Mapping Security Standards

Adoption in the Internet

or

The Long and Painful Path to Security

José Legatheaux Martins
Departamento de Informática da FCT/UNL

Trust and Security on the Internet

- The principles of the basic architecture of the Internet have always favoured simplicity and scalability over security

- This was a clever decision since, at that time, it prevented the adoption of wrong solutions to then poorly understood problems and technologies, which would have make the Internet architecture centralized, fragile and unable to scale and evolve.

Could it have been different?

- Public-Key Cryptosystems, the foundation of scalable decentralized security, were invented after TCP/IP was being "standardized" (late 70's - early 80´s)
- During the 90's the use of strong Symmetric Cryptosystems in the Internet was forbidden
- Cerf, V.; Kahn, R. (1974). "A Protocol for Packet Network Intercommunication". IEEE Transactions on Communications, **2** (5): 637–648.
- Vinton Cerf, Yogen Dalal, Carl Sunshine (December 1974), RFC 675, Specification of Internet Transmission Control Protocol
- Diffie, Whitfield; Hellman, Martin E. (November 1976). "New Directions in Cryptography". IEEE Transactions on Information Theory. **22** (6): 644–654
- Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM. **21** (2): 120–126.

Encryption of Content

- If used end-to-end: only the audience that knows the cryptographic keys can read the content

- If only used in parts of the transmission path: listening of the public parts of the path is made impossible

Cryptographic Signature

- Proofs the identity of the sender (proof of authenticity)

- Shows any tampering with the content

- Used with timestamp to avoid non-repudiation

Cryptosystems are at the Heart of

- Authentication of servers / entities / persons — based on public/private key pairs

- Key and other information certificates build with digital signatures - again based on public/private keys pairs

- Integrity and confidentiality of messages exchanges

Trust and Security Today

- Security mechanisms were added as needed in a continuous trial and error process
- Standardized year after year by the IETF
- Some of these standards bring new operational costs that sometimes do not immediately produce the intended results
- Thus, sometimes, progress in their deployment is disappointingly slow.

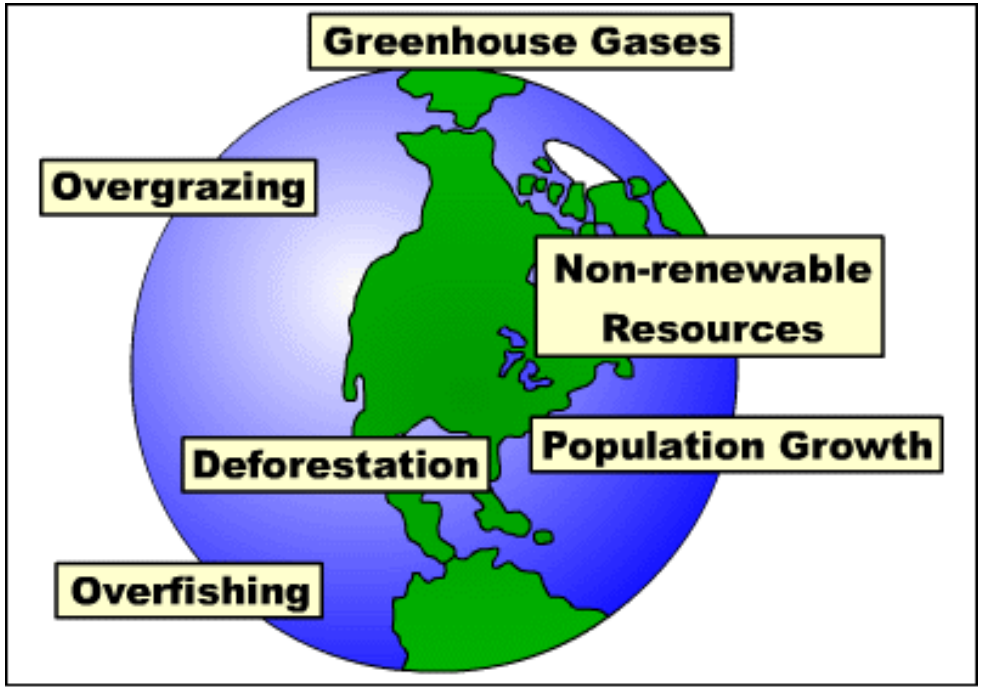
When Accessing an URL, We Must Trust

- That the DNS mapping to an IP address is genuine
- That the routing system is passing packets to the correct endpoint / interface
- That the SSL/TLS connection and the site certificate are genuine
- That the Web Public Key Infrastructure is not corrupted
- That others cannot sniff which site I am trying to access

Most Internet Actors do Not Implement all Possible Security Standards

- Does some DNS domain is secured with DNSSEC?
- Does my DNS resolution provider (resolver) implements DNSSEC?
- Does my ISP implements routing security measures?
- Do the sites I visit implement HTTPS with all up to date options and really genuine certificates?
- I am using a mail system preventing identity spoofing?

Tragedy of Commons (Garret Harding - 1968)



TRAGEDY OF THE GLOBAL COMMONS

- Security mechanisms add burden, increase operational costs and do not immediately improve providers revenues
- They are mostly a common good, and not a direct good of a specific service provider
- Unless it looses customers for not implementing them

