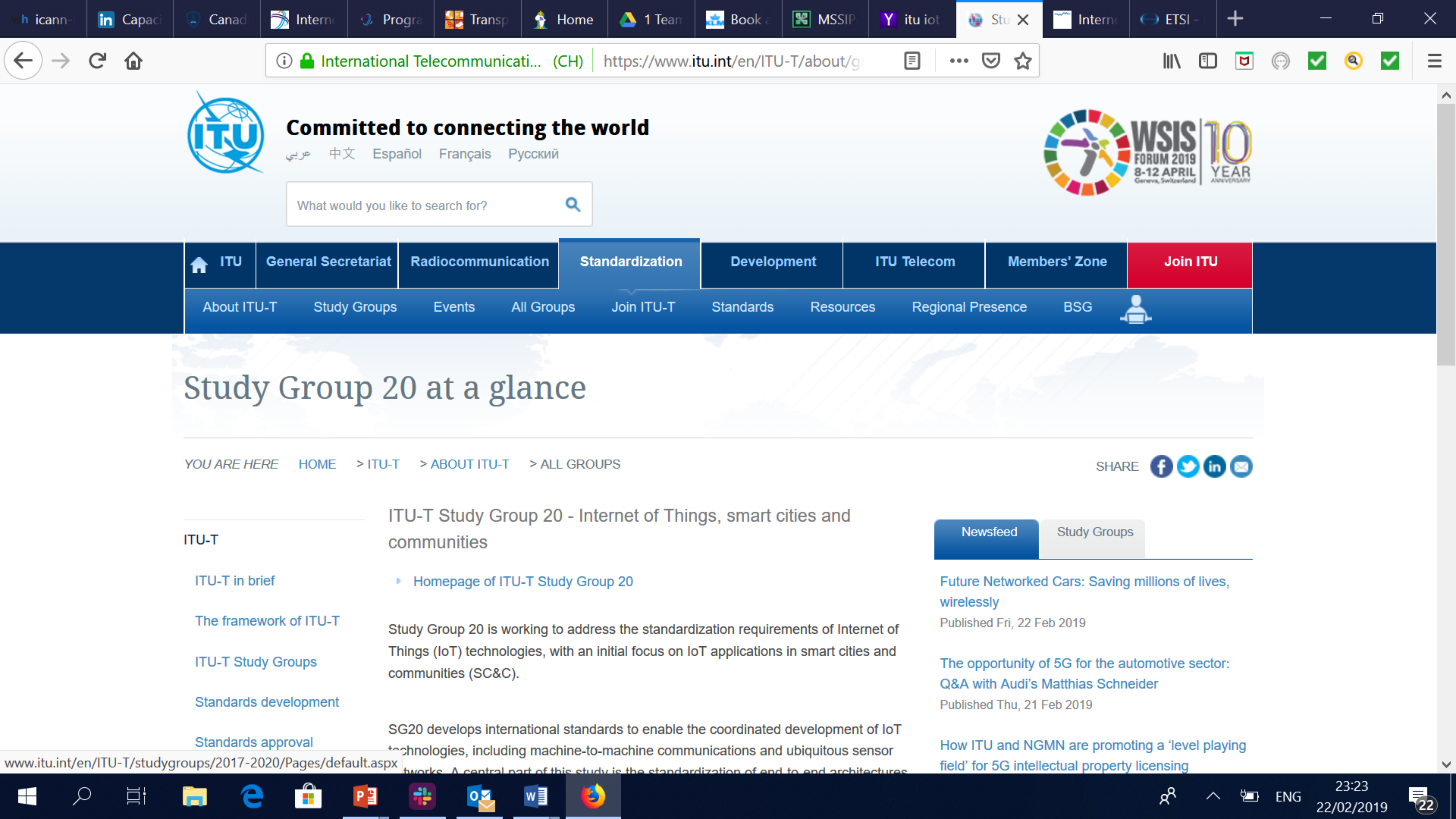
A true Internet of Things (IoT) requires "things" to be able to use Internet Protocols. Various "things" have always been on the Internet, and general-purpose computers at data centers and homes are usually capable of using the Internet protocols as they have been defined for them. However, there is considerable value in extending the Internet to more constrained devices that often need optimized versions or special use of these protocols.

RELATED ARTICLES

Rough Guide to IETF 103: Internet of Things

Rough Guide to IETF 102: Internet of Things

Managing the Internet of Things – It's All About



Study Group 20 at a glance

YOU ARE HERE HOME > ITU-T > ABOUT ITU-T > ALL GROUPS

ITU-T

- ITU-T in brief
- The framework of ITU-T
- ITU-T Study Groups
- Standards development
- Standards approval

ITU-T Study Group 20 - Internet of Things, smart cities and communities

- Homepage of ITU-T Study Group 20

Study Group 20 is working to address the standardization requirements of Internet of Things (IoT) technologies, with an initial focus on IoT applications in smart cities and communities (SC&C).

SG20 develops international standards to enable the coordinated development of IoT technologies, including machine-to-machine communications and ubiquitous sensor networks. A central part of this study is the standardization of end-to-end architectures

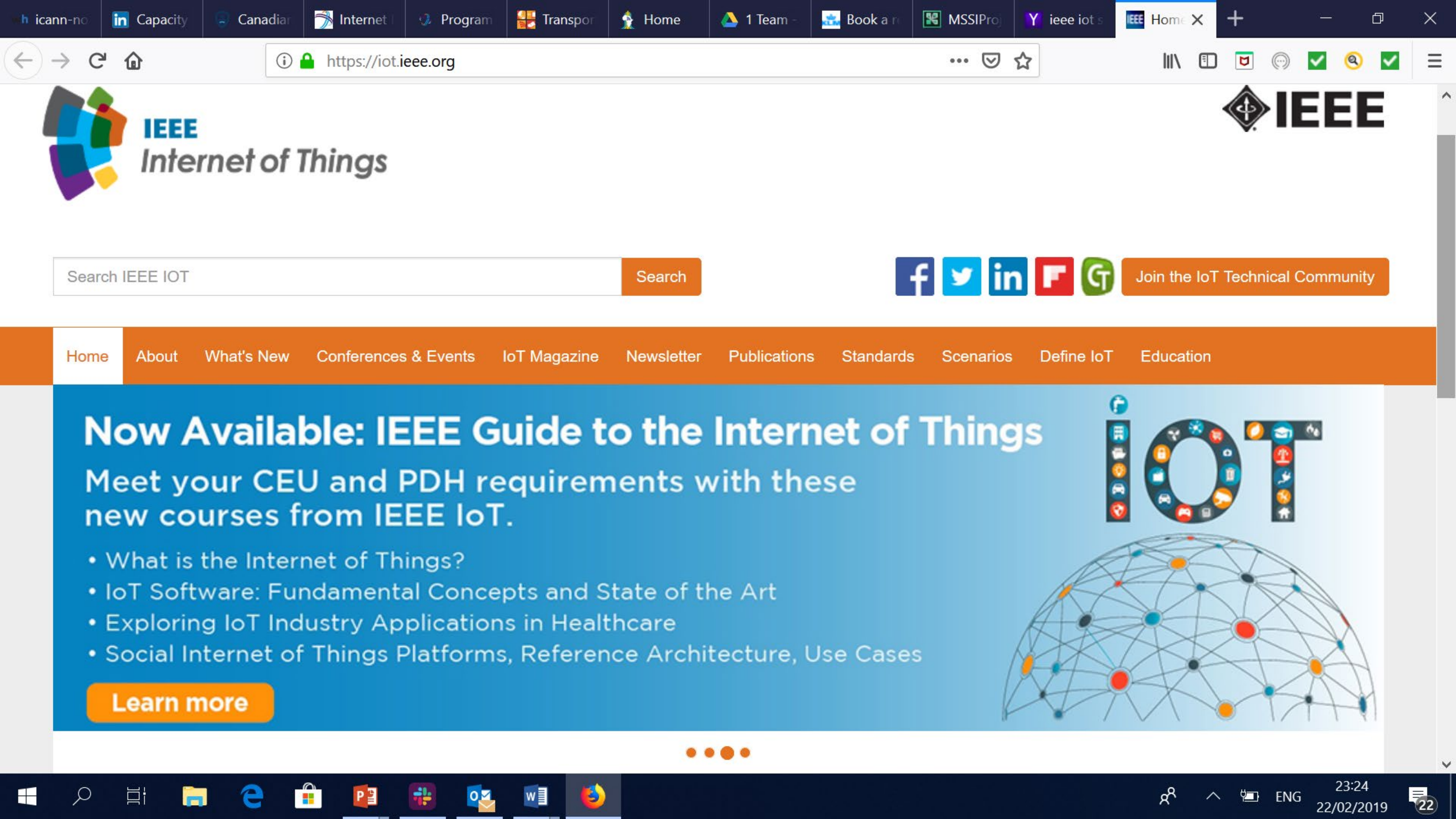
Newsfeed | Study Groups

Future Networked Cars: Saving millions of lives, wirelessly
Published Fri, 22 Feb 2019

The opportunity of 5G for the automotive sector: Q&A with Audi's Matthias Schneider
Published Thu, 21 Feb 2019

How ITU and NGMN are promoting a 'level playing field' for 5G intellectual property licensing

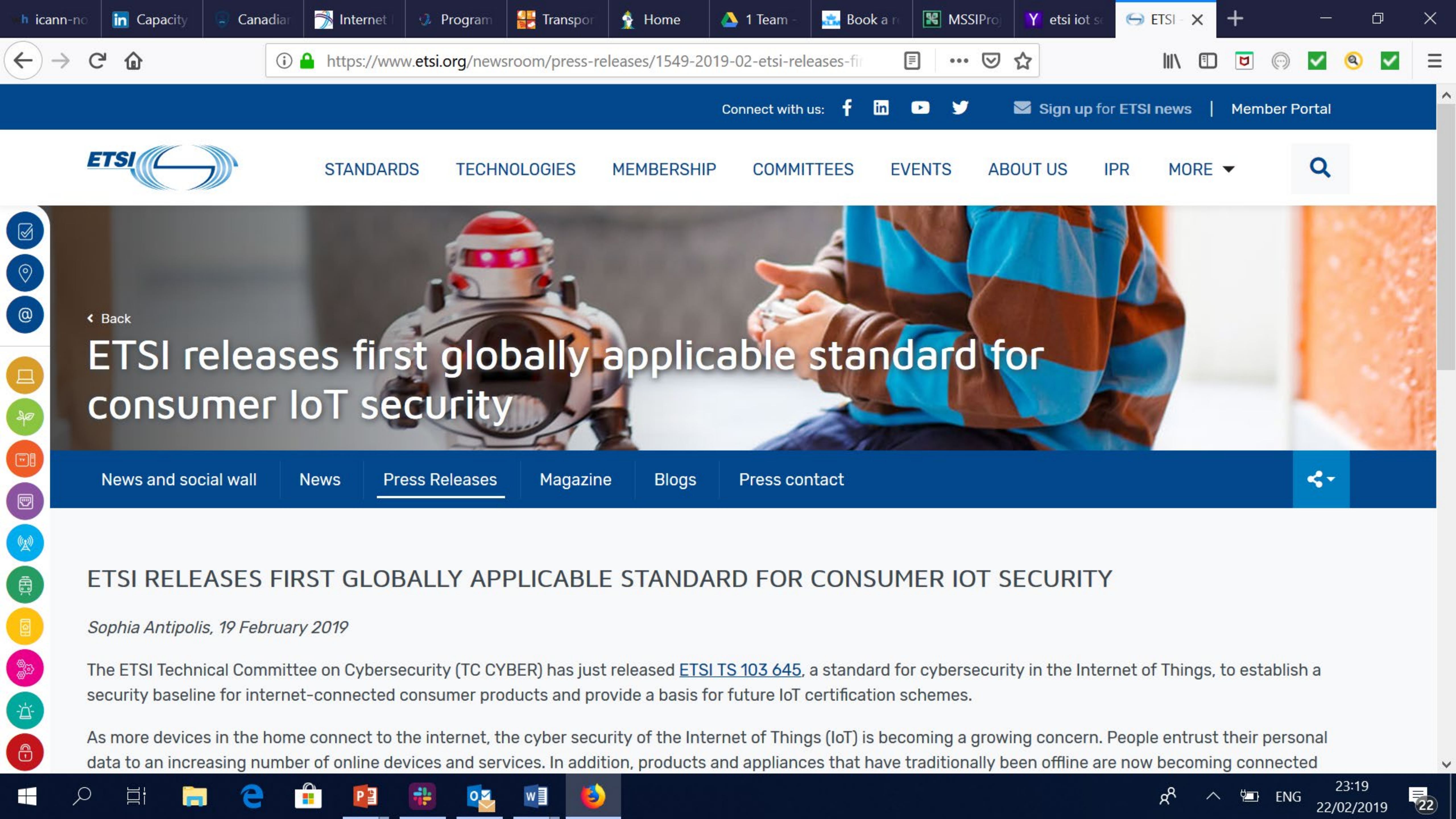
www.itu.int/en/ITU-T/studygroups/2017-2020/Pages/default.aspx



Now Available: IEEE Guide to the Internet of Things

Meet your CEU and PDH requirements with these new courses from IEEE IoT.

- What is the Internet of Things?
- IoT Software: Fundamental Concepts and State of the Art
- Exploring IoT Industry Applications in Healthcare
- Social Internet of Things Platforms, Reference Architecture, Use Cases



ETSI RELEASES FIRST GLOBALLY APPLICABLE STANDARD FOR CONSUMER IOT SECURITY

Sophia Antipolis, 19 February 2019

The ETSI Technical Committee on Cybersecurity (TC CYBER) has just released ETSI TS 103 645, a standard for cybersecurity in the Internet of Things, to establish a security baseline for internet-connected consumer products and provide a basis for future IoT certification schemes.

As more devices in the home connect to the internet, the cyber security of the Internet of Things (IoT) is becoming a growing concern. People entrust their personal data to an increasing number of online devices and services. In addition, products and appliances that have traditionally been offline are now becoming connected

We create the world of tomorrow with the choices and actions of today ...

More information

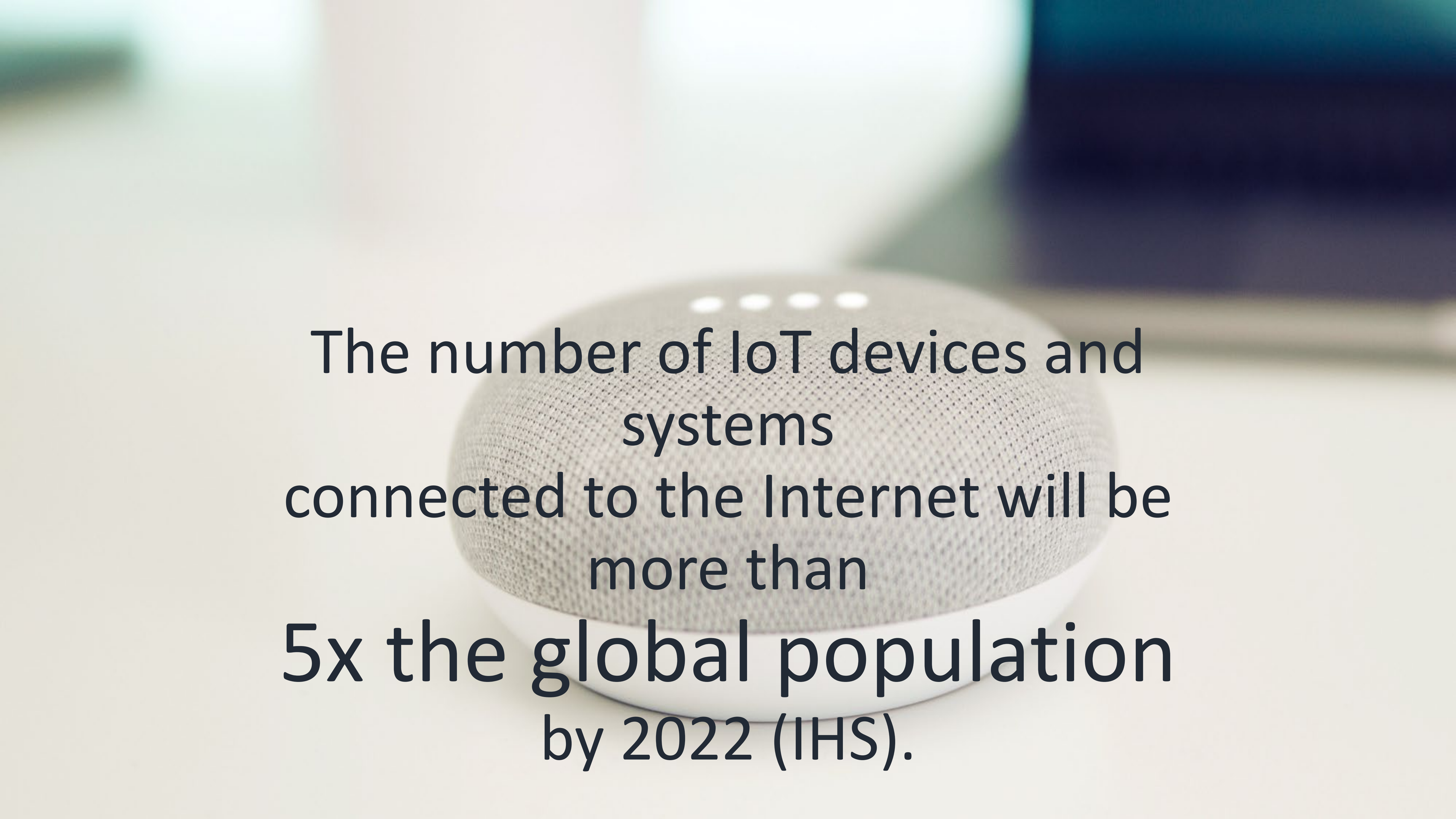
- Internet Society activities:
- http://www.internetsociety.org
- IGF DC IoT activities:
- http://www.iot-dynamic-coalition.org/
- IEEE new standard for IoT Security
- IETF work on MUD

IoT Global Good Practice

www.iot-dynamic-coalition.org

Internet of Things:
Trust Framework for Privacy & Security

Internet Society



The number of IoT devices and systems

connected to the Internet will be more than

5x the global population

by 2022 (IHS).

As more and more devices are connected, privacy and security risks increase.

And most consumers don’t even know it.