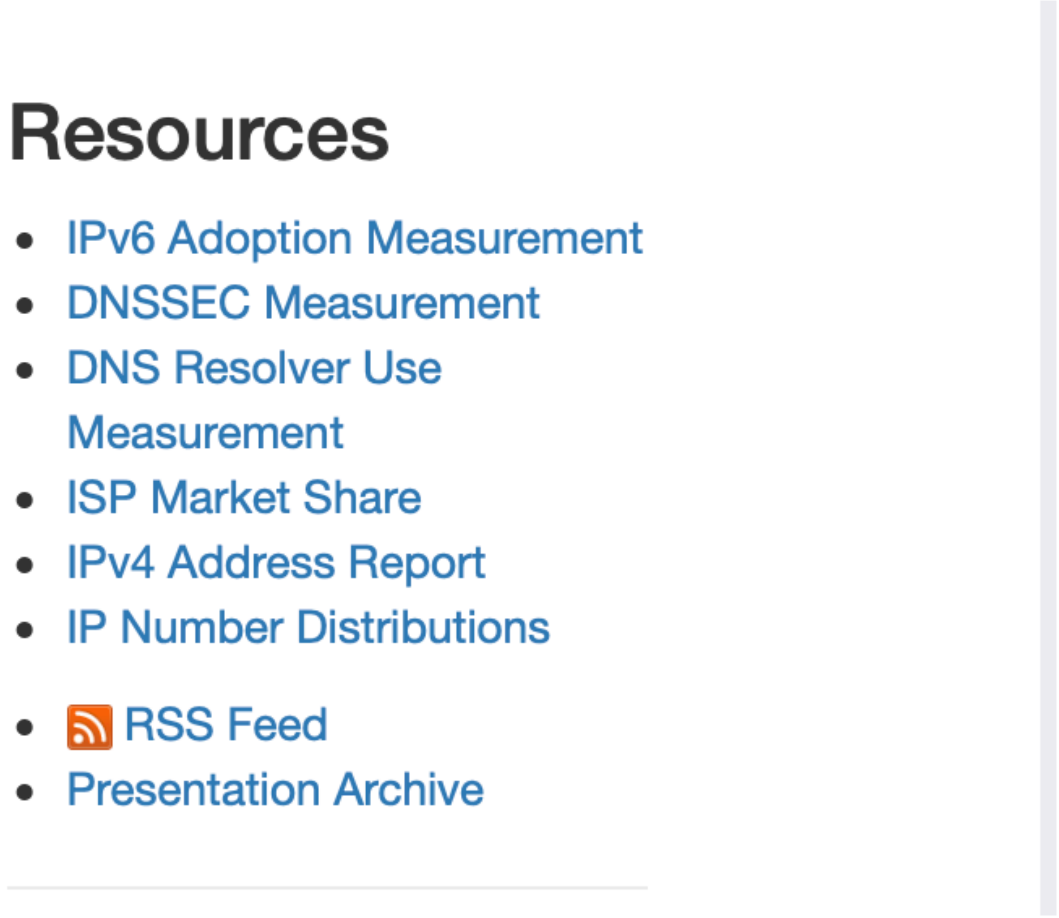
Agenda

- Mapping **Routing Security** adoption progress
- Mapping **DNSSEC validation** progress
- Mapping **HTTPS adoption** progress

APNIC Observatories

- APNIC Laboratories, lead by Geof Houston, setup an extensive Internet Monitoring Infrastructure

https://labs.apnic.net



Resources

- IPv6 Adoption Measurement
- DNSSEC Measurement
- DNS Resolver Use Measurement
- ISP Market Share
- IPv4 Address Report
- IP Number Distributions