Challenges

Manufacturers

Cost/size

Functionality

Time to market

Future-proofing

Services

New uses

Massive volume

Naïve players

Limited insight

Consumers

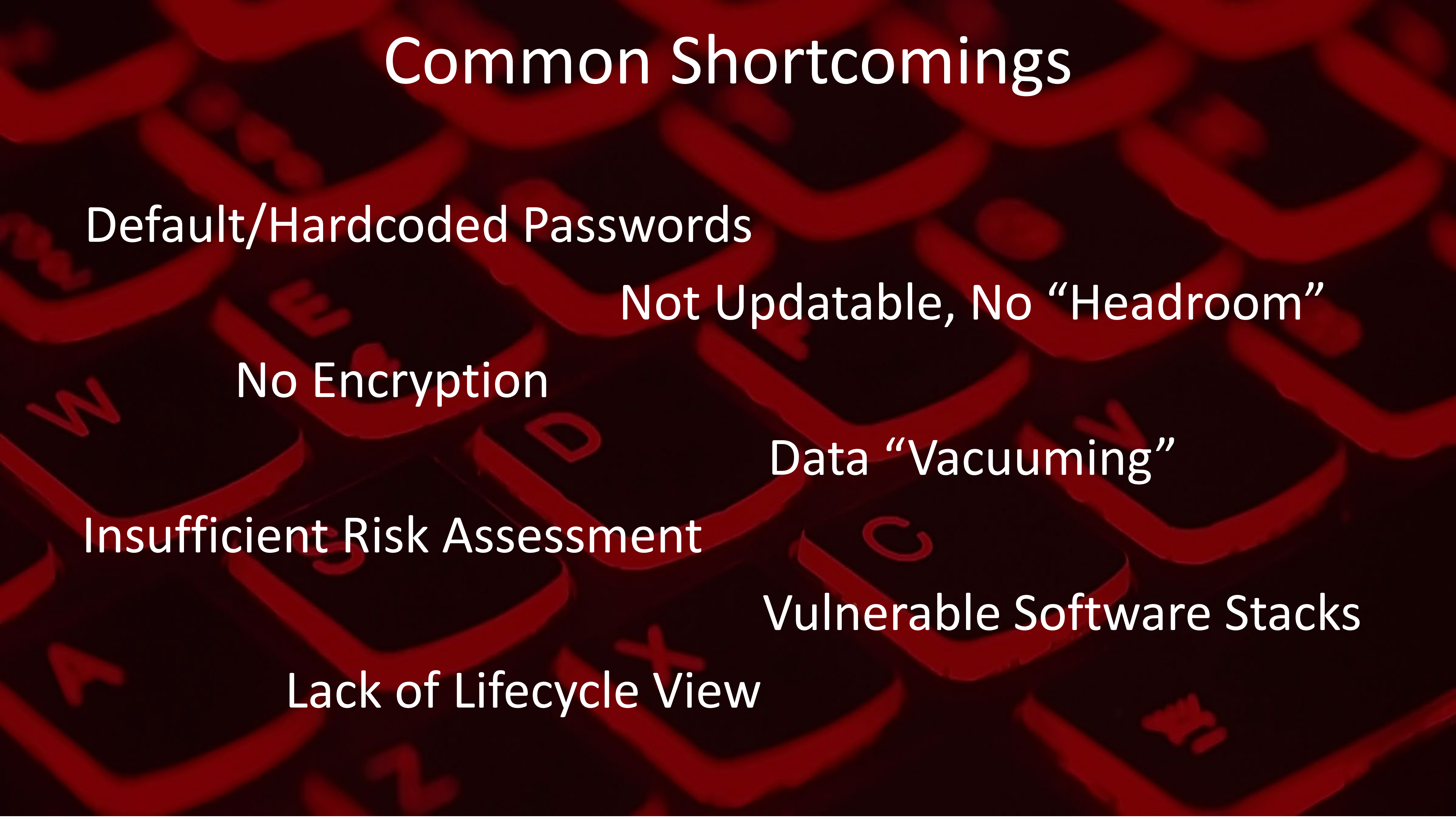
Cost/convenience

Naïve users

DIY approach

Flying blind

Common Shortcomings



Default/Hardcoded Passwords

Not Updatable, No “Headroom”

No Encryption

Data “Vacuuming”

Insufficient Risk Assessment

Vulnerable Software Stacks

Lack of Lifecycle View

IoT Security & Privacy – A Collective Responsibility

IoT vendors and their supply chain

Distribution channels

Policymakers and governments

Consumer testing and product review organizations

Consumers and enterprises

IoT Trust by Design

1

Work with manufacturers and suppliers to adopt and implement the IoT Trust Framework

2

Mobilize consumers to drive demand for security and privacy capabilities as a market differentiator

3

Encourage policy and regulations to push for better security and privacy features in IoT

A Comprehensive IoT Trust Framework

A Comprehensive Framework Should Address All Dimensions

The entire system

Devices & Sensors

Apps and Platforms

Cloud & Web Services

Full range of consumer concerns

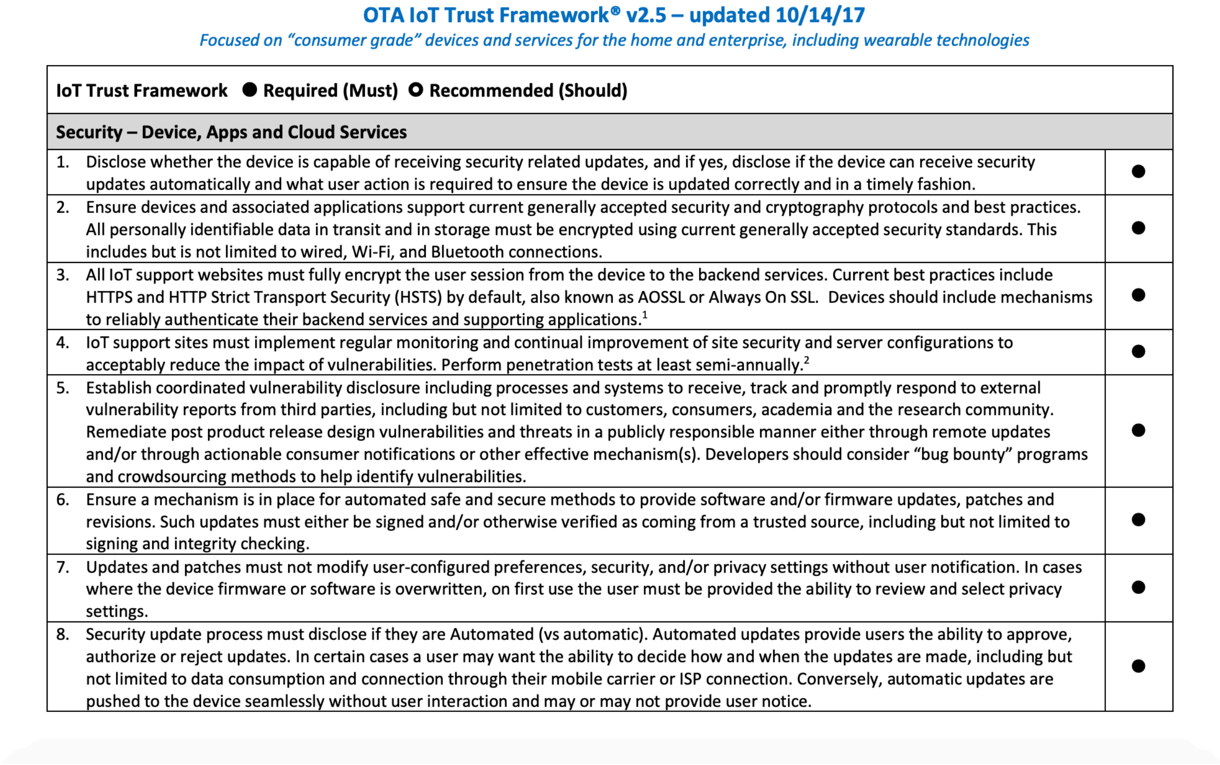
Security

Privacy

Lifecycle

IoT Trust Framework

- The Internet Society's **IoT Trust Framework** includes 40 strategic principles necessary to address IoT security, privacy and lifecycle issues
- Focus:
- Perfection is the enemy of good
- Measurable principles vs. standards development
- Consumer grade devices, (home, office, and wearables)
- Address known vulnerabilities and threats
- Actionable and vendor neutral



OTA IoT Trust Framework® v2.5 – updated 10/14/17

Focused on "consumer grade" devices and services for the home and enterprise, including wearable technologies

IoT Trust Framework ● Required (Must) ○ Recommended (Should)	
Security – Device, Apps and Cloud Services	
1. Disclose whether the device is capable of receiving security related updates, and if yes, disclose if the device can receive security updates automatically and what user action is required to ensure the device is updated correctly and in a timely fashion.	●
2. Ensure devices and associated applications support current generally accepted security and cryptography protocols and best practices. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This includes but is not limited to wired, Wi-Fi, and Bluetooth connections.	●
3. All IoT support websites must fully encrypt the user session from the device to the backend services. Current best practices include HTTPS and HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL. Devices should include mechanisms to reliably authenticate their backend services and supporting applications.[1]	●
4. IoT support sites must implement regular monitoring and continual improvement of site security and server configurations to acceptably reduce the impact of vulnerabilities. Perform penetration tests at least semi-annually.[2]	●
5. Establish coordinated vulnerability disclosure including processes and systems to receive, track and promptly respond to external vulnerability reports from third parties, including but not limited to customers, consumers, academia and the research community. Remediate post product release design vulnerabilities and threats in a publicly responsible manner either through remote updates and/or through actionable consumer notifications or other effective mechanism(s). Developers should consider "bug bounty" programs and crowdsourcing methods to help identify vulnerabilities.	●
6. Ensure a mechanism is in place for automated safe and secure methods to provide software and/or firmware updates, patches and revisions. Such updates must either be signed and/or otherwise verified as coming from a trusted source, including but not limited to signing and integrity checking.	●
7. Updates and patches must not modify user-configured preferences, security, and/or privacy settings without user notification. In cases where the device firmware or software is overwritten, on first use the user must be provided the ability to review and select privacy settings.	●
8. Security update process must disclose if they are Automated (vs automatic). Automated updates provide users the ability to approve, authorize or reject updates. In certain cases a user may want the ability to decide how and when the updates are made, including but not limited to data consumption and connection through their mobile carrier or ISP connection. Conversely, automatic updates are pushed to the device seamlessly without user interaction and may or may not provide user notice.	●

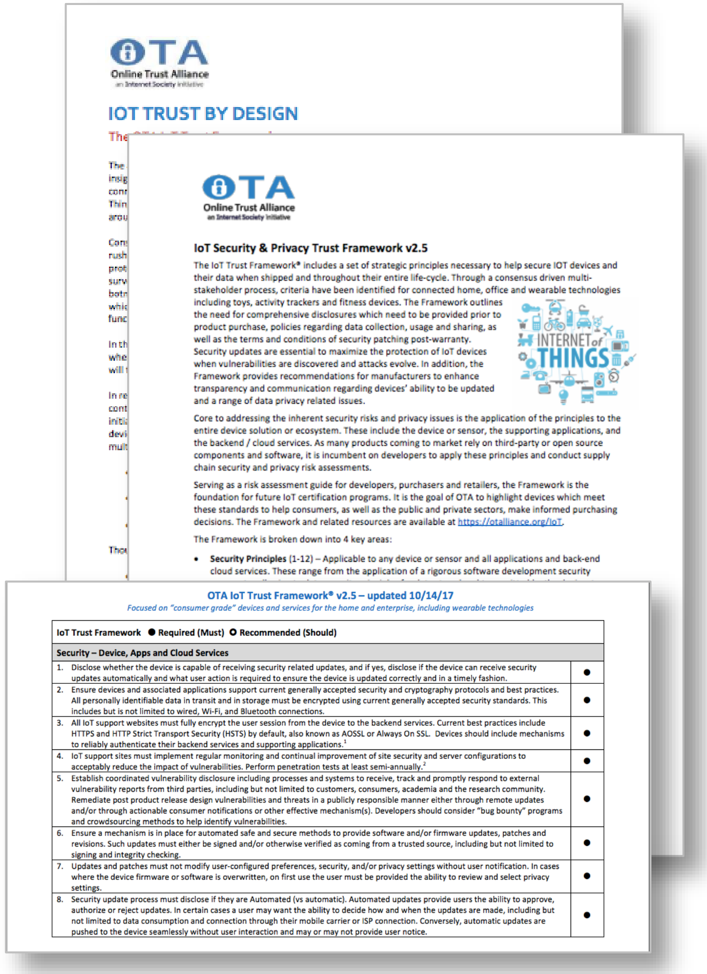
A Framework for Action

The IoT Trust Framework principles address:

Authentication	Encryption	Security	Updates
Privacy	Disclosures	Control	Communications

- Focused on consumer segment (e.g., smart home and wearables)
- Developed with input from more than 100 stakeholders
- Guiding principles (vs. specifications), intended as foundation for trustmark/certification program

Resources to Help



OTA Online Trust Alliance an Internet Society initiative

IOT TRUST BY DESIGN

OTA Online Trust Alliance an Internet Society initiative

IoT Security & Privacy Trust Framework v2.5

The IoT Trust Framework® includes a set of strategic principles necessary to help secure IOT devices and their data when shipped and throughout their entire life-cycle. Through a consensus driven multi-stakeholder process, criteria have been identified for connected home, office and wearable technologies including toys, activity trackers and fitness devices. The Framework outlines the need for comprehensive disclosures which need to be provided prior to product purchase, policies regarding data collection, usage and sharing, as well as the terms and conditions of security patching post-warranty. Security updates are essential to maximize the protection of IoT devices when vulnerabilities are discovered and attacks evolve. In addition, the Framework provides recommendations for manufacturers to enhance transparency and communication regarding devices' ability to be updated and a range of data privacy related issues.

Core to addressing the inherent security risks and privacy issues is the application of the principles to the entire device solution or ecosystem. These include the device or sensor, the supporting applications, and the backend / cloud services. As many products coming to market rely on third-party or open source components and software, it is incumbent on developers to apply these principles and conduct supply chain security and privacy risk assessments.

Serving as a risk assessment guide for developers, purchasers and retailers, the Framework is the foundation for future IoT certification programs. It is the goal of OTA to highlight devices which meet these standards to help consumers, as well as the public and private sectors, make informed purchasing decisions. The Framework and related resources are available at https://otalliance.org/IoT.

The Framework is broken down into 4 key areas:

- **Security Principles** (1-12) – Applicable to any device or sensor and all applications and back-end cloud services. These range from the application of a rigorous software development security

OTA IoT Trust Framework® v2.5 – updated 10/14/17

Focused on "consumer grade" devices and services for the home and enterprise, including wearable technologies

IoT Trust Framework ● Required (Must) ○ Recommended (Should)	
Security – Device, Apps and Cloud Services	
1. Disclose whether the device is capable of receiving security related updates, and if yes, disclose if the device can receive security updates automatically and what user action is required to ensure the device is updated correctly and in a timely fashion.	●
2. Ensure devices and associated applications support current generally accepted security and cryptography protocols and best practices. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This includes but is not limited to wired, Wi-Fi, and Bluetooth connections.	●
3. All IoT support websites must fully encrypt the user session from the device to the backend services. Current best practices include HTTPS and HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL. Devices should include mechanisms to reliably authenticate their backend services and supporting applications.[1]	●
4. IoT support sites must implement regular monitoring and continual improvement of site security and server configurations to acceptably reduce the impact of vulnerabilities. Perform penetration tests at least semi-annually.[2]	●
5. Establish coordinated vulnerability disclosure including processes and systems to receive, track and promptly respond to external vulnerability reports from third parties, including but not limited to customers, consumers, academia and the research community. Remediate post product release design vulnerabilities and threats in a publicly responsible manner either through remote updates and/or through actionable consumer notifications or other effective mechanism(s). Developers should consider "bug bounty" programs and crowdsourcing methods to help identify vulnerabilities.	●
6. Ensure a mechanism is in place for automated safe and secure methods to provide software and/or firmware updates, patches and revisions. Such updates must either be signed and/or otherwise verified as coming from a trusted source, including but not limited to signing and integrity checking.	●
7. Updates and patches must not modify user-configured preferences, security, and/or privacy settings without user notification. In cases where the device firmware or software is overwritten, on first use the user must be provided the ability to review and select privacy settings.	●
8. Security update process must disclose if they are Automated (vs automatic). Automated updates provide users the ability to approve, authorize or reject updates. In certain cases a user may want the ability to decide how and when the updates are made, including but not limited to data consumption and connection through their mobile carrier or ISP connection. Conversely, automatic updates are pushed to the device seamlessly without user interaction and may or may not provide user notice.	●

OTA Online Trust Alliance

Securing the Internet of Things

A Collaborative & Shared Responsibility

Internet of Things

A Vision for the Future

OTA Online Trust Alliance an Internet Society initiative

OTA Online Trust Alliance

SMART HOME CHECKLIST

Maximizing Security, Privacy & Personal Safety

OTA Online Trust Alliance an Internet Society initiative

THE ENTERPRISE IOT SECURITY CHECKLIST

Best Practices for Securing Consumer-Grade IoT in the Enterprise

CONSUMER-GRADE IOT IN THE ENTERPRISE

The Internet of Things (IoT) has found its way into all aspects of our lives. In particular, "consumer-grade" IoT devices such as smart TVs, thermostats, smart speakers, fitness trackers and other devices are now used regularly in enterprises, either purchased by staff or brought in by employees.

This IoT insurgence represents a unique challenge since many of these devices are deployed without IT's knowledge or not accounted for as a normal part of IT security planning, yet they have characteristics that can create serious vulnerabilities. While some IoT products are designed with strong security, many have a simple or non-existent user interface, default (or hardcoded) passwords, open hardware and software ports, limited local password protection, lack the ability to be updated, "phone home" frequently, collect more data than expected and use insecure backend services.

CONNECTSMART!

CONSUMERS INTERNATIONAL

Internet Society

Take action today by understanding how to better protect yourself and your family

Check out our tips on how to connect smart!

Internet Society

Top tips for Internet of Things security and privacy.

1. **Learn how to "shop smart" for connected devices.** You don't want to have to return a connected device because it is spying on you. Returning things is a pain. Learn how to "shop smart," and buy privacy respecting connected devices so you won't have to.

19 April 2018

IoT Security for Policymakers

"Cybersecurity will be the most pressing challenge of the next decade, and IoT will play a critical role in it."