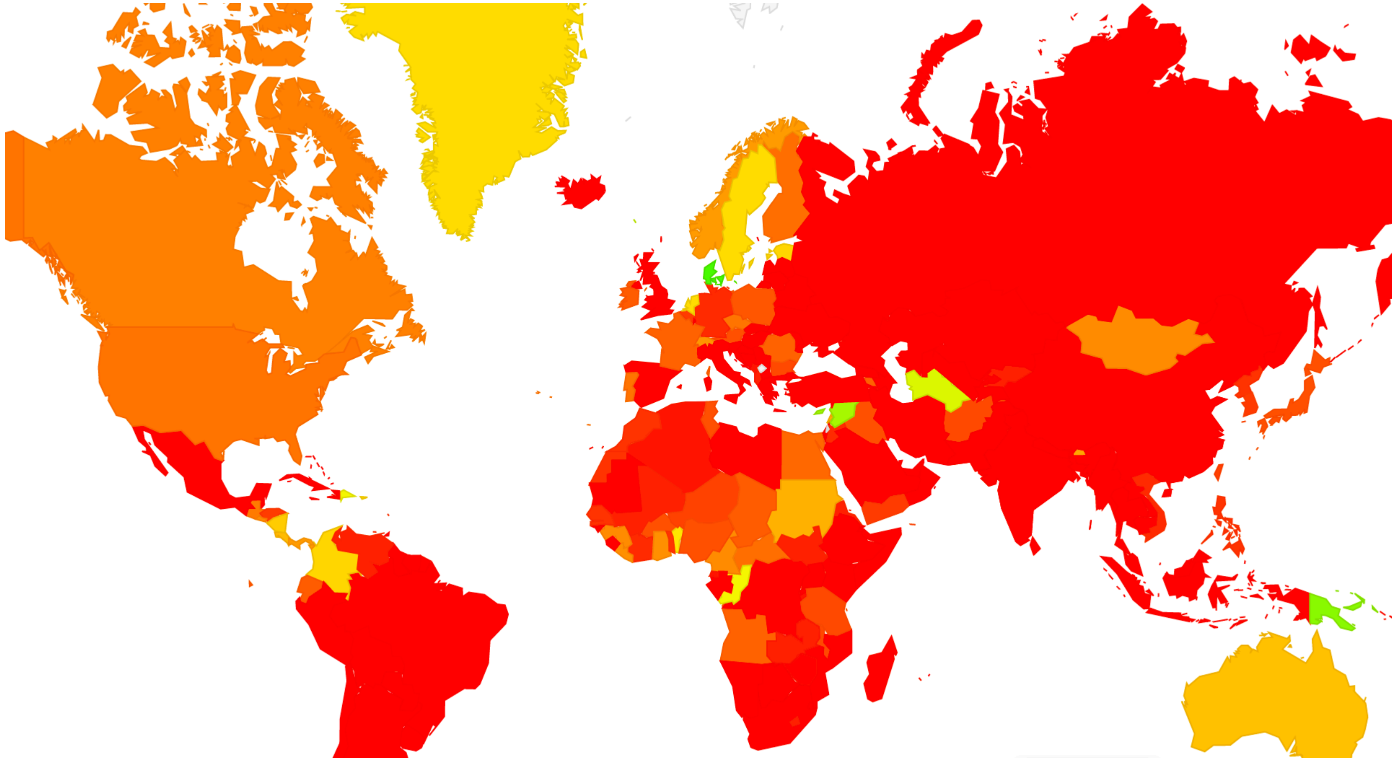
- RSS Feed
- Presentation Archive

Securing Routing

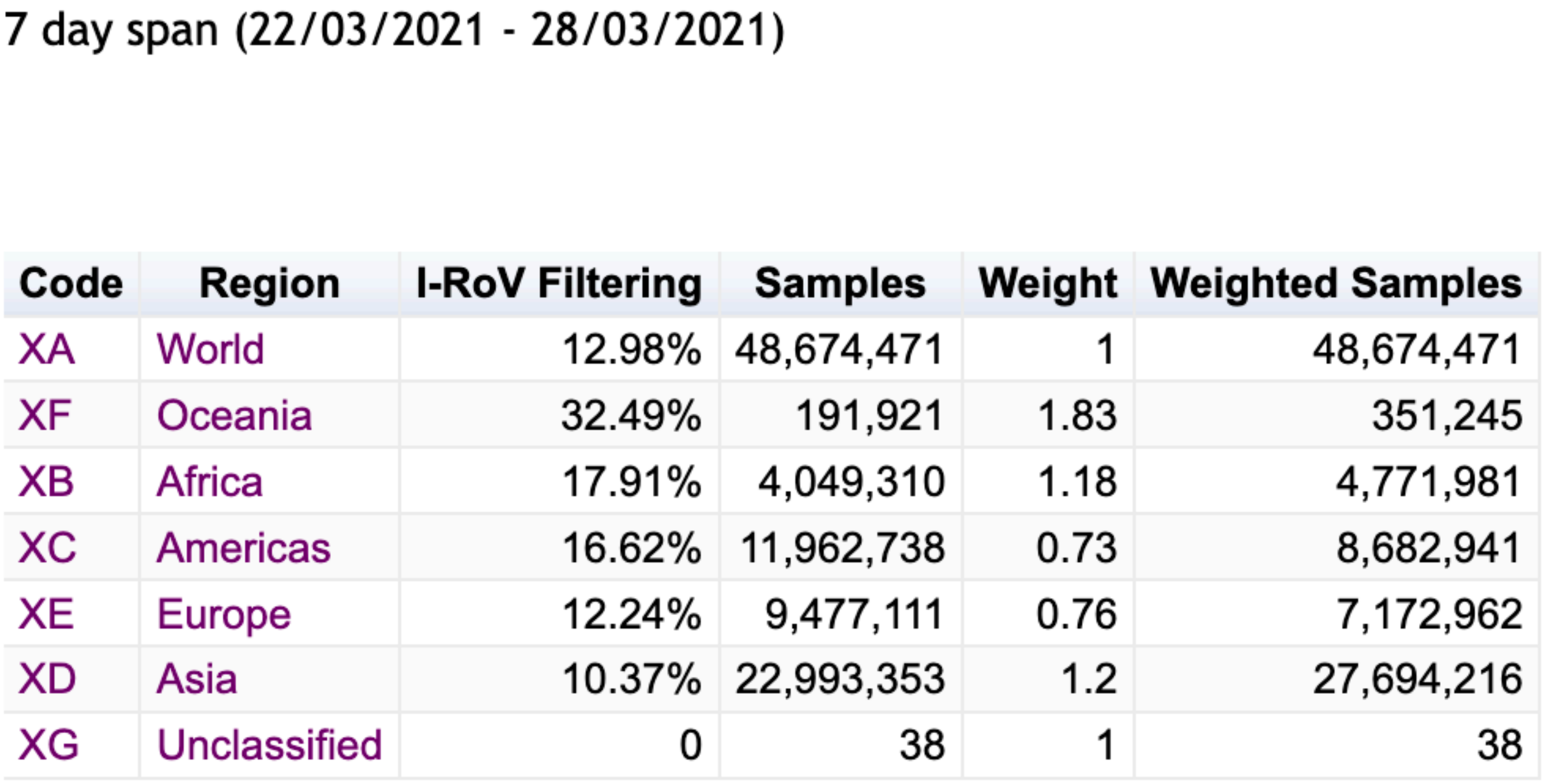
- BGP – Border Gateway Protocol – The protocol that supports routing packets in the core of the Internet. It has no security measures built in. Mostly defined in the 90's, got updates in 2006
- ROV – Route Origin Validation – It is a certificate allowing network operators to check whether an AS is allowed to originate a given route, signed by the Regional Internet Registry
- RPKI – Resource Public Key Infrastructure – the set of mechanisms used to issue and validate ROVs

Route Origin Validation Worldwide

- Regional NICs assign ranges of IP addresses to Networks
- Owners of IP address ranges can publish certificates of the valid routes they can originate
- Thus, core routers of the Internet can check if the routes they receive were originated by the owners of the announced IP addresses
- This is a step in a good direction since BGPSEC, which fully authenticate routes, is not yet a realistic alternative



Route Origin Validation (ROV) Worldwide

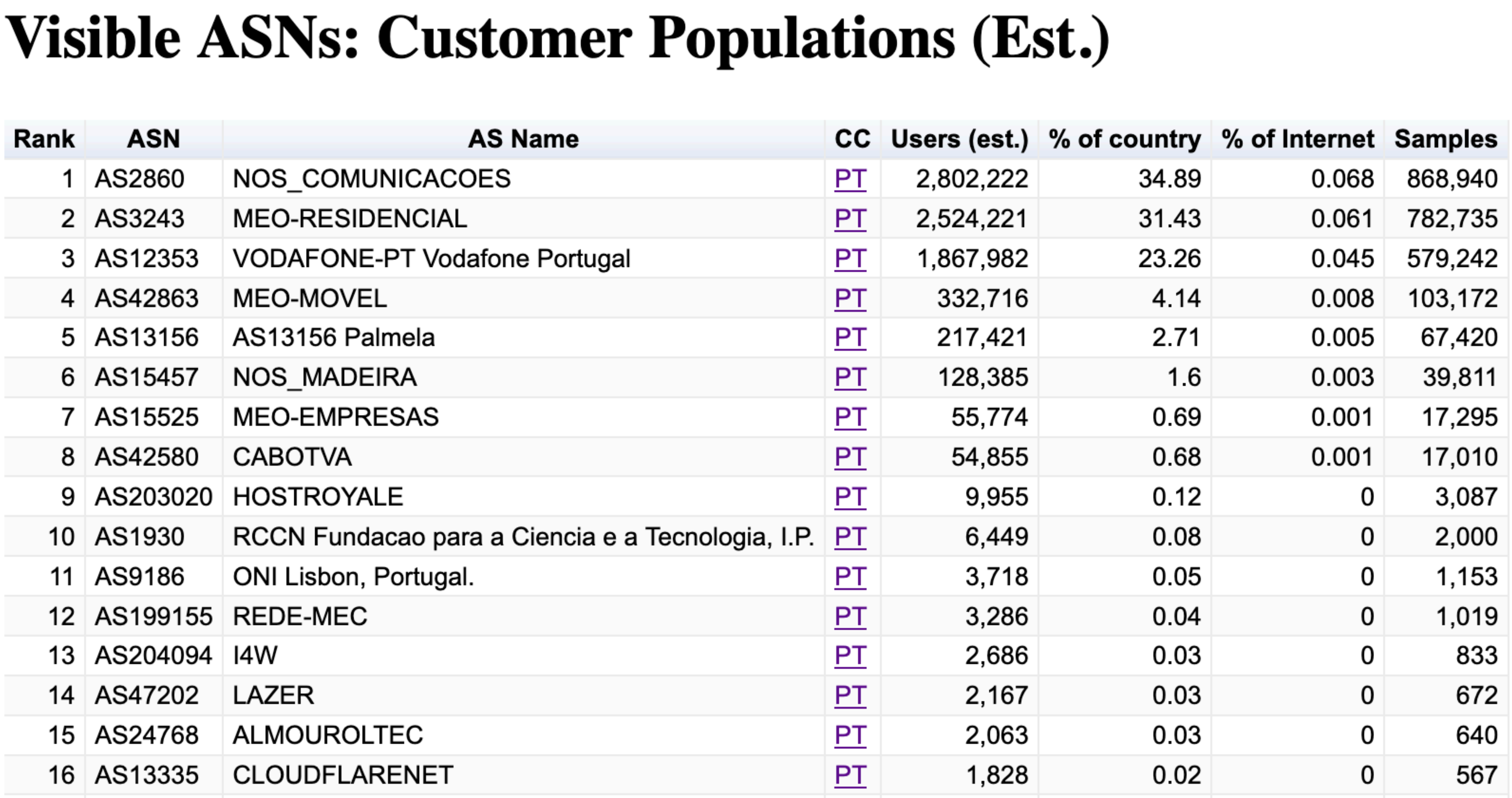


7 day span (22/03/2021 - 28/03/2021)

Code	Region	I-RoV Filtering	Samples	Weight	Weighted Samples
XA	World	12.98%	48,674,471	1	48,674,471
XF	Oceania	32.49%	191,921	1.83	351,245
XB	Africa	17.91%	4,049,310	1.18	4,771,981
XC	Americas	16.62%	11,962,738	0.73	8,682,941
XE	Europe	12.24%	9,477,111	0.76	7,172,962
XD	Asia	10.37%	22,993,353	1.2	27,694,216
XG	Unclassified	0	38	1	38

BGP Prefix Origin Validation – RFC 6811 was published in 2013

Dimension of Autonomous Systems in PT

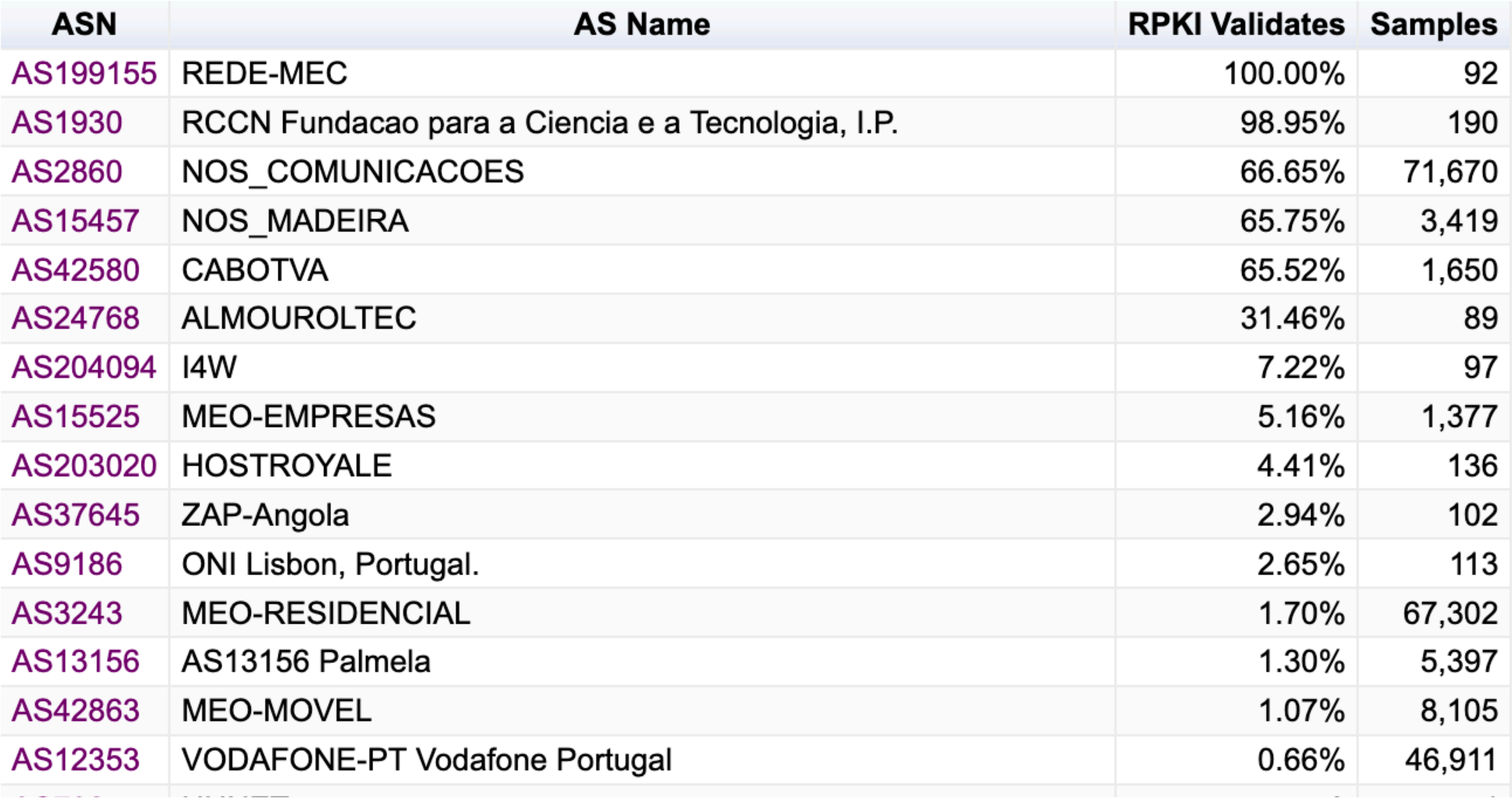


Visible ASNs: Customer Populations (Est.)