Internet Society 2017 Global Internet Report

Internet Society

https://www.internetsociety.org/iot/

What we’re doing about it

Encouraging the use of multistakeholder processes to solve complex security issues

National Multistakeholder Processes

Working with all stakeholders in country, to produce local recommendations on IoT security. Two main avenues:

- Consumer protection
- Network resiliency

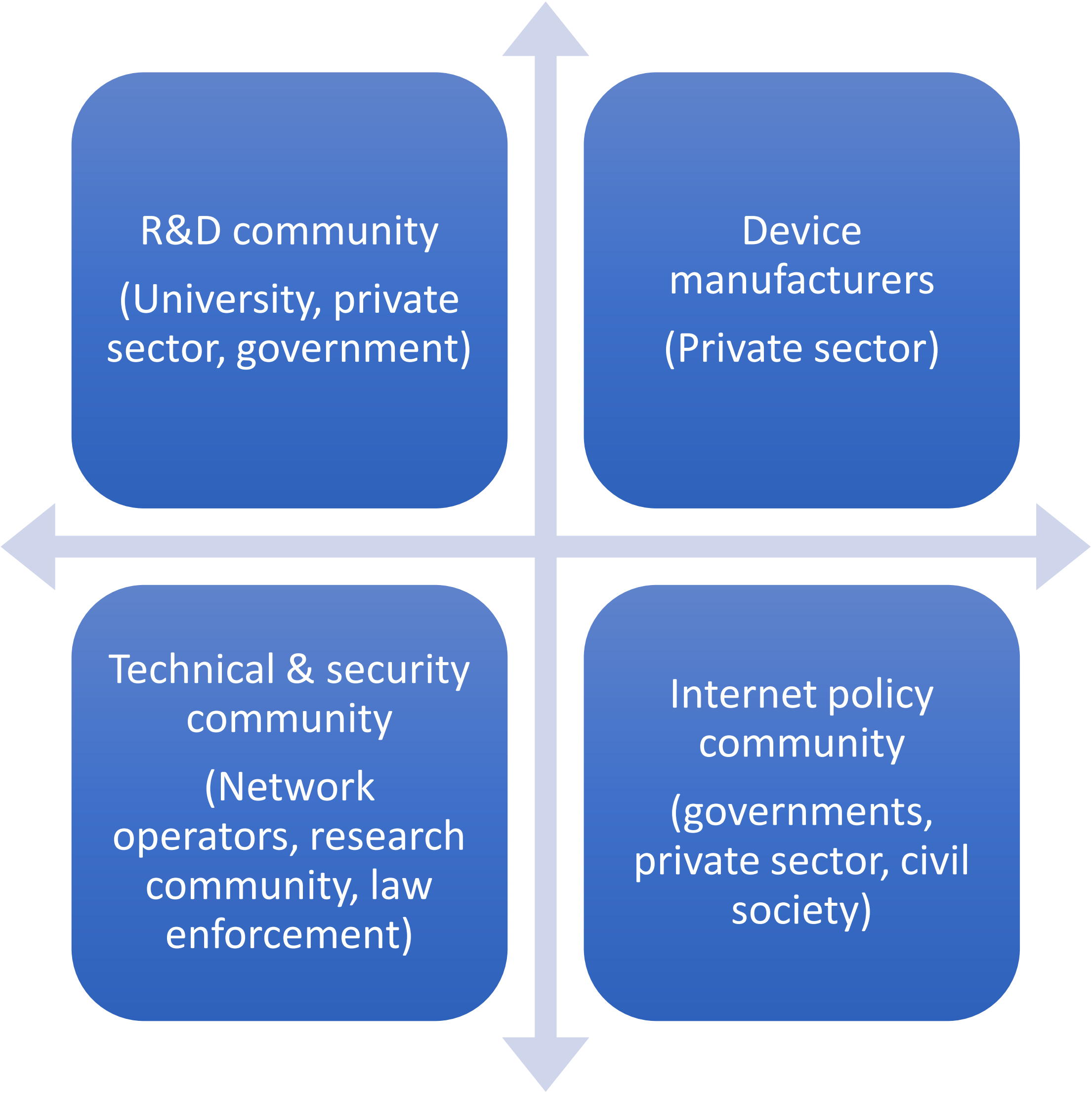
Moderated, in-person meetings with the larger stakeholder group. In between these sessions, leverage:

- **Smaller workshops with special interest groups**
- **Virtual roundtables and webinars**
- **Online communication platforms for general discussion**

Canada, process finalized: https://iotsecurity2018.ca

Ongoing in

- France
- Senegal
- Philippines
- Uruguay



R&D community

(University, private sector, government)

Device manufacturers

(Private sector)

Technical & security community

(Network operators, research community, law enforcement)

Internet policy community

(governments, private sector, civil society)

Get involved.

www.internetsociety.org/iot

lacnog

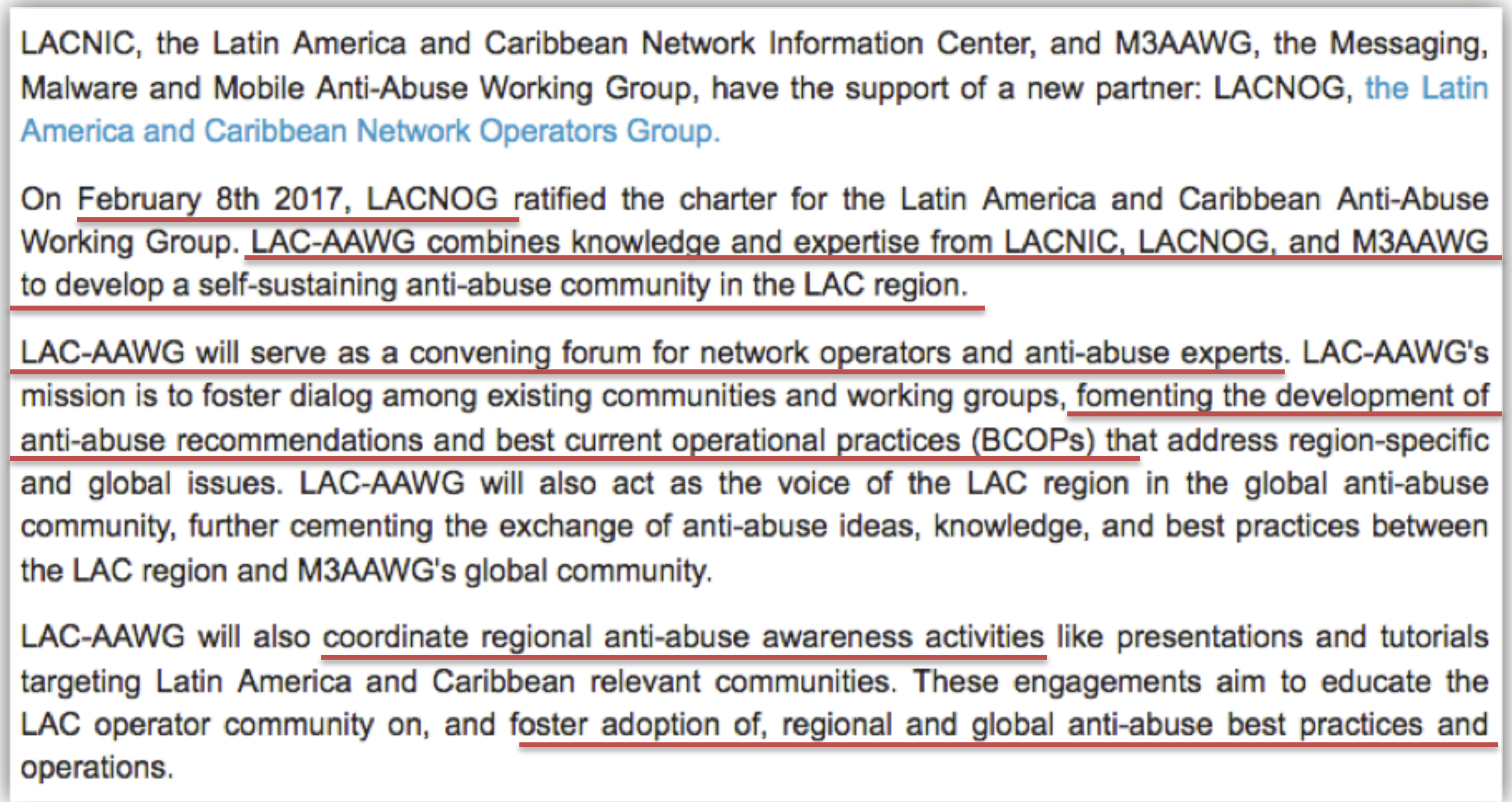
M³AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Latin America and Caribbean Anti-Abuse Working Group **LAC-AAWG**

Lucimara Desiderá

LAC-AAWG co-chair

lacnog M3AAWG MESSAGING MALWARE MOBILE ANTI-ABUSE WORKING GROUP lacnic



LACNIC, the Latin America and Caribbean Network Information Center, and M3AAWG, the Messaging, Malware and Mobile Anti-Abuse Working Group, have the support of a new partner: LACNOG, the Latin America and Caribbean Network Operators Group.

On February 8th 2017, LACNOG ratified the charter for the Latin America and Caribbean Anti-Abuse Working Group. LAC-AAWG combines knowledge and expertise from LACNIC, LACNOG, and M3AAWG to develop a self-sustaining anti-abuse community in the LAC region.

LAC-AAWG will serve as a convening forum for network operators and anti-abuse experts. LAC-AAWG's mission is to foster dialog among existing communities and working groups, fomenting the development of anti-abuse recommendations and best current operational practices (BCOPs) that address region-specific and global issues. LAC-AAWG will also act as the voice of the LAC region in the global anti-abuse community, further cementing the exchange of anti-abuse ideas, knowledge, and best practices between the LAC region and M3AAWG's global community.

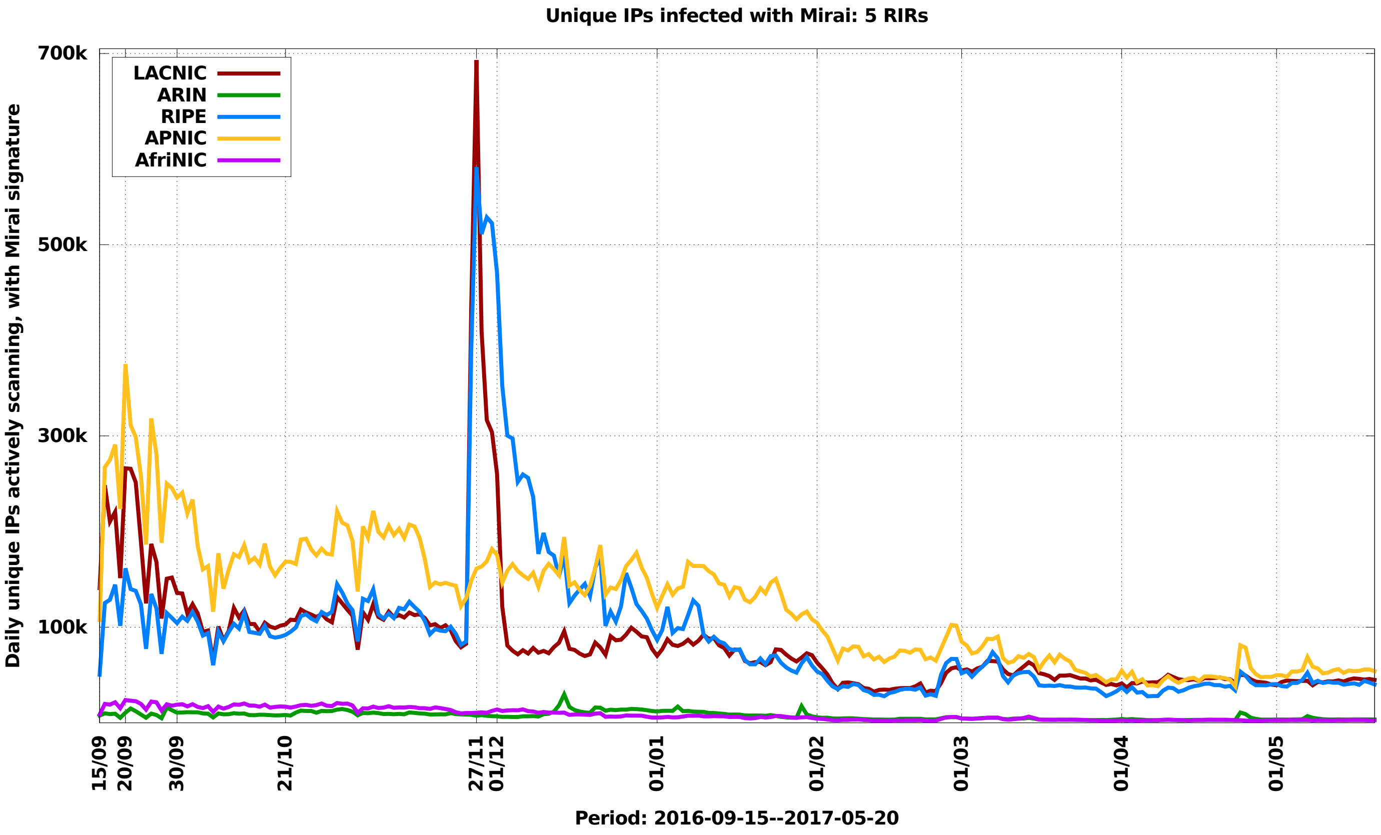
LAC-AAWG will also coordinate regional anti-abuse awareness activities like presentations and tutorials targeting Latin America and Caribbean relevant communities. These engagements aim to educate the LAC operator community on, and foster adoption of, regional and global anti-abuse best practices and operations.

www.lacnic.net/en/web/anuncios/2017-amenazas-en-linea-se-fortalece

Who we are

- Founding **co-chairs**
  - Lucimara Desiderá (CERT.br/NIC.br)
  - Christian O'Flaherty (ISOC)
- Liaison **LACNIC**
  - Graciela Martines
- Liaison **M^{3}AAWG**
  - Severin Walker / Dennis Dayman
- Liaison **BCOPs** WG
  - Ariel Weher

Devices Infected by Mirai



Fonte: CERT.br

CPE (In)Security

- standard credentials for numerous devices
- credentials that cannot be changed (hardcoded)
- use of obsolete and insecure protocols and algorithms
- undocumented accesses (backdoors)
- lack of automated and secure update mechanisms
- unnecessary and/or insecure services enabled by default
- services that cannot be disabled
- insecure remote management

Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition

Joint Publication of

- M³AAWG - Messaging, Malware and Mobile Anti-Abuse Working Group
- LACNOG - Latin American and Caribbean Network Operators Group
- Editor: Lucimara, LAC-AAWG Chair / CERT.br

Currently available in:

- English, Japanese and Korean

New translations to be released soon:

- Portuguese, Spanish, French and German

https://www.lacnog.net/docs/lac-bcop-1

https://www.m3aawg.org/CPESecurityBP

LACNOG- M³AAWG 공동 작성
CPE(가입자 댁내장치) 최소 보안 요구사항에 대한
Best Current Operational Practices
LAC-BCOP-1

2019 년 5 월

문서는 LACNOG 웹사이트에서 다운로드 가능합니다. www.lacnog.net/docs/lac-bcop-1

LACNOG-M³AAWG 共同作業による
顧客側通信機器 (CPE) が備えるべき
最低限のセキュリティ要件についての
Best Current Operati
LAC-BCO

May 2019

この文書の原文は LACNOG の Web サイト www.la
この文書の原文は M³AAWG の Web サイト www.m

この文書は LACNOG[1] (Latin American and Caribbean N
(Messaging, Malware and Mobile Anti-Abuse Working Gro
Current Operational Practices (BCOP)である。LACNOG
AAWG[3] (Latin American and Caribbean Anti-Abuse Work
した草案をもとに M³AAWG 会員と Senior Technical A
調作業によって作成された。

目次

[1] Latin American and Caribbean Network Operators Group (LACNOG
[2] Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAW
[3] Latin American and Caribbean Anti-Abuse Working Group (LAC-AA
[4] LACNOG BCOP Working Group, https://www.lacnog.net/wg-bcop

LACNOG
Latin American and Caribbean Network Operators Group
Department of Montevideo, Oriental Republic of Uruguay
www.lacnog.net

LACNOG-M³AAWG Joint Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition LAC-BCOP-1

May 2019

This document is available on the LACNOG website at www.lacnog.net/docs/lac-bcop-1

This document is available on the M³AAWG website at www.m3aawg.org/CPESecurityBP

This is a joint Best Current Operational Practices (BCOP) document developed by LACNOG[1] (Latin American and Caribbean Network Operators Group) and M³AAWG[2] (Messaging, Malware and Mobile Anti-Abuse Working Group). It is the product of LACNOG's original drafts by its working groups LAC-AAWG[3] (Latin American and Caribbean Anti-Abuse Working Group) and BCOP Working Group[4], in cooperation with M³AAWG members, Senior Technical Advisors and the M³AAWG Technical Committee.

Table of Contents

[1] The Latin American and Caribbean Network Operators Group (LACNOG), https://www.lacnog.net/
[2] Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), https://www.m3aawg.org/
[3] Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG), https://www.lacnog.net/lac-aawg/
[4] LACNOG BCOP Working Group, https://www.lacnog.net/wg-bcops/

LACNOG
Latin American and Caribbean Network Operators Group
Department of Montevideo, Oriental Republic of Uruguay
www.lacnog.net

M³AAWG
Messaging, Malware and Mobile Anti-Abuse Working Group
781 Beach Street, Suite 302
San Francisco, California 94109 U.S.A. – www.m3aawg.org

What is inside?

A reference checklist for hardware decisions

→ Let’s ask vendors for better products while improving our networks! 😀

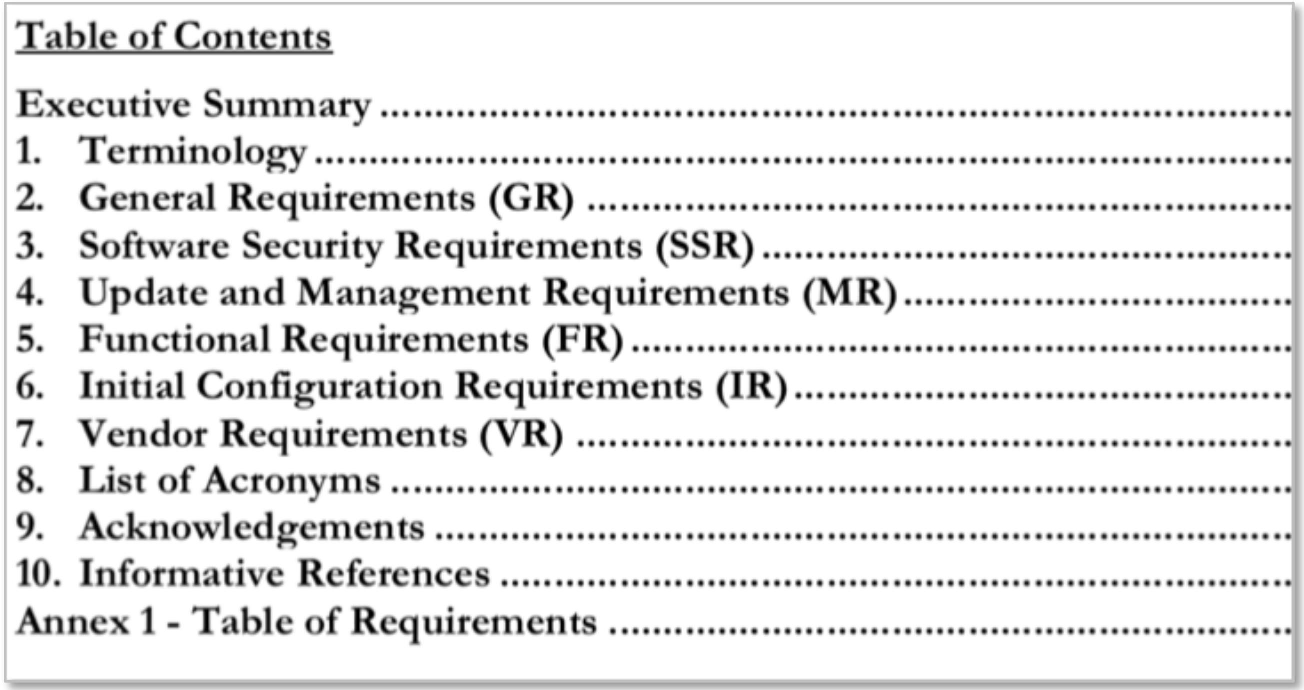


Table of Contents

How to participate

- List **BCOP** bcop@lacnog.org
  - open list of the BCOP Working Group (LACNOG) for discussion of Best Current Operational Practices;
- List **LACNOG** lacnog@lacnog.org
  - open mailing list for discussion of general topics on network operations, not limited to Security;

Thank you!