Rank	ASN	AS Name	CC	Users (est.)	% of country	% of Internet	Samples
1	AS2860	NOS_COMUNICACOES	PT	2,802,222	34.89	0.068	868,940
2	AS3243	MEO-RESIDENCIAL	PT	2,524,221	31.43	0.061	782,735
3	AS12353	VODAFONE-PT Vodafone Portugal	PT	1,867,982	23.26	0.045	579,242
4	AS42863	MEO-MOVEL	PT	332,716	4.14	0.008	103,172
5	AS13156	AS13156 Palmela	PT	217,421	2.71	0.005	67,420
6	AS15457	NOS_MADEIRA	PT	128,385	1.6	0.003	39,811
7	AS15525	MEO-EMPRESAS	PT	55,774	0.69	0.001	17,295
8	AS42580	CABOTVA	PT	54,855	0.68	0.001	17,010
9	AS203020	HOSTROYALE	PT	9,955	0.12	0	3,087
10	AS1930	RCCN Fundacao para a Ciencia e a Tecnologia, I.P.	PT	6,449	0.08	0	2,000
11	AS9186	ONI Lisbon, Portugal.	PT	3,718	0.05	0	1,153
12	AS199155	REDE-MEC	PT	3,286	0.04	0	1,019
13	AS204094	I4W	PT	2,686	0.03	0	833
14	AS47202	LAZER	PT	2,167	0.03	0	672
15	AS24768	ALMOUROLTEC	PT	2,063	0.03	0	640
16	AS13335	CLOUDFLARENET	PT	1,828	0.02	0	567

4 ASs concentrate more than 90% users

Route Origin Validation in Portugal



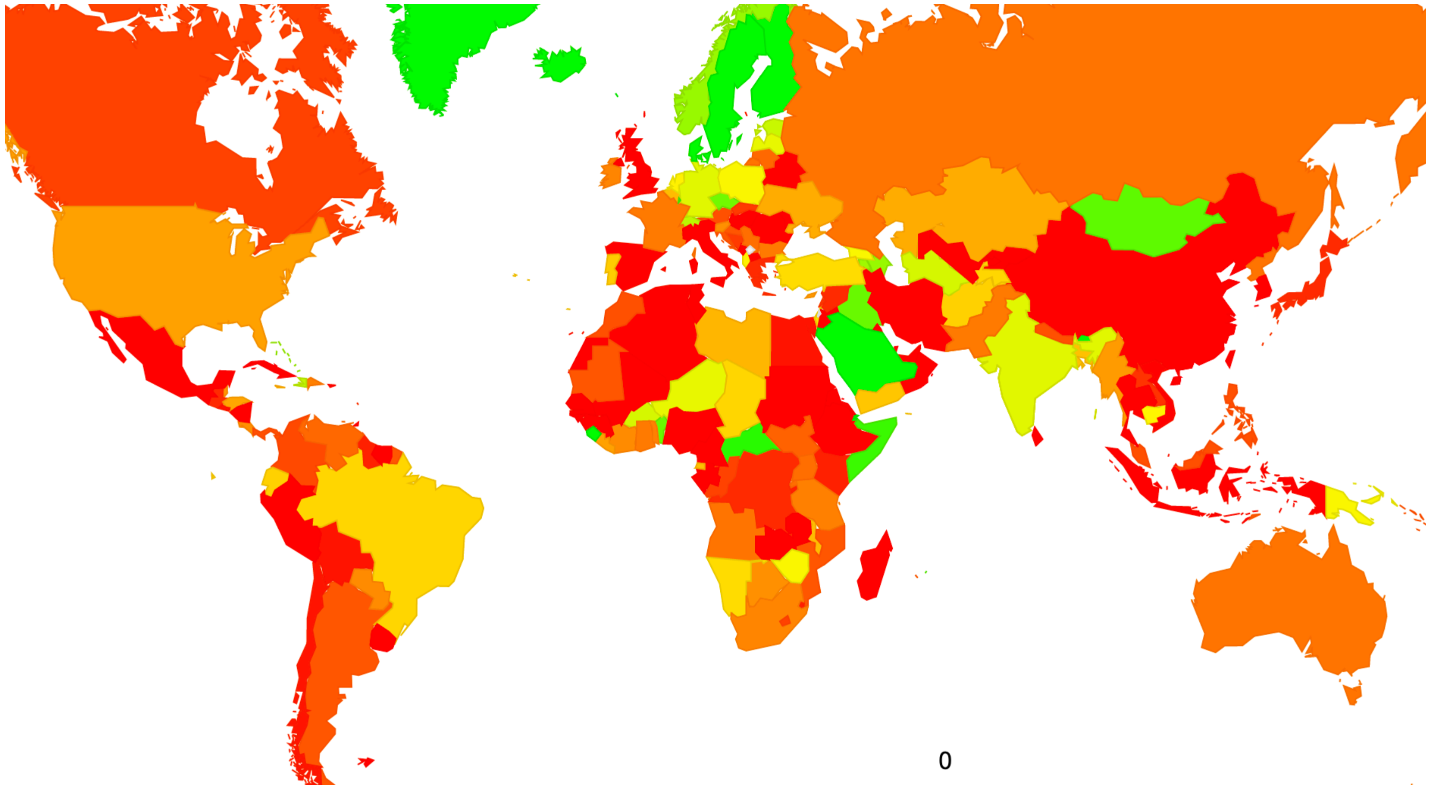
ASN	AS Name	RPKI Validates	Samples
AS199155	REDE-MEC	100.00%	92
AS1930	RCCN Fundacao para a Ciencia e a Tecnologia, I.P.	98.95%	190
AS2860	NOS_COMUNICACOES	66.65%	71,670
AS15457	NOS_MADEIRA	65.75%	3,419
AS42580	CABOTVA	65.52%	1,650
AS24768	ALMOUROLTEC	31.46%	89
AS204094	I4W	7.22%	97
AS15525	MEO-EMPRESAS	5.16%	1,377
AS203020	HOSTROYALE	4.41%	136
AS37645	ZAP-Angola	2.94%	102
AS9186	ONI Lisbon, Portugal.	2.65%	113
AS3243	MEO-RESIDENCIAL	1.70%	67,302
AS13156	AS13156 Palmela	1.30%	5,397
AS42863	MEO-MOVEL	1.07%	8,105
AS12353	VODAFONE-PT Vodafone Portugal	0.66%	46,911

DNSSEC Deployment Worldwide

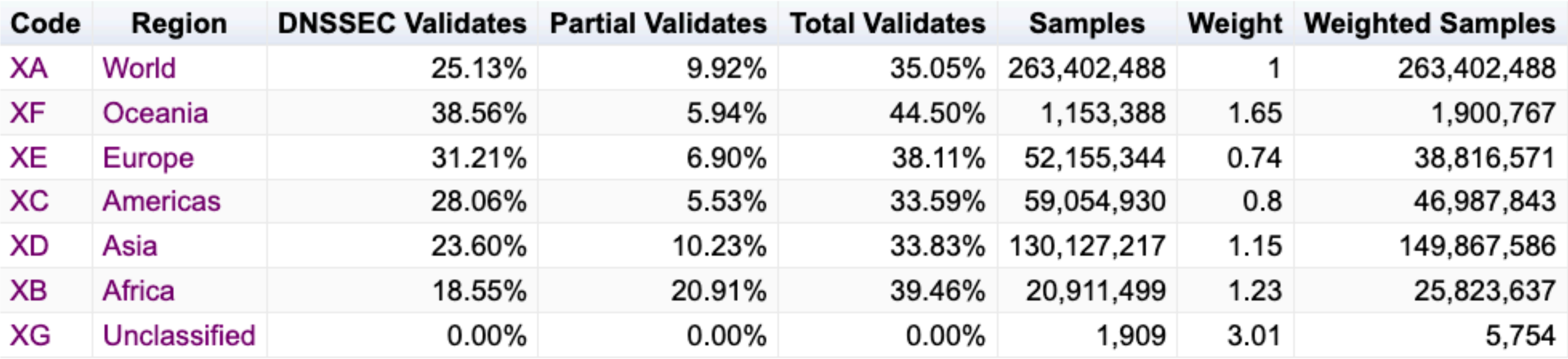
- It is easy to test if the domain name of a site is DNSSEC certified. However, one cannot easily find figures on the percentage of domain zones implementing DNSSEC
- **Of the domains ending in .PT, only around 2.75% of the (active) domains support DNSSEC**
- Anyway, for those that implement it, do end users receive the benefits of its adoption?
- In general, end-system outsource to the so-called resolvers the hard work of navigating the DNS
- Do these resolvers perform DNSSEC validation when DNSSEC information is available?

DNSSEC Validation Availability Worldwide

- Verifying all DNSSEC signatures by the end systems is not realistic. Thus, users are dependent of their resolvers providers doing it
- In this map, green countries are those where most users receive DNSSEC verified information **when it is available**