Questions?

lucimara@cert.br

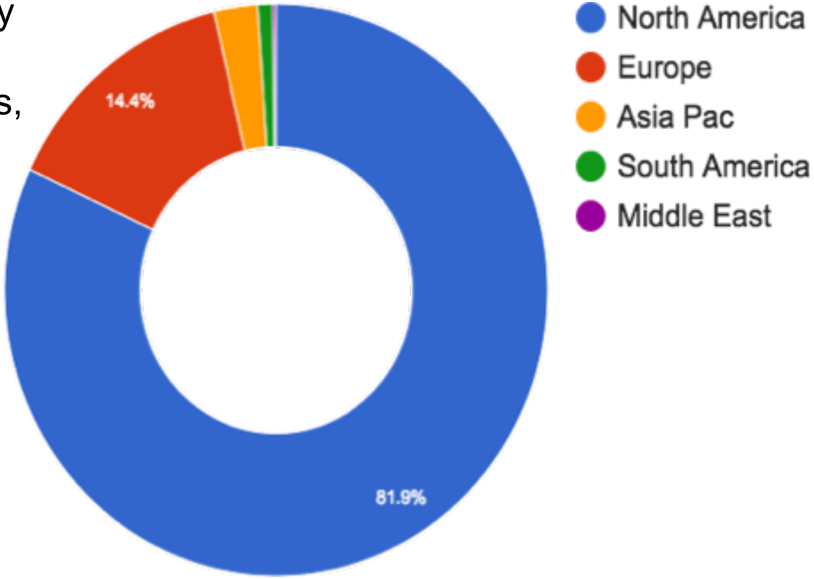
M^{3}AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

M^{3}AAWG Overview

Lucimara Desiderá
GFCE Triple-I
La Paz, BO

Who is M³AAWG?

"The Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) is where the industry comes together to work against botnets, malware, spam, viruses, DoS attacks and other online exploitation"



➔200 member orgs worldwide

➔300-600 conference participants

What does M^{3}AAWG Do?

The “M” *cubed*:

- ➔ <u>Messaging:</u> abuse on any messaging platform, from email to SMS texting
- ➔ <u>Malware:</u> abuse is often just a symptom and vector for viruses and malicious code
- ➔ <u>Mobile:</u> addressing messaging and malware issues emerging on mobile as an increasingly ubiquitous platform

Message, Mobile and Malware Anti-Abuse Working Group

M^{3}AAWG Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers

Develop and Publish:

- ➔ Best practice papers
- ➔ Position statements
- ➔ Training and educational

Types of Output

Types of Documents Produced by M³AAWG	
BCPs	Best Common Practices codify industry knowledge, hallway conversations and experience, into guidelines and authoritative statements on the state of industry practices and dynamics
Technical Whitepapers	Provide state-of-the-industry reports on technologies at play in the messaging industry, how they are being used, and how they contribute to anti-abuse efforts
Public Policy	Actively seeks to provide the necessary technical and strategic guidance to protect end-users' online experience as government, Internet and public policy agencies worldwide develop new Internet policies and legislation*

Message, Mobile and Malware Anti-Abuse Working Group

M³AAWG Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers

March 2015

Executive Summary

Table of Contents

1. Introduction
2. Types of Hosting
3. Types of Abuse
4. Prevention
5. Detection and Identification
6. Remediation

Appendix 1: Glossary of Standard Terms
Appendix 2: Legal and Other Resources
Appendix 3: A Note about Data Security
Appendix 4: Ticketing Systems

*https://www.m3aawg.org/for-the-industry/published-comments

Dynamics of a Working Group

Individual industry actors can't …

➔ ***effectively*** or ***efficiently*** fight online abuse *alone*
➔ ***protect*** end-users and customers in a vacuum

As an **active working group M^{3}AAWG** can …

➔ ***effectively*** and ***efficiently*** fight online abuse *together*
➔ ***collaboratively protect*** end-users and customers

M^{3}AAWG's successes are rooted in …

➔ ***working group participation***, in service of
➔ ***cooperation***, to create
➔ effective and efficient anti-abuse outcomes
➔ in a ***trusted*** environment

A Circle of Trust for Participants

M^{3}AAWG provides a trusted forum and framework for open discussion of abuse issues in an atmosphere of confidentiality and cooperation.

A trusted environment facilitates a level of free, open participation key to anti-abuse efforts.

Creating and maintaining such an environment is the platform on which all of the other cooperative efforts are built.

Who do we work with?

➔Unsolicited Commercial Enforcement Net

- Operation Safety Net

➔Internet Society

- Provided training material

➔i^{2}Coalition

- Hosting BCP

➔EastWest Institute

- 2013 Cyber Security Award for China & India Work

➔Anti-Phishing Working Group (APWG)

- Anti-Phishing Best Practices for ISPs and Mailbox Providers

➔LACNIC / LACNOG

- BCPs to reflect dynamics in the LAC region
- LAC-AAWG Started in 2017

Current Work

Committee	Work or Accomplishment
Abuse Desk	Training materials currently being developed for ISPs and service platform operators.
Data and ID Protection	Several BCPs produced concerning encryption, 3rd party DNS providers, and other communications security topics
DDoS	BGP Flowspec Best Practices published Full day workshops with NANOG and non-members held
DNS Abuse	Ongoing commentary and focus on GDPR impact to WHOIS in ICANN
Hosting	Cryptomining Anti-Abuse BCP
Mobile	Collaboration with GSMA on RCS Anti-Abuse recommendations and training and preparation for 5G
LAC-AAWG	Device Security BCOP published and translated into multiple languages

Regional working groups

LAC-AAWG

- May2019: published a joint Best Current Operational Practice (BCOP) on CPE Security Requirements
- October2019: LACNIC32/LACNOG2-2019: provide training

JP-AAWG

- Nov2018: 1st JP-AAWG conference held in Tokyo with 400+ attendees for a 1-day, 2-track meeting.
- November 14th – 15th 2019: 2nd JP-AAWG Conference to be held in Tokyo with M3AAWG participation

AFR-AAWG

- Work continues with AfricaCERT to establish a new regional working group with a focus on providing training materials.
- Plans to contribute at the AfriNIC December 2019 meeting in Angola

Upcoming Meeting

47th General Meeting

October 14-17, 2019

Fairmont

The Queen Elizabeth

Montreal, Canada

For more information about attendance or membership, contact

severin@m3aawg.org

MANRS

Normas Mutuamente Acordadas para el Enrutamiento Seguro en Internet

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.

Internet Society lacnic

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.

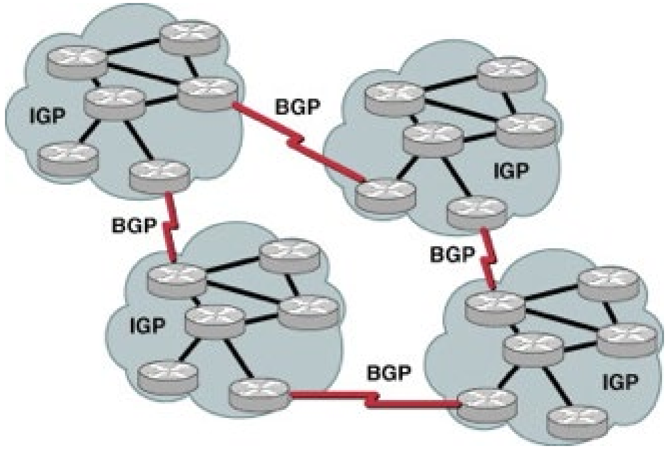
Una mala configuración de una red no solo afecta el servicio para sus usuarios, sino que puede afectar a otros operadores en cualquier parte del mundo.

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

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.

lacnic

Internet Society

lacnog

NIC MÉXICO

Red CLARA

Cooperación Latino Americana de Redes Avanzadas

ANUIES

ANUIES - TIC

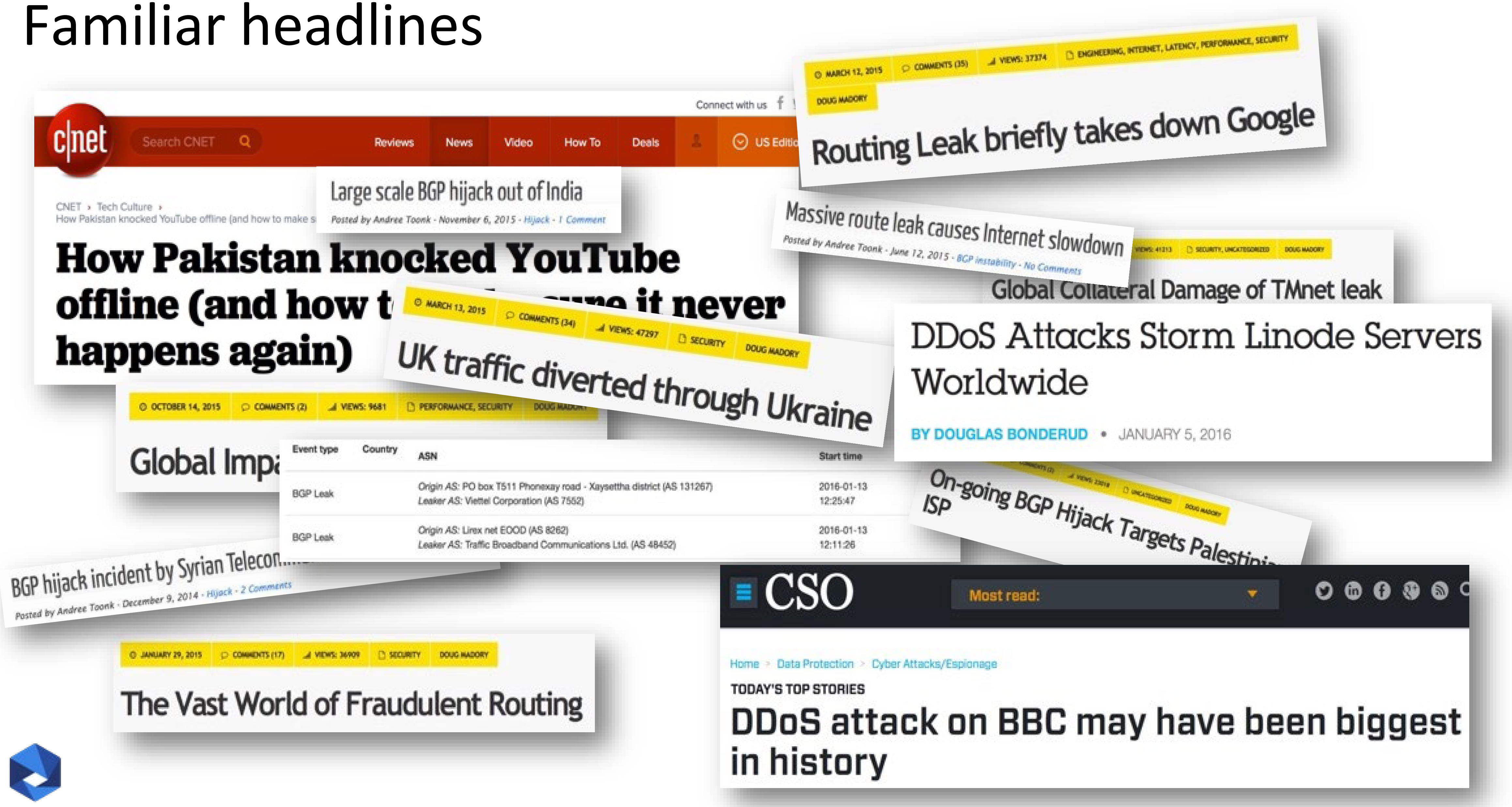
cudi

Corporación Universitaria para el Desarrollo de Internet A.C.
Internet 2 - México

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



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

Routing Leak briefly takes down Google

c|net Search CNET Reviews News Video How To Deals US Editio… Connect with us

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

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

Large scale BGP hijack out of India

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

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

On-going BGP Hijack Targets Palestini… 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

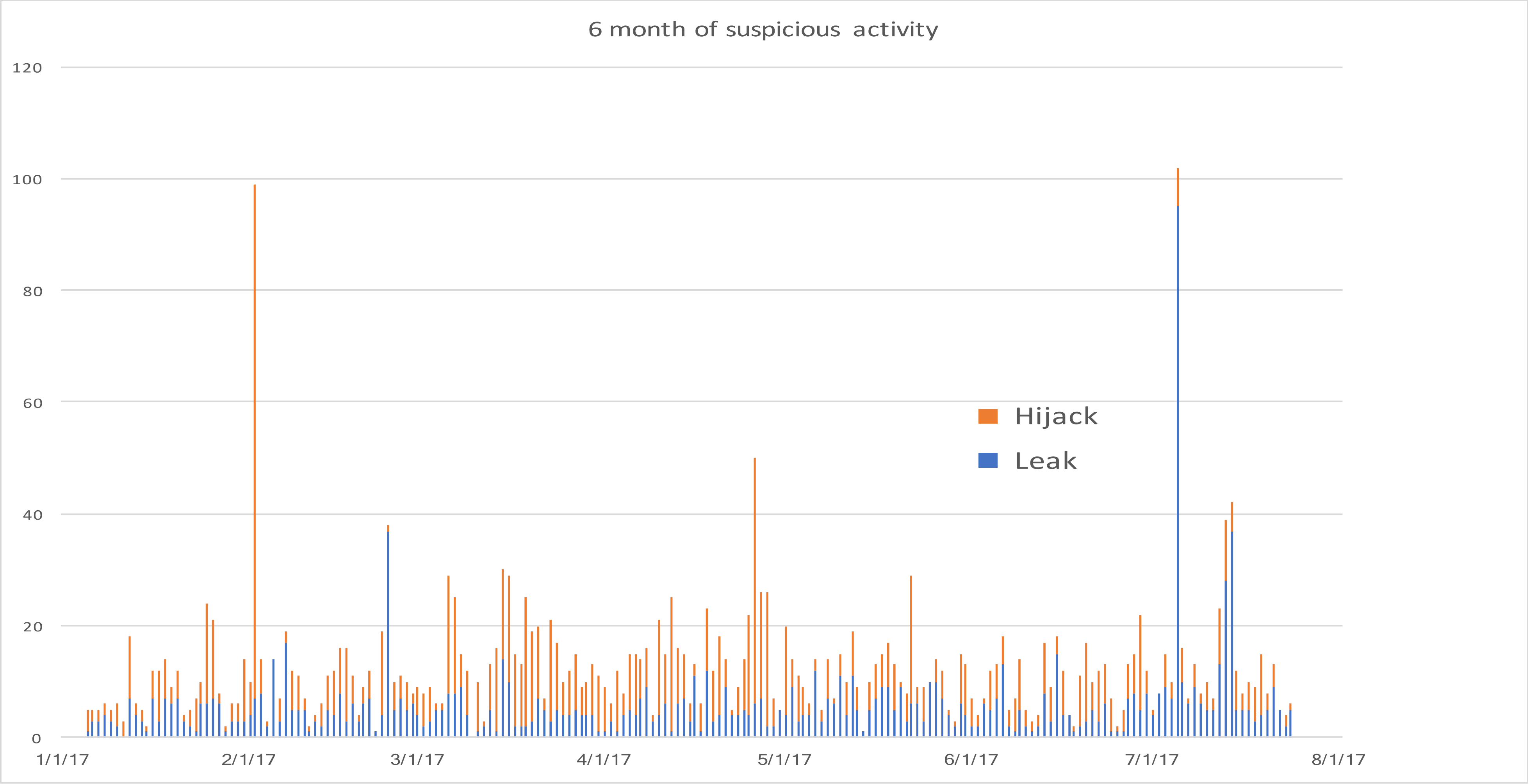
CSO Most read:

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 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.