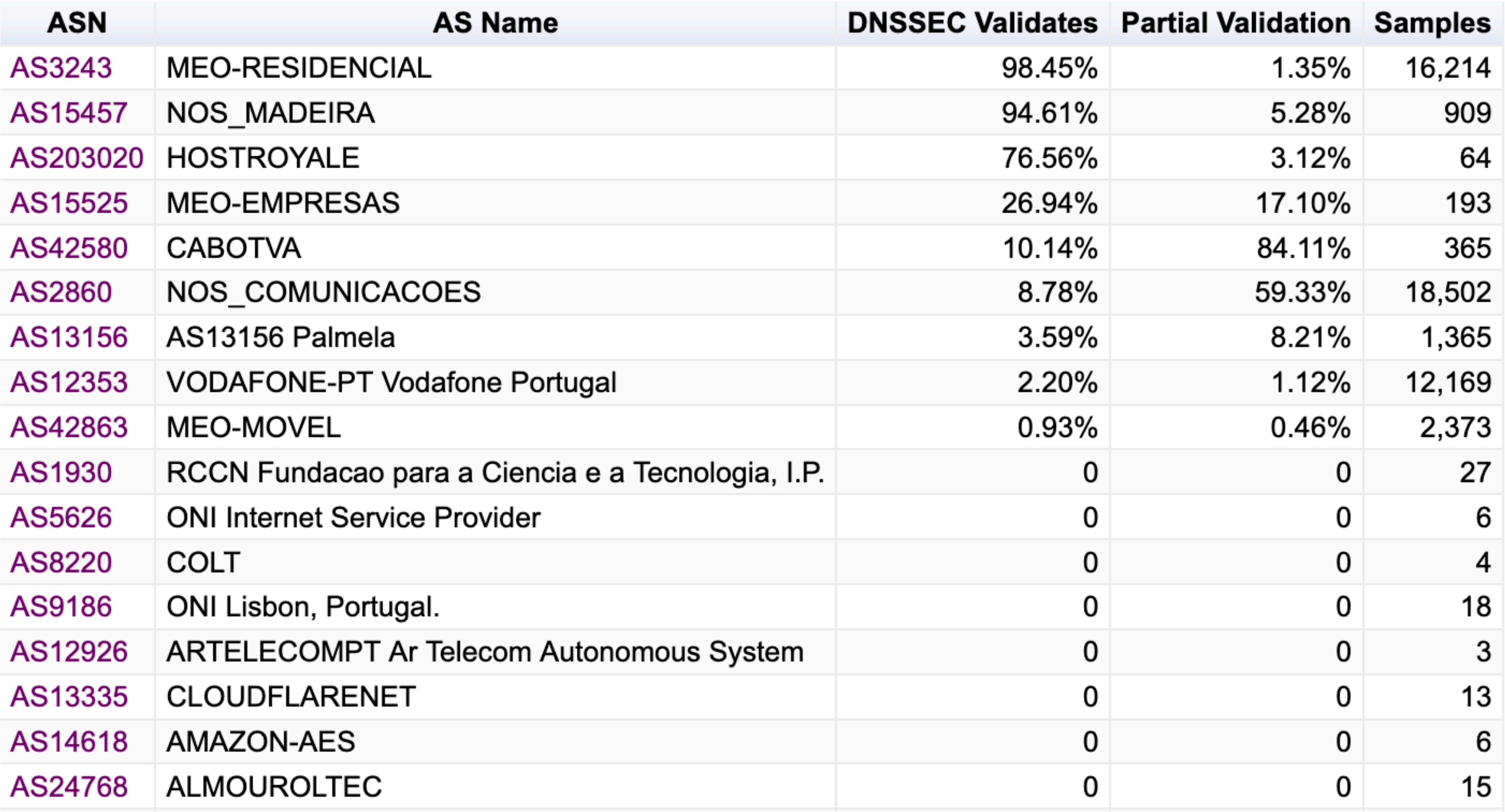


DNSSEC Validation Ratio Worldwide



Code	Region	DNSSEC Validates	Partial Validates	Total Validates	Samples	Weight	Weighted Samples
XA	World	25.13%	9.92%	35.05%	263,402,488	1	263,402,488
XF	Oceania	38.56%	5.94%	44.50%	1,153,388	1.65	1,900,767
XE	Europe	31.21%	6.90%	38.11%	52,155,344	0.74	38,816,571
XC	Americas	28.06%	5.53%	33.59%	59,054,930	0.8	46,987,843
XD	Asia	23.60%	10.23%	33.83%	130,127,217	1.15	149,867,586
XB	Africa	18.55%	20.91%	39.46%	20,911,499	1.23	25,823,637
XG	Unclassified	0.00%	0.00%	0.00%	1,909	3.01	5,754

DNSSEC Validation Ratio in Portugal



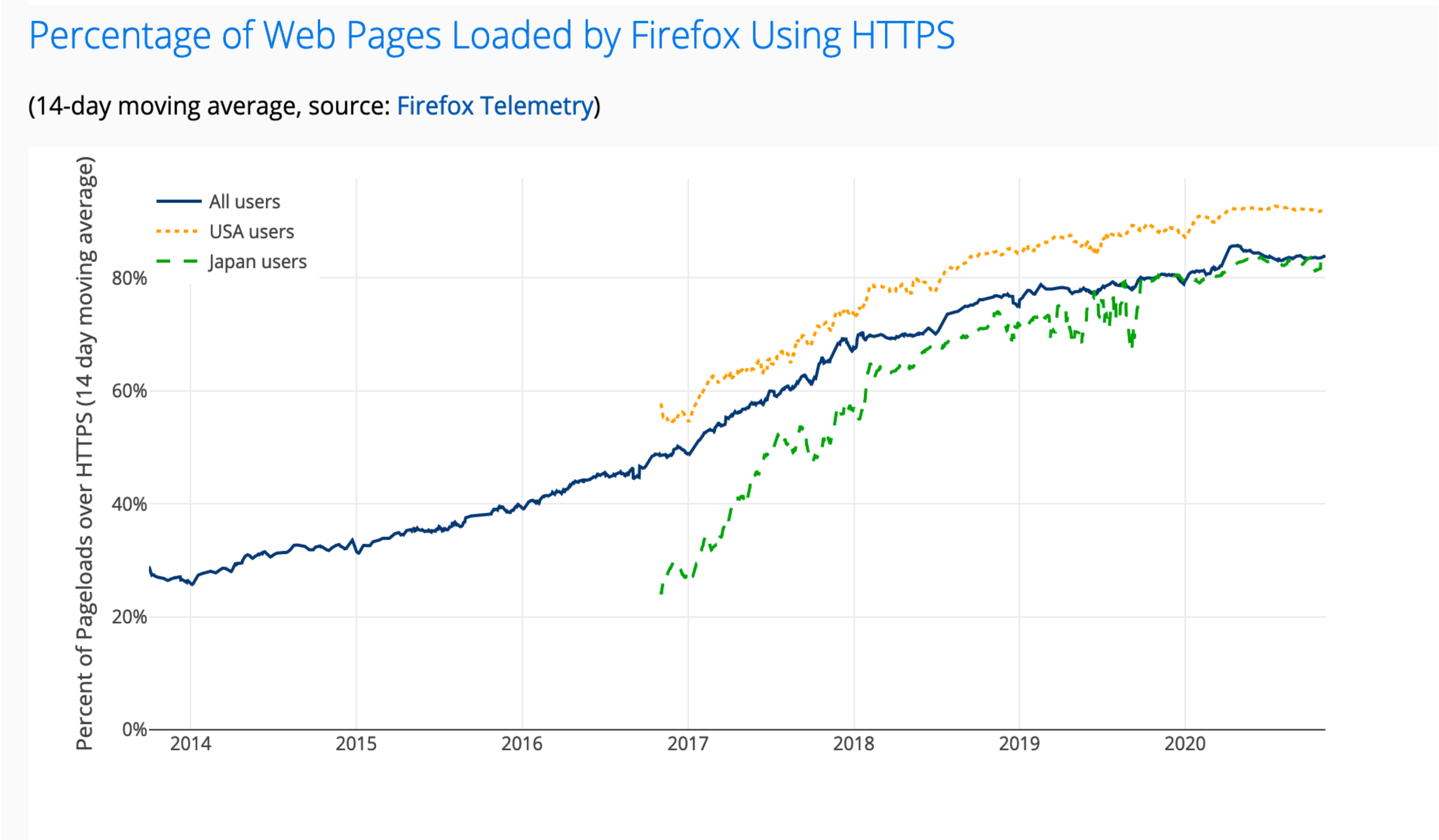
ASN	AS Name	DNSSEC Validates	Partial Validation	Samples
AS3243	MEO-RESIDENCIAL	98.45%	1.35%	16,214
AS15457	NOS_MADEIRA	94.61%	5.28%	909
AS203020	HOSTROYALE	76.56%	3.12%	64
AS15525	MEO-EMPRESAS	26.94%	17.10%	193
AS42580	CABOTVA	10.14%	84.11%	365
AS2860	NOS_COMUNICACOES	8.78%	59.33%	18,502
AS13156	AS13156 Palmela	3.59%	8.21%	1,365
AS12353	VODAFONE-PT Vodafone Portugal	2.20%	1.12%	12,169
AS42863	MEO-MOVEL	0.93%	0.46%	2,373
AS1930	RCCN Fundacao para a Ciencia e a Tecnologia, I.P.	0	0	27
AS5626	ONI Internet Service Provider	0	0	6
AS8220	COLT	0	0	4
AS9186	ONI Lisbon, Portugal.	0	0	18
AS12926	ARTELECOMPT Ar Telecom Autonomous System	0	0	3
AS13335	CLOUDFLARENET	0	0	13
AS14618	AMAZON-AES	0	0	6
AS24768	ALMOUROLTEC	0	0	15