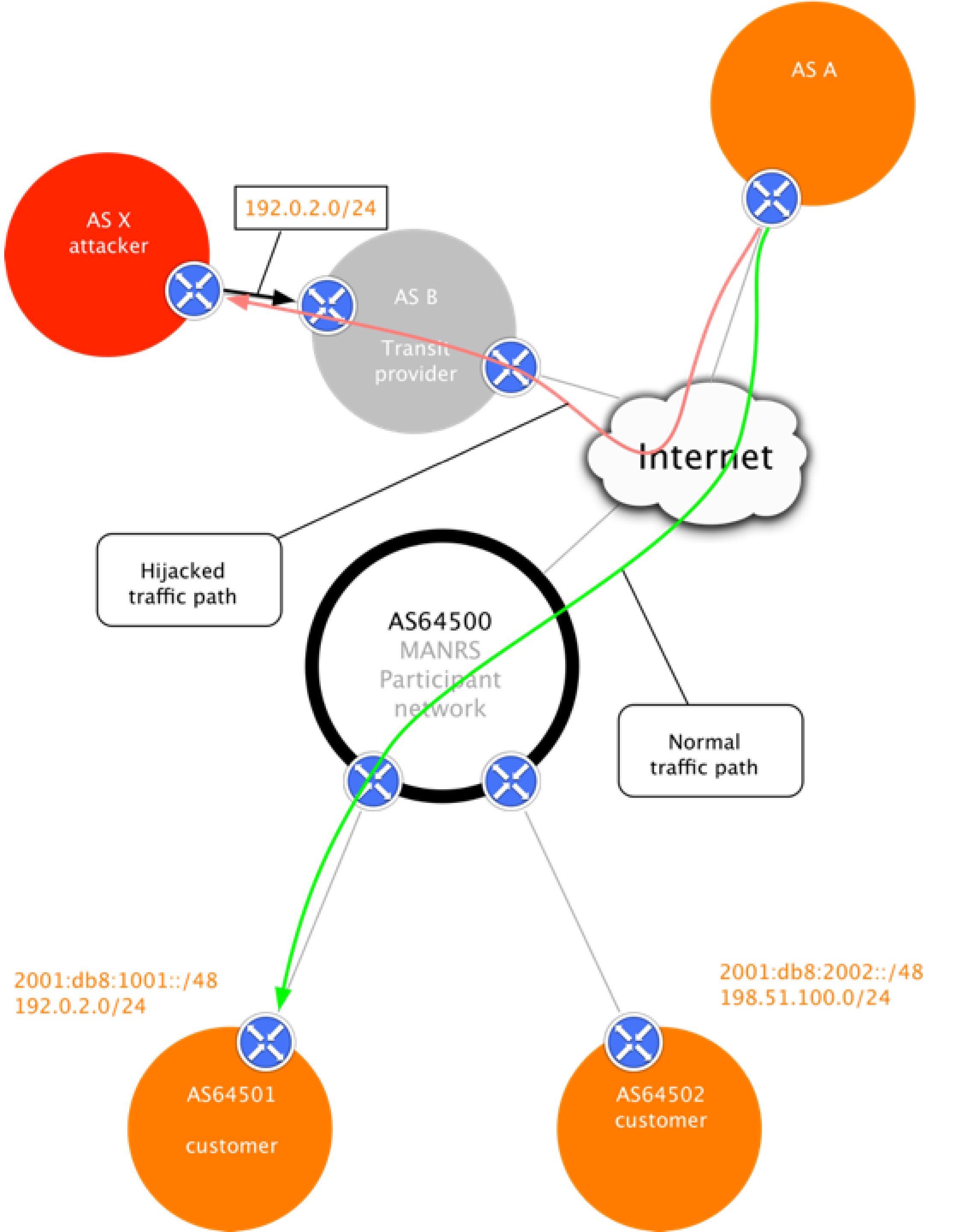
The Honor System: Routing Issues

- 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

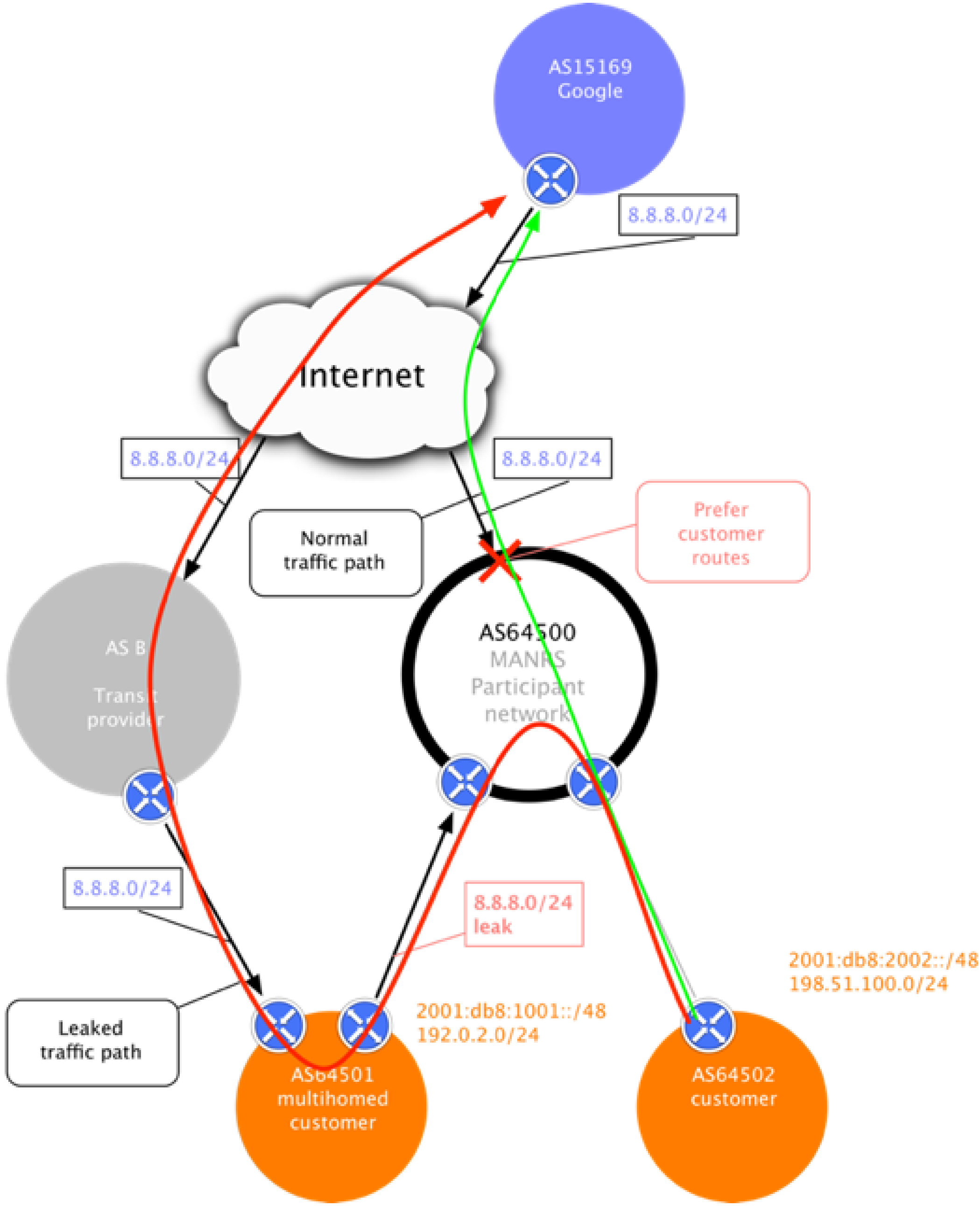
- **Route hijacking,** also known as “BGP hijacking” when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretends that the network is their client. This routes traffic to the attacker, while the victim suffers an outage.

- ***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)*



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/)*

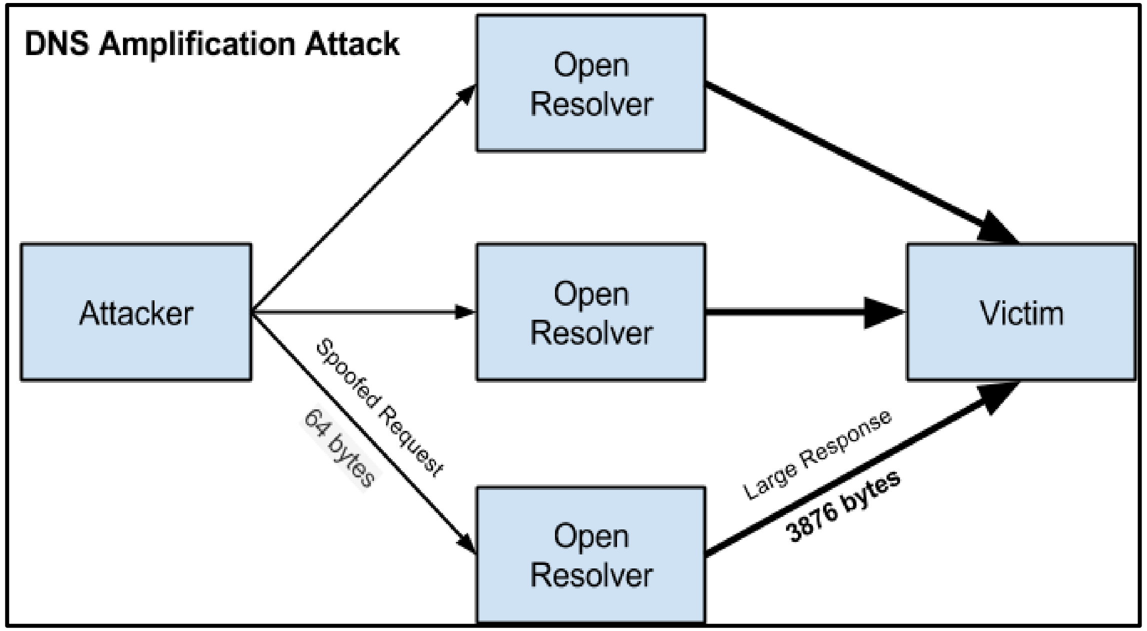


IP Address Spoofing

- **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

MANRS

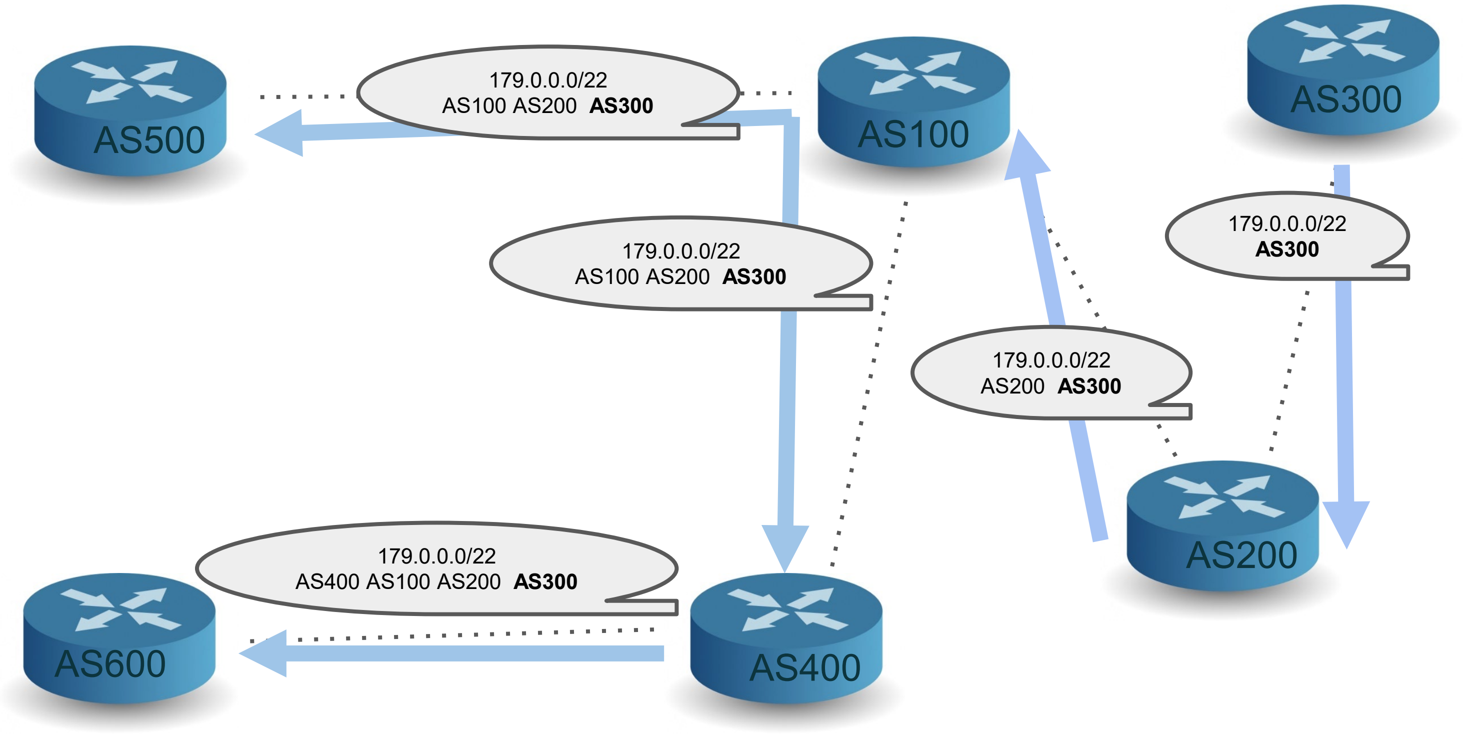
Preguntas

RPKI

Infraestructura de clave pública para recursos de numeración de Internet

gerardo@lacnic.net
Gerardo Rada

Repaso de BGP



Quien originó el anuncio del 179/22?

AS 300

Quienes son los vecinos o pares del AS100?

AS 200, AS 400, AS 500

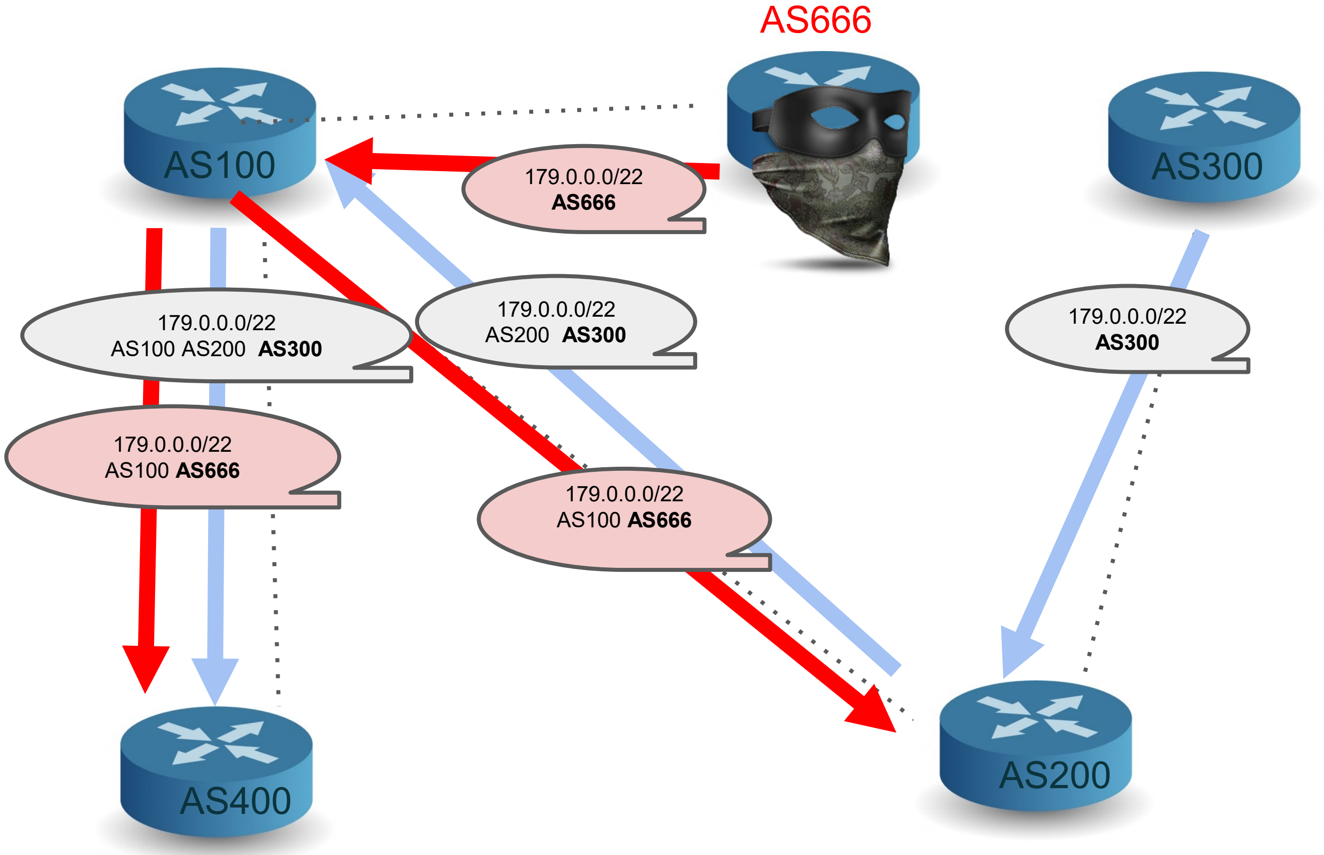
Quienes propagaron la ruta?

AS 200, AS 100, AS 400

Quienes conocen la ruta

TODOS

HIJACKING “CAMINO MÁS CORTO”



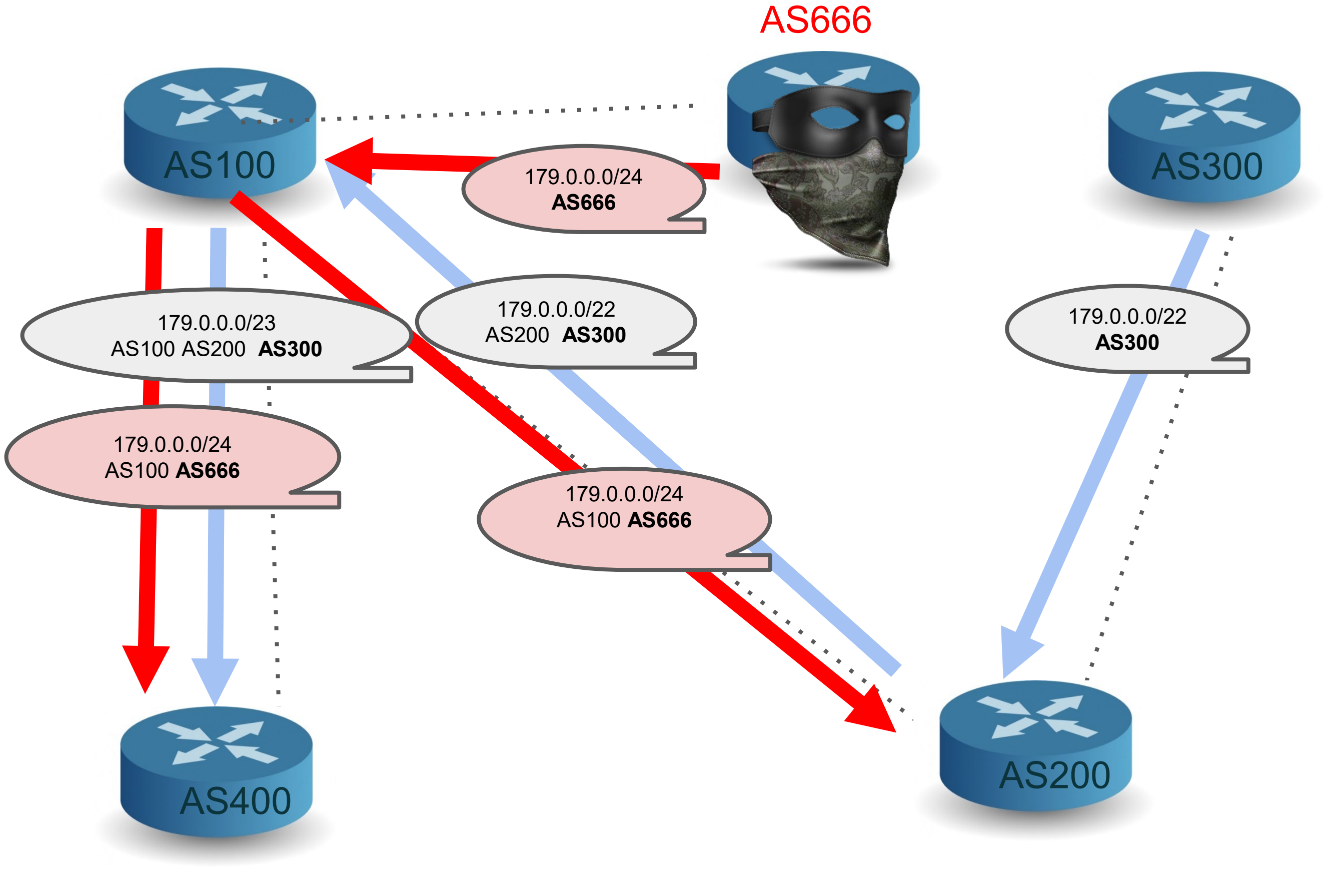
Qué pasa con los AS100y AS400?

Qué pasa con el AS200?

Cómo se da cuenta el AS300 que hay un problema?

Qué puede hacer el AS300 para solucionarlo?

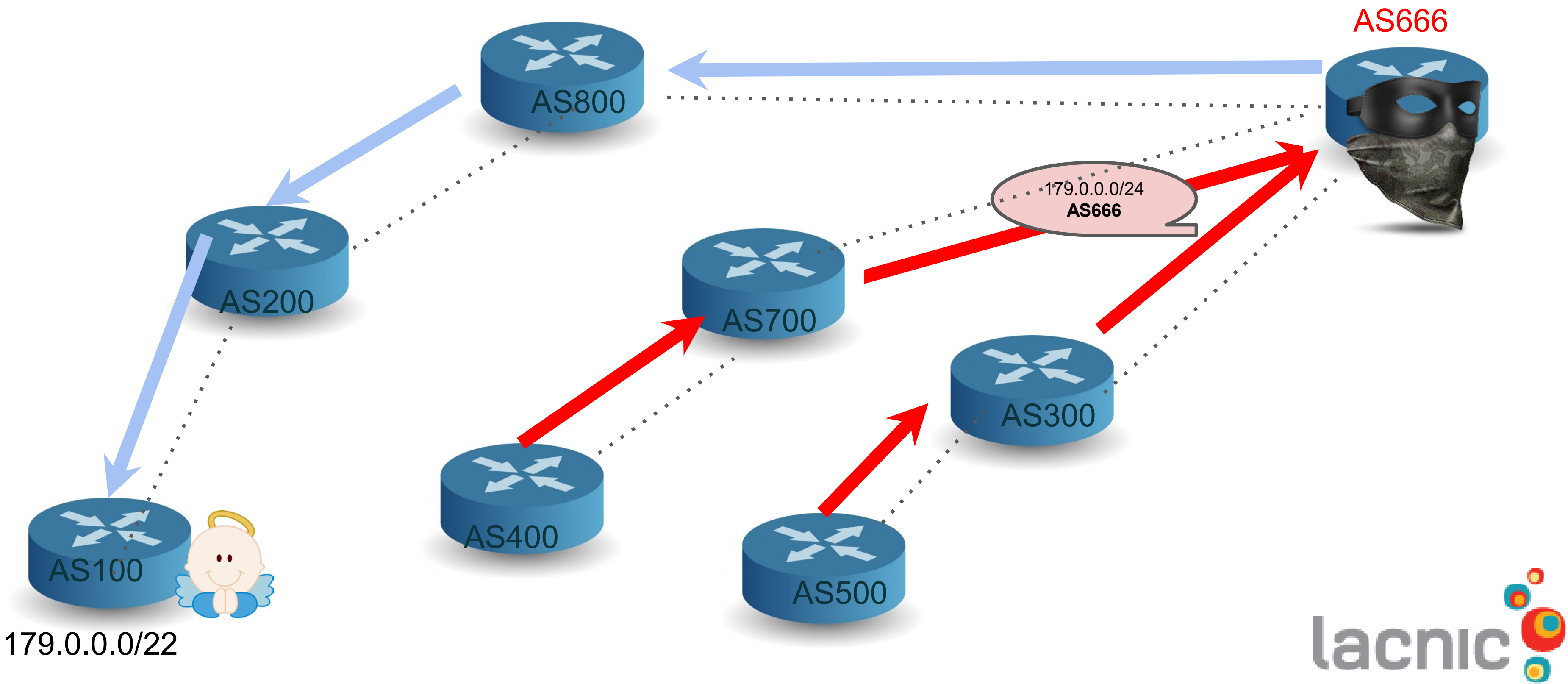
HIJACKING “RUTA MÁS ESPECÍFICA”



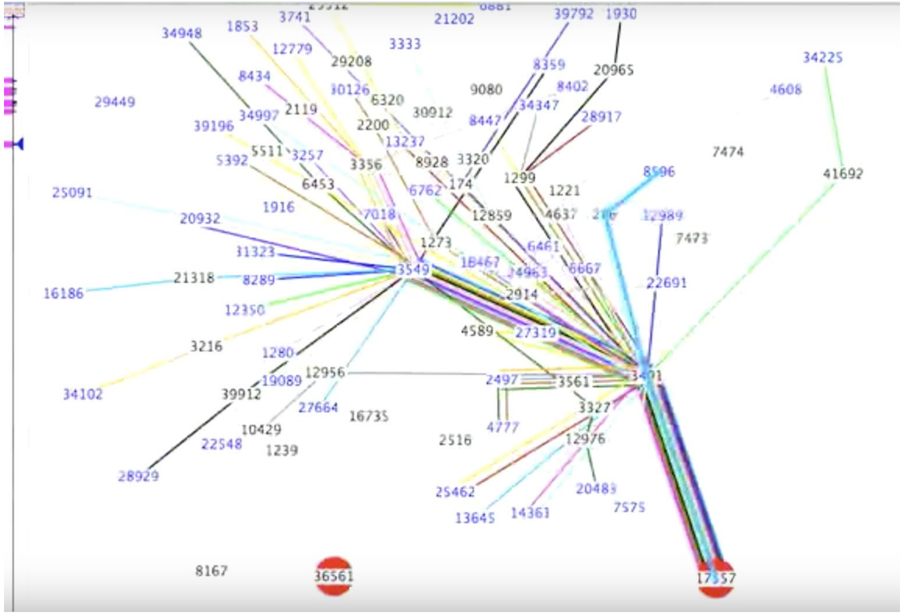
Qué pasa con el AS200?

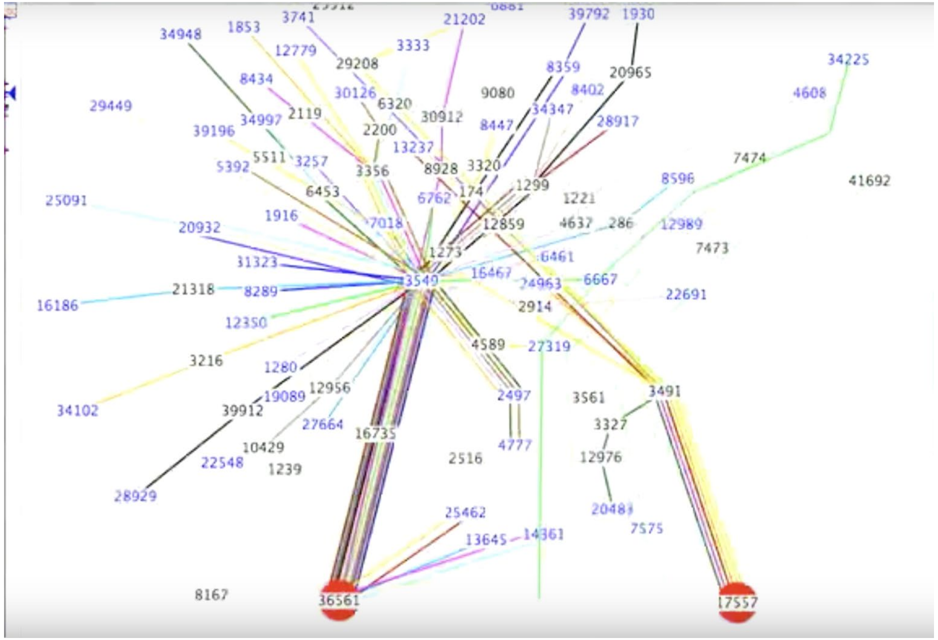
Qué puede hacer el AS300 para solucionarlo?

Kapela - Pilosov



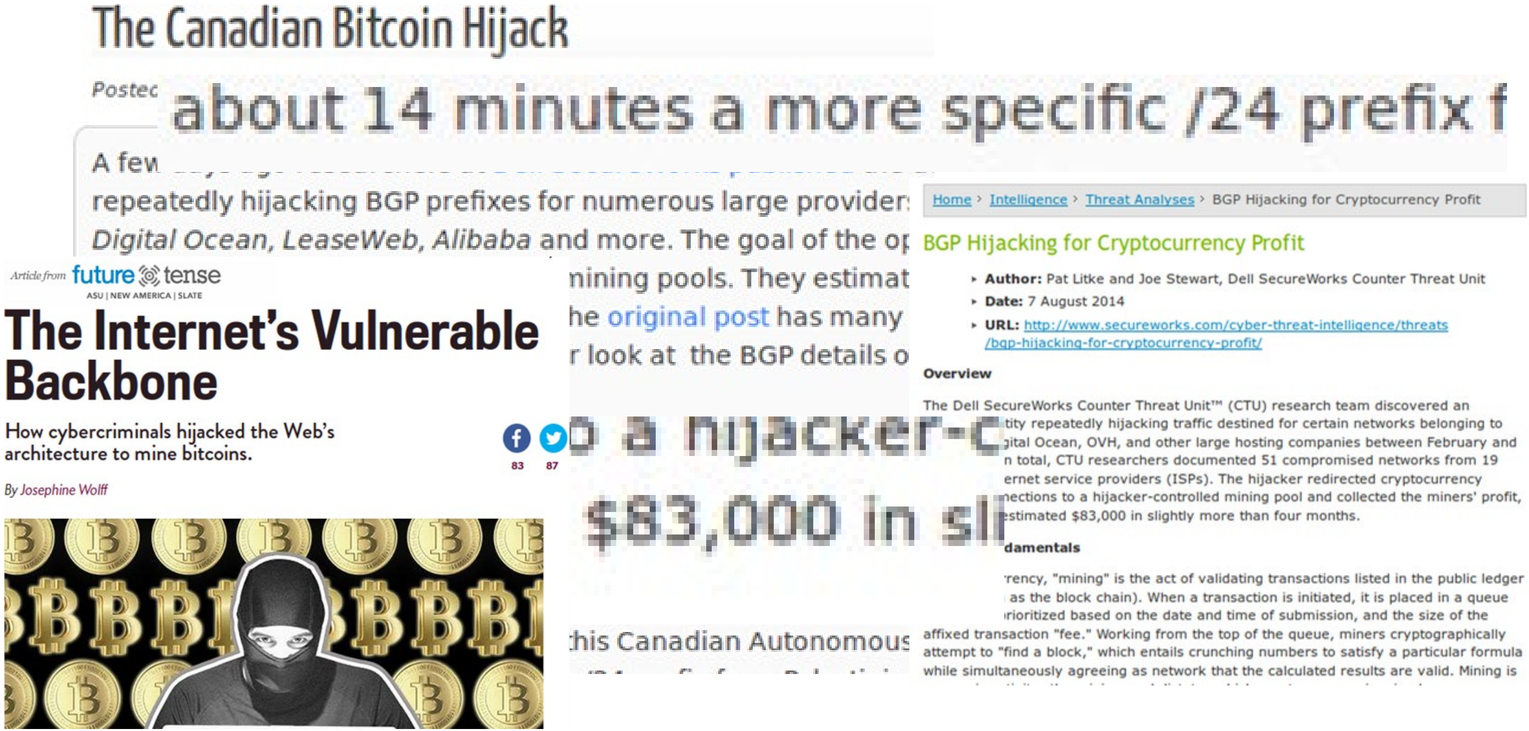
Caso Youtube - Pakistan Telecom





https://www.youtube.com/watch?v=IzLPKuAOe50

Caso Robo de Bitcoin



The Canadian Bitcoin Hijack

Postec

about 14 minutes a more specific /24 prefix f

A few

repeatedly hijacking BGP prefixes for numerous large provider

Digital Ocean, LeaseWeb, Alibaba and more. The goal of the op

nining pools. They estimat

he original post has many

r look at the BGP details o

o a hijacker-c

$83,000 in sli

his Canadian Autonomous

Article from future tense ASU | NEW AMERICA | SLATE

The Internet's Vulnerable Backbone

How cybercriminals hijacked the Web's architecture to mine bitcoins.

83 87

By Josephine Wolff

Home › Intelligence › Threat Analyses › BGP Hijacking for Cryptocurrency Profit

BGP Hijacking for Cryptocurrency Profit

- **Author:** Pat Litke and Joe Stewart, Dell SecureWorks Counter Threat Unit
- **Date:** 7 August 2014
- **URL:** http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/

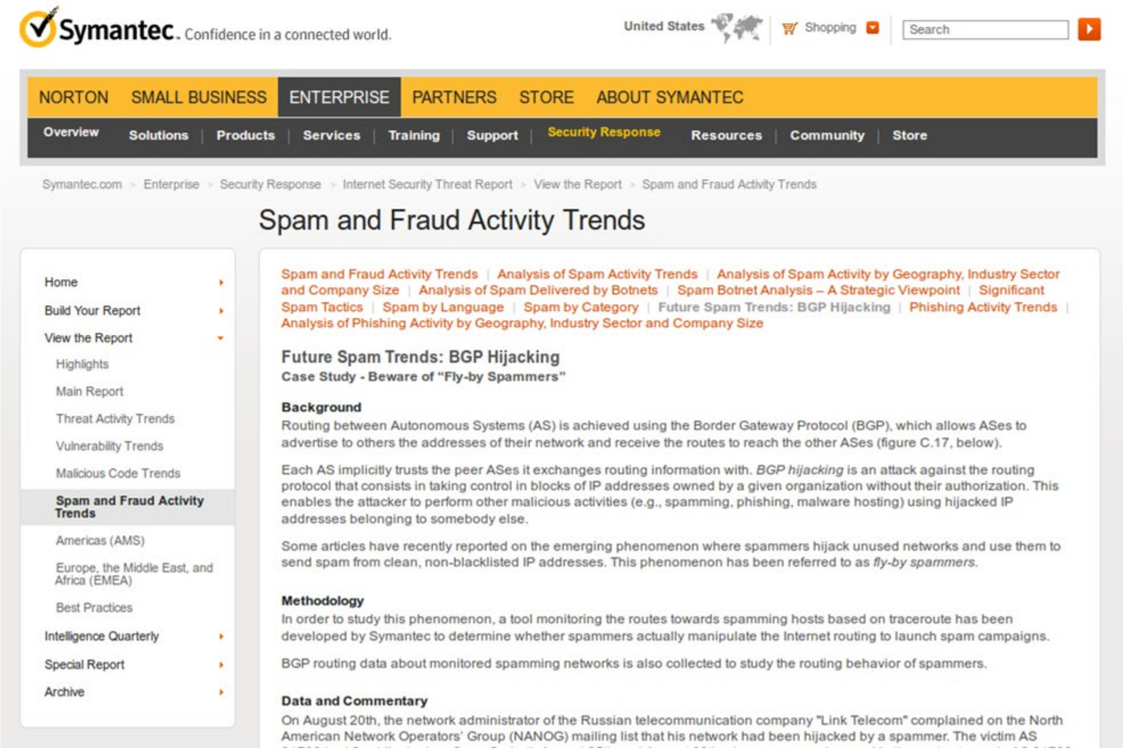
Overview

The Dell SecureWorks Counter Threat Unit™ (CTU) research team discovered an
tity repeatedly hijacking traffic destined for certain networks belonging to
gital Ocean, OVH, and other large hosting companies between February and
n total, CTU researchers documented 51 compromised networks from 19
ernet service providers (ISPs). The hijacker redirected cryptocurrency
nections to a hijacker-controlled mining pool and collected the miners' profit,
estimated $83,000 in slightly more than four months.

damentals

rency, "mining" is the act of validating transactions listed in the public ledger
as the block chain). When a transaction is initiated, it is placed in a queue
rioritized based on the date and time of submission, and the size of the
affixed transaction "fee." Working from the top of the queue, miners cryptographically
attempt to "find a block," which entails crunching numbers to satisfy a particular formula
while simultaneously agreeing as network that the calculated results are valid. Mining is

Caso SPAM y Más SPAM


Symantec. Confidence in a connected world.
United States
Shopping
Search
NORTON
SMALL BUSINESS
ENTERPRISE
PARTNERS
STORE
ABOUT SYMANTEC
Overview
Solutions
Products
Services
Training
Support
Security Response
Resources
Community
Store
Symantec.com > Enterprise > Security Response > Internet Security Threat Report > View the Report > Spam and Fraud Activity Trends
Home
Build Your Report
View the Report
Highlights
Main Report
Threat Activity Trends
Vulnerability Trends
Malicious Code Trends
Spam and Fraud Activity Trends
Americas (AMS)
Europe, the Middle East, and Africa (EMEA)
Best Practices
Intelligence Quarterly
Special Report
Archive
Spam and Fraud Activity Trends | Analysis of Spam Activity Trends | Analysis of Spam Activity by Geography, Industry Sector and Company Size | Analysis of Spam Delivered by Botnets | Spam Botnet Analysis – A Strategic Viewpoint | Significant Spam Tactics | Spam by Language | Spam by Category | Future Spam Trends: BGP Hijacking | Phishing Activity Trends | Analysis of Phishing Activity by Geography, Industry Sector and Company Size

Spam and Fraud Activity Trends

Future Spam Trends: BGP Hijacking

Case Study - Beware of "Fly-by Spammers"

Background

Routing between Autonomous Systems (AS) is achieved using the Border Gateway Protocol (BGP), which allows ASes to advertise to others the addresses of their network and receive the routes to reach the other ASes (figure C.17, below).

Each AS implicitly trusts the peer ASes it exchanges routing information with. *BGP hijacking* is an attack against the routing protocol that consists in taking control in blocks of IP addresses owned by a given organization without their authorization. This enables the attacker to perform other malicious activities (e.g., spamming, phishing, malware hosting) using hijacked IP addresses belonging to somebody else.

Some articles have recently reported on the emerging phenomenon where spammers hijack unused networks and use them to send spam from clean, non-blacklisted IP addresses. This phenomenon has been referred to as *fly-by spammers*.

Methodology

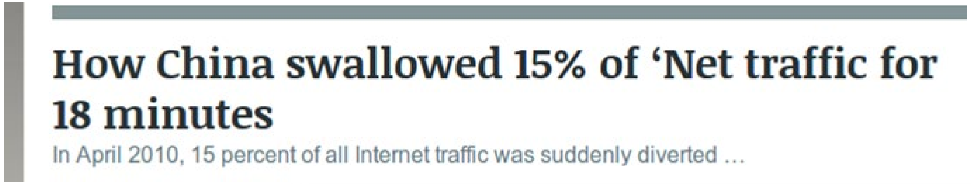
In order to study this phenomenon, a tool monitoring the routes towards spamming hosts based on traceroute has been developed by Symantec to determine whether spammers actually manipulate the Internet routing to launch spam campaigns.

BGP routing data about monitored spamming networks is also collected to study the routing behavior of spammers.

Data and Commentary

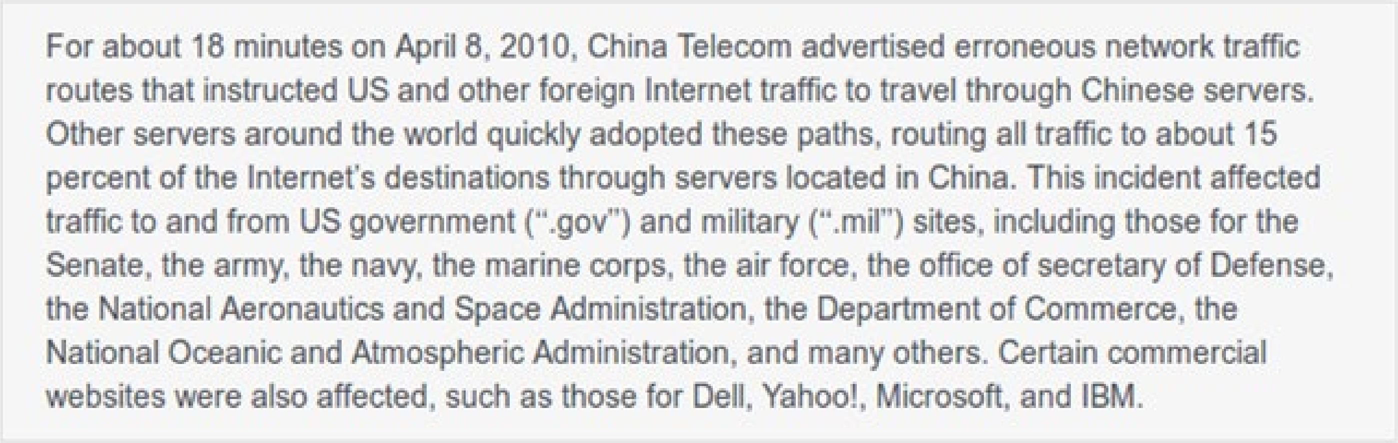
On August 20th, the network administrator of the Russian telecommunication company "Link Telecom" complained on the North American Network Operators' Group (NANOG) mailing list that his network had been hijacked by a spammer. The victim AS

Caso Agujeros Negros



How China swallowed 15% of ‘Net traffic for 18 minutes

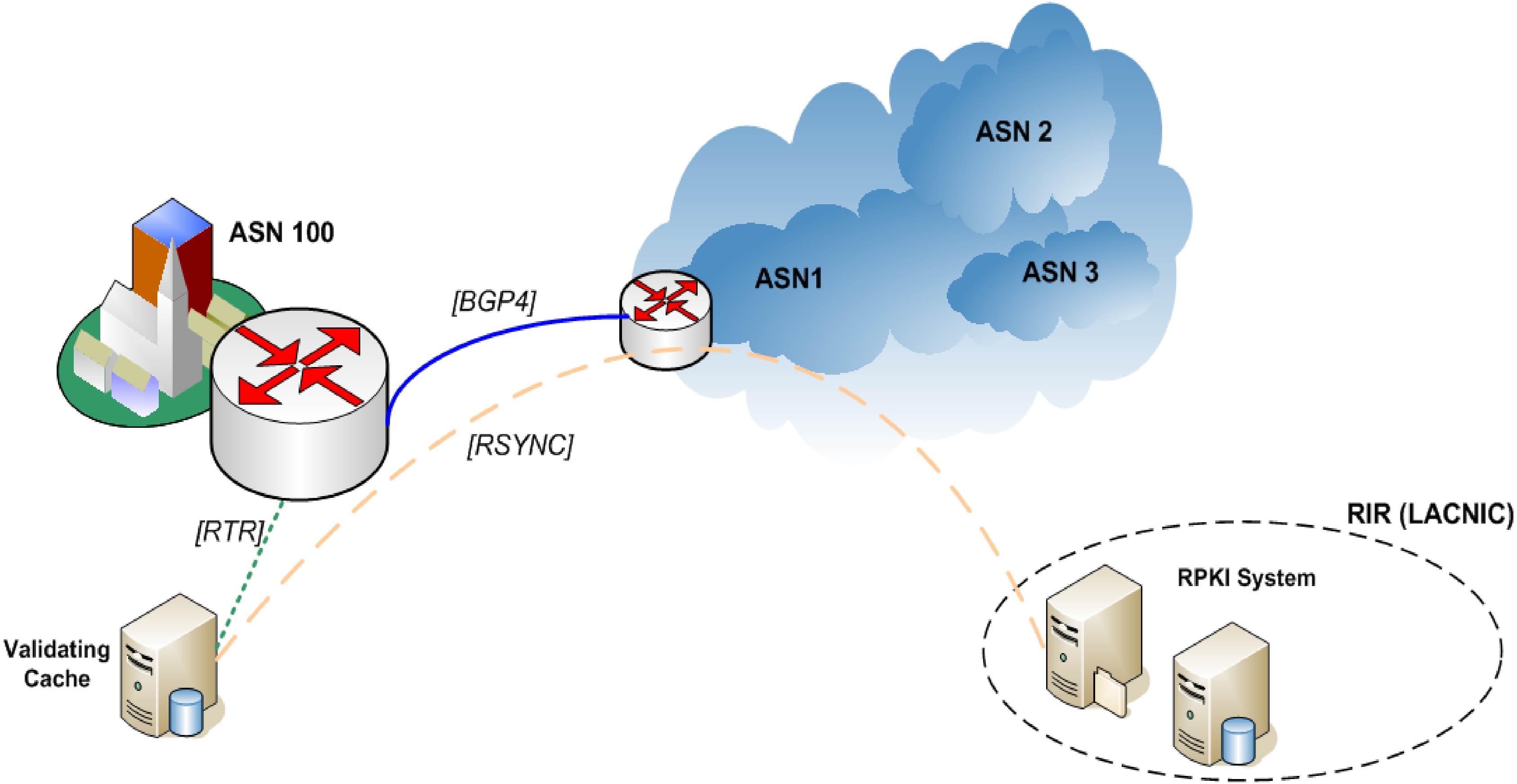
In April 2010, 15 percent of all Internet traffic was suddenly diverted …



For about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed US and other foreign Internet traffic to travel through Chinese servers. Other servers around the world quickly adopted these paths, routing all traffic to about 15 percent of the Internet's destinations through servers located in China. This incident affected traffic to and from US government (“.gov”) and military (“.mil”) sites, including those for the Senate, the army, the navy, the marine corps, the air force, the office of secretary of Defense, the National Aeronautics and Space Administration, the Department of Commerce, the National Oceanic and Atmospheric Administration, and many others. Certain commercial websites were also affected, such as those for Dell, Yahoo!, Microsoft, and IBM.

ROA - AUTORIZACIÓN A ORIGINAR RUTAS

Es un documento firmado donde se indica cual es ASN autorizado a originar rutas


ASN 2
ASN 100
ASN1
ASN 3
[BGP4]
[RSYNC]
[RTR]
RIR (LACNIC)
RPKI System
Validating
Cache

HERRAMIENTAS

http://tools.labs.lacnic.net/announcement/set

https://bgp.he.net/

https://milacnic.lacnic.net

nic.br cgi.br cert.br

GFCE Triple-I Capacity Building | The Internet Infrastructure Security Day

La Paz, BO | August 5, 2019

National Program
“For a Safer Internet”

Lucimara Desiderá, M.Sc.

Security Analyst

lucimara@cert.br

cert.br nic.br cgi.br

CGI.br Members

As established by the presidential decree Nº 4.829, 03/09/2003

9 representatives from the Government

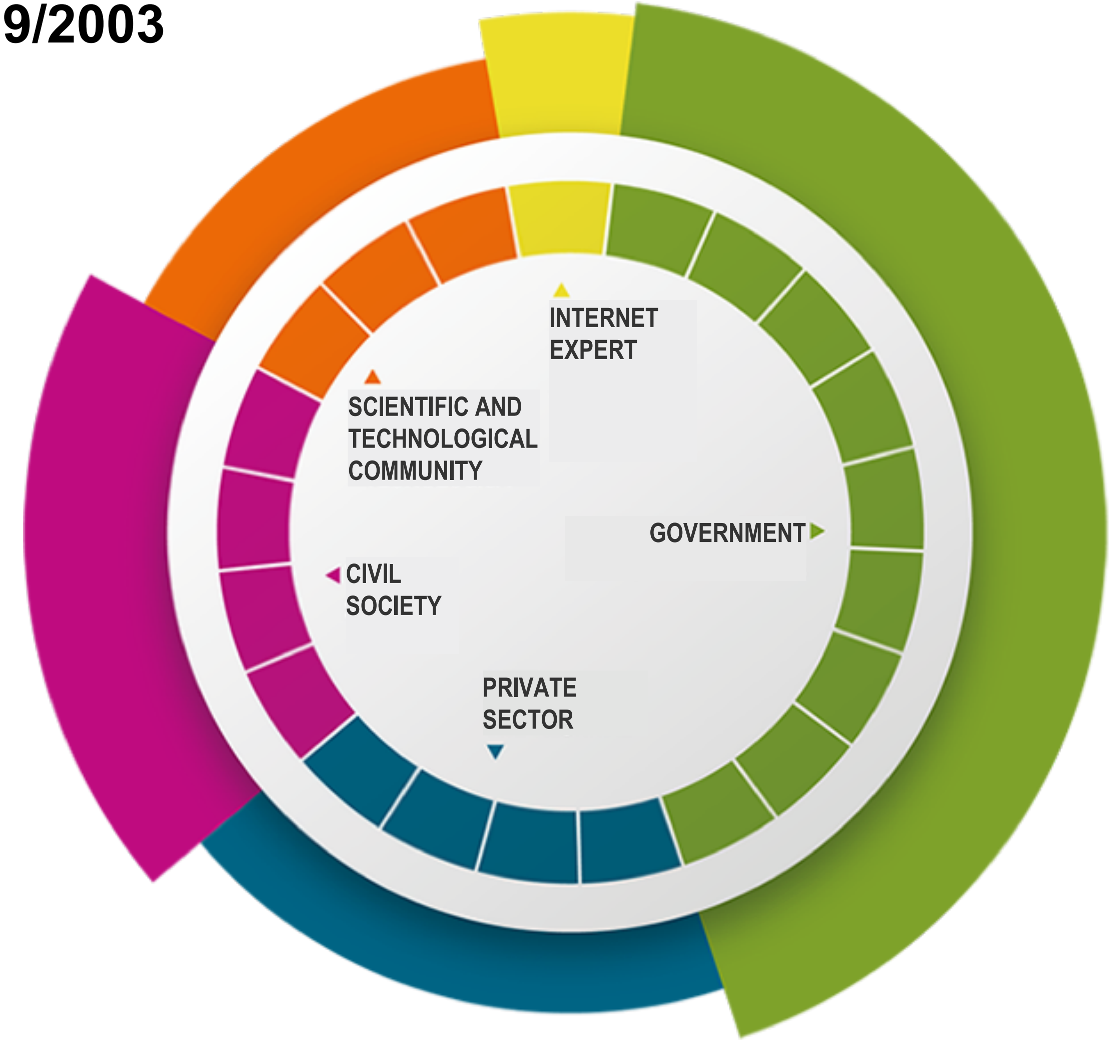
Ministry of Science, Technology and Innovation (coordination)
Ministry of Communications
Presidential Cabinet
Ministry of Defense
Ministry of Development, Industry and Foreign Trade
Ministry of Planning, Budget and Management
National Telecommunication Agency
National Council for Scientific and Technological Development
National Council of State Secretariats for Science, Technology and Information

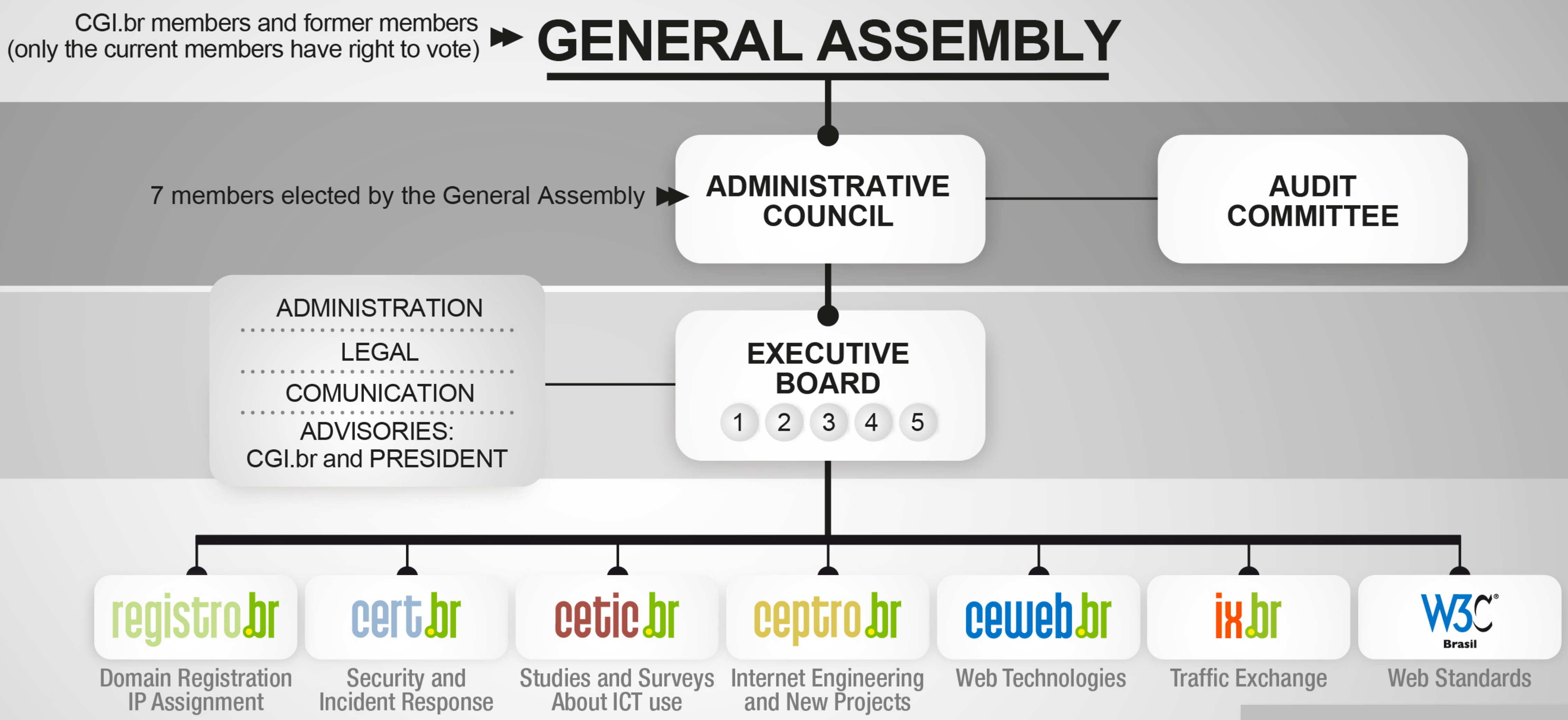
12 representatives from private sector & civil society

Private Sector (4)

- Internet access and content providers
- Telecommunication infrastructure providers
- Hardware, telecommunication and software industries
- Enterprises that use the Internet

Civil Society (4)
Scientific and technological community (3)
Internet Expert (1)





CGI.br members and former members (only the current members have right to vote) ▸▸ **GENERAL ASSEMBLY**

7 members elected by the General Assembly ▸▸ **ADMINISTRATIVE COUNCIL** — **AUDIT COMMITTEE**

ADMINISTRATION

LEGAL

COMUNICATION

ADVISORIES: CGI.br and PRESIDENT

EXECUTIVE BOARD 1 2 3 4 5

registro.br — Domain Registration IP Assignment

cert.br — Security and Incident Response

cetic.br — Studies and Surveys About ICT use

ceptro.br — Internet Engineering and New Projects

ceweb.br — Web Technologies

ix.br — Traffic Exchange

W3C Brasil — Web Standards

1 Chief Executive Officer
2 Administrative and Financial Director
3 IT and Services Director
4 Director of Special Projects and Development
5 Consulting Director for CGI.br activities

NIC.br:

Not for profit organization that implements all services and decisions of CGI.br.

Incident Management

- Coordination
- Technical Analysis
- Support for recovery

Training and Awareness

- Courses
- Presentations
- Best Practices
- Meetings

Trend Analysis

- Distributed Honeypots
- SpamPots
- Processing of threat feeds

Creation:

August/1996: report with a proposed model for incident management for the country is published by the Brazilian Internet Steering Committee – CGI.br[1]

June/1997: CGI.br creates CERT.br (at that time called NBSO – *NIC BR Security Office*) based on the report's recommendations[2]

[1] https://www.nic.br/grupo/historico-gts.htm | [2] https://www.nic.br/pagina/gts/157

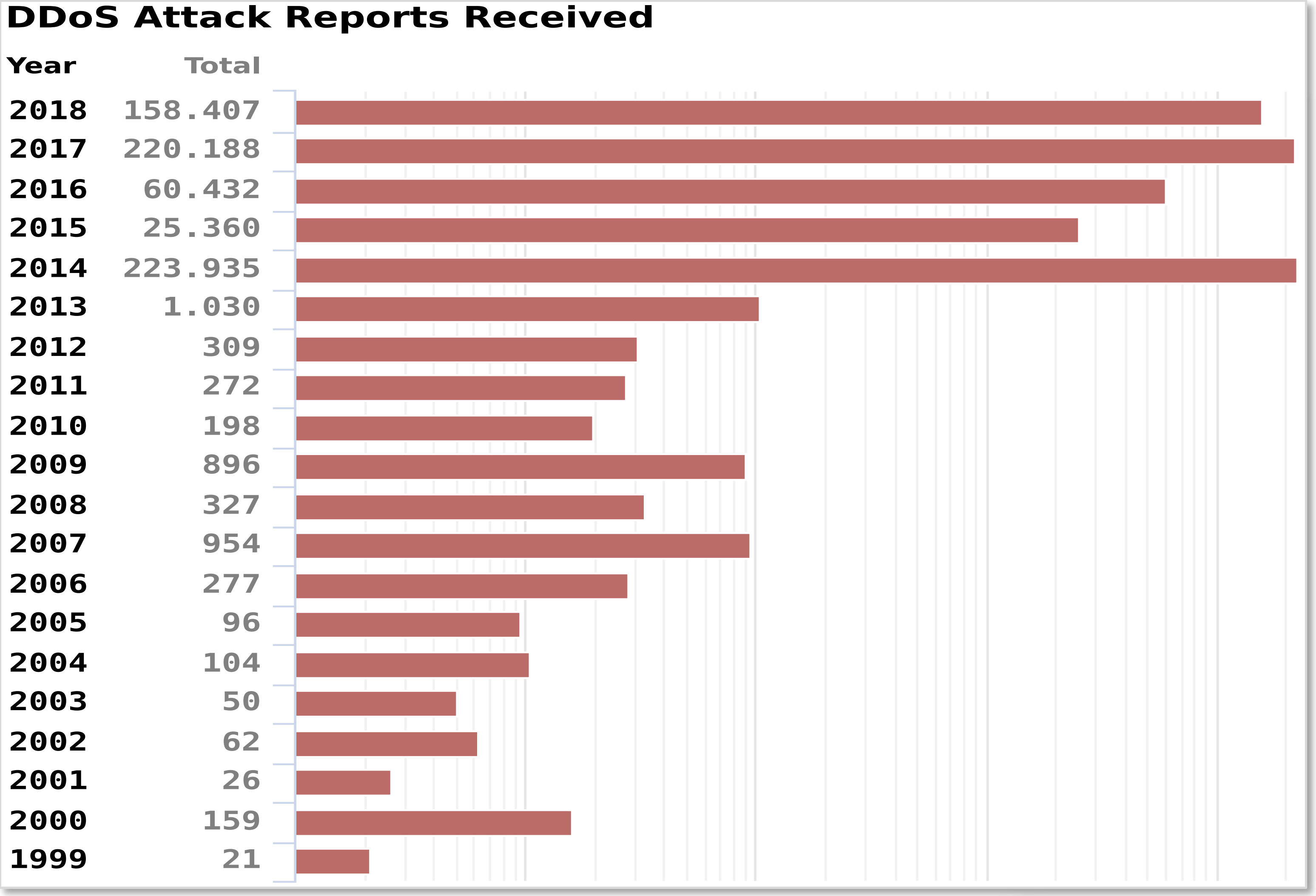
Mission

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

Focus of the Activities

- National focal point for security incident reports
- Support technical analysis and the understanding of attacks and threats
- Develop collaborative relationships with other entities
- Increase the capacity of incident detection, event correlation and trend analysis in the country
- Transfer the acquired knowledge through courses, best practices and awareness materials

Incidents Reported to CERT.br:
DDoS notifications – history



DDoS Attack Reports Received

Year	Total
2018	158.407
2017	220.188
2016	60.432
2015	25.360
2014	223.935
2013	1.030
2012	309
2011	272
2010	198
2009	896
2008	327
2007	954
2006	277
2005	96
2004	104
2003	50
2002	62
2001	26
2000	159
1999	21

Brazilian ISPs Ecosystem

Cetic.br National ISPs Survey

- Total ISPs (estimated): 6618
- Respondents: 2177
- 75% have 1000 clients or less

https://www.cetic.br/pesquisa/provedores/

IX.br SP

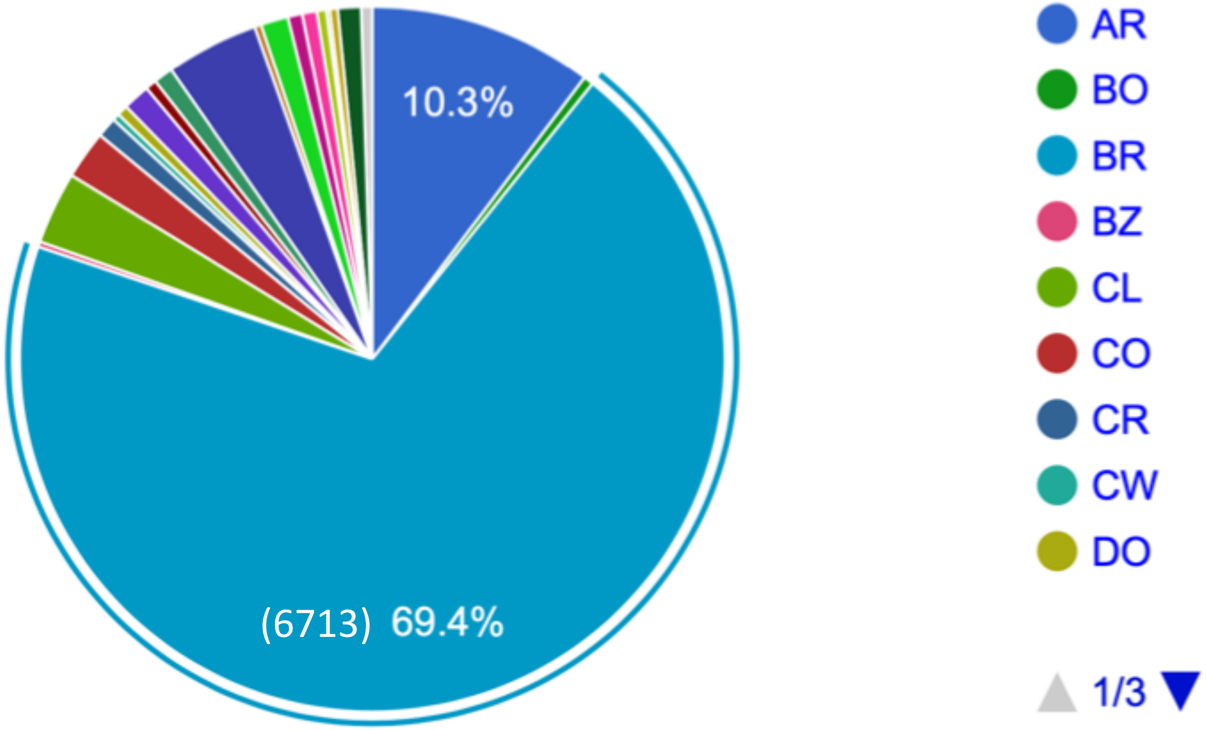
One of the biggest in the world

- #1 in participants (1467)
- #3 in traffic – both average (3.5T) and peak (5.1T)

https://www.pch.net/ixp/dir

≈700 ASes use MikroTik as core router

LACNIC ASN Allocation Stats



http://www.lacnic.net/en/web/lacnic/estadisticas-asignacion

We need a healthier ecosystem:
National Initiative – A More Secure Internet Program

Objectives:

- Reduce Denial of Service attacks originating in Brazilian networks
- Reduce the Prefix Hijacking, Route Leak, and IP Spoofing
- Reduce the vulnerabilities and configuration failures in network elements
- Create a culture of security

Incentive to adopt best practices:

- Hardening
- Close open services
- Routing Security
- Anti-spoofing (BCP 38)

Joint initiative:

- NIC.br/CGI.br, ISOC and ISPs, Hosting and Telco Associations

https://bcp.nic.br/i+seg

PROGRAMA INTERNET +SEGURA

PRINCIPAIS PROBLEMAS DE SEGURANÇA NA INFRAESTRUTURA DA INTERNET
Ataques DDoS
Sistemas mal configurados que permitem amplificação
Sequestro de prefixos
Vazamento de rotas
Ataques de força bruta
PROGRAMA POR UMA INTERNET MAIS SEGURA
bcp.nic.br/i+seg
CORREÇÃO DOS PROBLEMAS
Interação com Operadoras, ISPs e outros AS
MATERIAL EDUCACIONAL E MELHORES PRÁTICAS
CRIAR CULTURA DE SEGURANÇA
PALESTRAS E CURSOS
INDICADORES DE SEGURANÇA
FILTROS NO IX.BR
PRINCIPAIS AÇÕES A SEREM ADOTADAS POR TODOS
MANRS
Hardening
Atender notificações do CERT.br

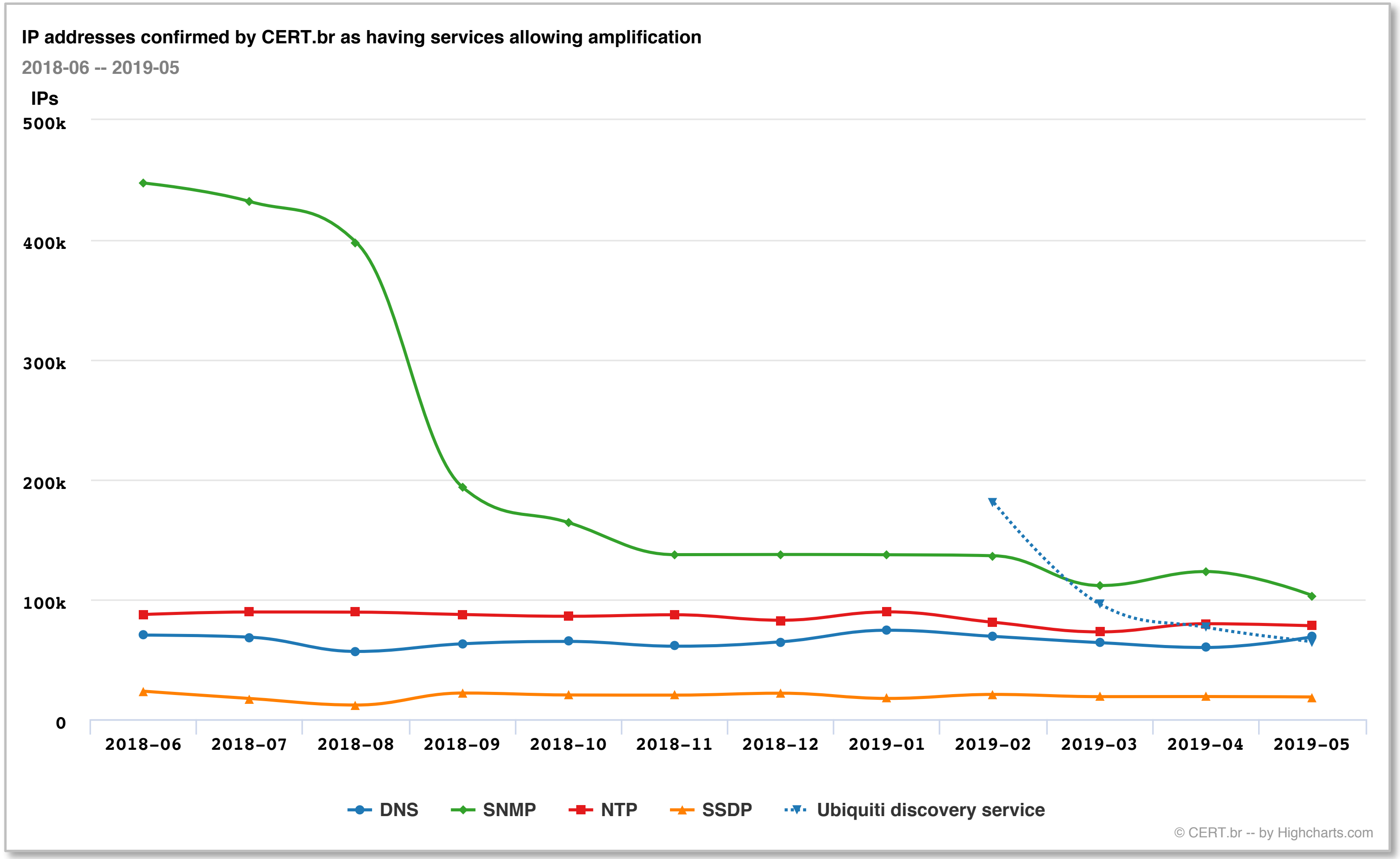
A More Secure Internet Program: Early Results – Reducing Open Services

Focusing more on the top 5:

- The top 1 (SNMP) reduced from 500K IPs to 100K
  - most in the big Telcos
- Ubiquity devices became abused recently
  - mostly on small ISPs

Common denominator in most of them:

- They are low cost CPEs (home routers)
- with bad factory defaults and do not allow changes most of the time



IP addresses confirmed by CERT.br as having services allowing amplification

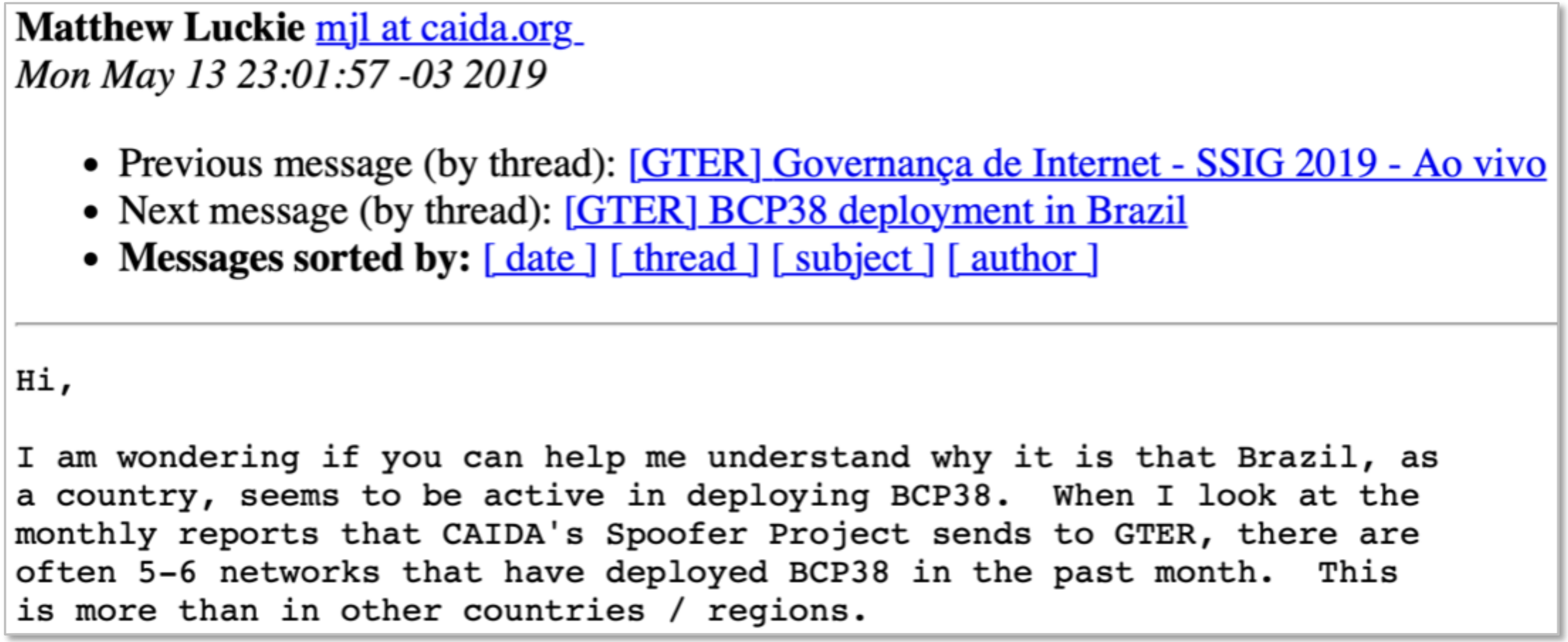
2018-06 -- 2019-05

© CERT.br -- by Highcharts.com

https://www.cert.br/stats/amplificadores/

A More Secure Internet Program:
Early Results – Antispoofing (BCP 38) Implementation

- Higher adoption than in other countries
- Noted by CAIDA Spoofer Project



Matthew Luckie mjl at caida.org
Mon May 13 23:01:57 -03 2019

- Previous message (by thread): [GTER] Governança de Internet - SSIG 2019 - Ao vivo
- Next message (by thread): [GTER] BCP38 deployment in Brazil
- **Messages sorted by:** [date] [thread] [subject] [author]

```
Hi,

I am wondering if you can help me understand why it is that Brazil, as
a country, seems to be active in deploying BCP38.  When I look at the
monthly reports that CAIDA's Spoofer Project sends to GTER, there are
often 5-6 networks that have deployed BCP38 in the past month.  This
is more than in other countries / regions.
```

https://eng.registro.br/pipermail/gter/2019-May/076685.html

Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition

Work developed by the LAC-AAWG – Latin American and Caribbean Anti-Abuse Working Group

Joint Publication of

- M^{3}AAWG - Messaging, Malware and Mobile Anti-Abuse Working Group
- LACNOG - Latin American and Caribbean Network Operators Group
- Editor: Lucimara, LAC-AAWG Chair / CERT.br

Currently available in:

- English, Japanese and Korean

New translations to be released soon:

- Portuguese, Spanish, French and German

www.lacnog.net/docs/lac-bcop-1
www.m3aawg.org/CPESecurityBP

LACNOG-M³AAWG Joint Best Current Operational Practices
on Minimum Security Requirements
for Customer Premises Equipment (CPE) Acquisition
LAC-BCOP-1

May 2019

This document is available on the LACNOG website at www.lacnog.net/docs/lac-bcop-1

This document is available on the M³AAWG website at www.m3aawg.org/CPESecurityBP

This is a joint Best Current Operational Practices (BCOP) document developed by LACNOG[1] (Latin American and Caribbean Network Operators Group) and M³AAWG[2] (Messaging, Malware and Mobile Anti-Abuse Working Group). It is the product of LACNOG's original drafts by its working groups LAC-AAWG[3] (Latin American and Caribbean Anti-Abuse Working Group) and BCOP Working Group[4], in cooperation with M³AAWG members, Senior Technical Advisors and the M³AAWG Technical Committee.

Table of Contents

[1] The Latin American and Caribbean Network Operators Group (LACNOG), https://www.lacnog.net/
[2] Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), https://www.m3aawg.org/
[3] Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG), https://www.lacnog.net/lac-aawg/
[4] LACNOG BCOP Working Group, https://www.lacnog.net/wg-bcops/

LACNOG
Latin American and Caribbean Network Operators Group
Department of Montevideo, Oriental Republic of Uruguay
www.lacnog.net

M³AAWG
Messaging, Malware and Mobile Anti-Abuse Working Group
781 Beach Street, Suite 302
San Francisco, California 94109 U.S.A. – www.m3aawg.org

Gracias!
Thank You!

www.cert.br

@ lucimara@cert.br   @certbr

August 5, 2019

nic.br   cgi.br

www.nic.br | www.cgi.br