Transport Layer Security Adoption

HTTPS / TLS / Deployment
for the WEB and Email Servers

Percentage of Pages Loaded Using HTTPS

Source: https://letsencrypt.org/stats/



Percentage of Web Pages Loaded by Firefox Using HTTPS

(14-day moving average, source: Firefox Telemetry)

Devil is in the Details (of HTTPS)

- Does the site **redirects** HTTP requests to HTTPS?
- Does the site has a **HSTS** (always forcing HTTPS) Policy?
- Does the site only uses TLS **safe versions**?
- Do the recommended **security HTTP headers** are present?
- Is the site public key (**certificate) and** the chain of certificates **valid?**
- *As well as:*
  - Does the site supports **DANE** (DNS Based Authentication of Named Entities – Requires DNSSEC)?
  - Does the server supports ***OCSP stapling*** (presenting short term certification of his certificate validity state)?

Devil is in the Details (of SMTP)

- Does the email domain has **SPF** (Sender Policy Framework) support **DKIM** (Domain Keys Identified Email) and **DMARK** (Domain-based Message Authentication, Reporting and Conformance)?
- Does the email server only uses safe TLS (or SSL) ***safe versions?***
- Is the site public key (**certificate)** **and** the chain of certificates **valid?**
- *As well as:*
  - Does the server supports **DANE** (DNS Based Authentication of Named Entities – Requires DNSSEC)?
  - SPF, DKIM and DMARK information are published on the DNS and are only full proof if the domain supports DNSSEC

WEB and Email Security Observatories

Examples of observatories and tools that perform extensive site tests

- **Mozilla Observatory** https://observatory.mozilla.org/analyze
- **Censys** https://censys.io
- https://internet.nl
- **Webcheck** https://webcheck.pt
- And several others

Analysis of Portuguese Web Providers

- Most small and medium users contract their web presence with a hosting provider that provides the management of their DNS, Web server and email service
- The way services are implemented by these providers has an huge impact on the security adoption rate by companies
- This study encompasses 6 of the todays Top 10 registrars of the .PT domain
- By 2019, 4 of these providers managed at least 50000 domains

Web Hosting Highest Security Level Provided

Fornecedor de serviços	IPv6	DNSSEC	HTTPS available	TLS characteristics	Internet.nl evaluation
PTISP	X	X	Yes	Partial	34%
AMEN	X	X	Yes	Partial	32%
DOMINIOS	X	Yes	Yes	Yes	76%
OVH	Yes	Yes	Yes	Partial	94%
SAMPLING	X	Yes	Yes	Partial	66%
WEBSP	X	X	Yes	Partial	32%

A More detailed View

Fornecedor de serviços	HTTPS redirect	HSTS	HTTPS characteristics	HTTP security headers	DANE	Validity of the certificate	OCSP stapling
PTISP	X	X	Partial	X	X	Yes	Partial
AMEN	Yes	X	Partial	X	X	Yes	Partial
DOMINIOS	Yes	X	Yes	X	X	Yes	Yes
OVH	Yes	X	Partial	X	X	Yes	Partial
SAMPLING	Yes	X	Partial	X	X	Yes	Yes
WEBSP	Yes	X	Partial	X	X	Yes	Yes

Mail Service Highest Security Level Provided

Fornecedor de serviços	IPv6	DNSSEC	SPF, DKIM, DMARC	TLS support	DANE	Internet.nl evaluation
PTISP	Yes	X	Partial	Partial	X	44%
AMEN	X	X	X	Partial	X	35%
DOMINIOS	X	Yes	X	Partial	X	65%
OVH	X	X	X	Partial	X	47%
SAMPLING	X	Yes	Partial	Partial	X	64%
WEBSP	X	X	Partial	Partial	X	42%

High Level Official Sites Security Level Assessment

Site	IPv6	DNSSEC	HTTPS available	TLS characteristics	Internet.nl evaluation
OVH	Yes	Yes	Yes	Partial	94%
presidencia.pt	X	Yes	X	X	37%
ministeriopublico.pt	X	X	Yes	Partial	27%
portugal.gov.pt	X	Yes	Yes	Partial	76%
sg.mai.gov.pt	X	X	Yes	Partial	37%
seg-social.pt	X	X	Yes	Partial	32%
parlamento.pt	X	Yes	Yes	Partial	58%

High Level Official Sites Security Level Assessment

Site	IPv6	DNSSEC	HTTPS available	TLS characteristics	Internet.nl evaluation
OVH	Yes	Yes	Yes	Partial	94%
www.tribunalconstitucional.pt	X	X	Yes	Partial	27%
cne.pt	X	X	X	X	6%
inem.pt	X	Yes	Yes	Partial	68%
covid19.min-saude.pt	X	X	Yes	Partial	39%
sns.gov.pt	X	X	Yes	Partial	32%
www.min-edu.pt	X	X	X	X	21%

Some Commercial Sites Security Assessment

Site	IPv6	DNSSEC	HTTPS available	TLS characteristics	Internet.nl evaluation
OVH	Yes	Yes	Yes	Partial	94%
olx.pt	X	X	Yes	Partial	49%
kuantokusta.pt	X	X	Yes	Partial	47%
wook.pt	X	X	Yes	Partial	34%
custojusto.pt	Yes	X	Yes	Partial	66%
proteste.pt	X	X	Yes	Partial	47%
continente.pt	X	X	Yes	Partial	49%
leroymerlin.pt	X	X	Yes	Partial	52%
elcorteingles.pt	X	X	Yes	Partial	34%
decathlon.pt	X	X	Yes	Partial	49%

Some Commercial Mail Security Assessment

Site	IPv6	DNSSEC	SPF, DKIM, DMARC	TLS support	DANE	Internet.nl evaluation
SAMPLING	X	Yes	Partial	Partial	X	64%
olx.pt	Yes	X	Yes	Partial	X	75%
proteste.pt	X	X	Partial	Partial	X	55%
continente.pt	X	X	Partial	Partial	X	56%
decathlon.pt	Yes	X	Partial	Partial	X	60%
continente.pt	X	X	Partial	Partial	X	56%

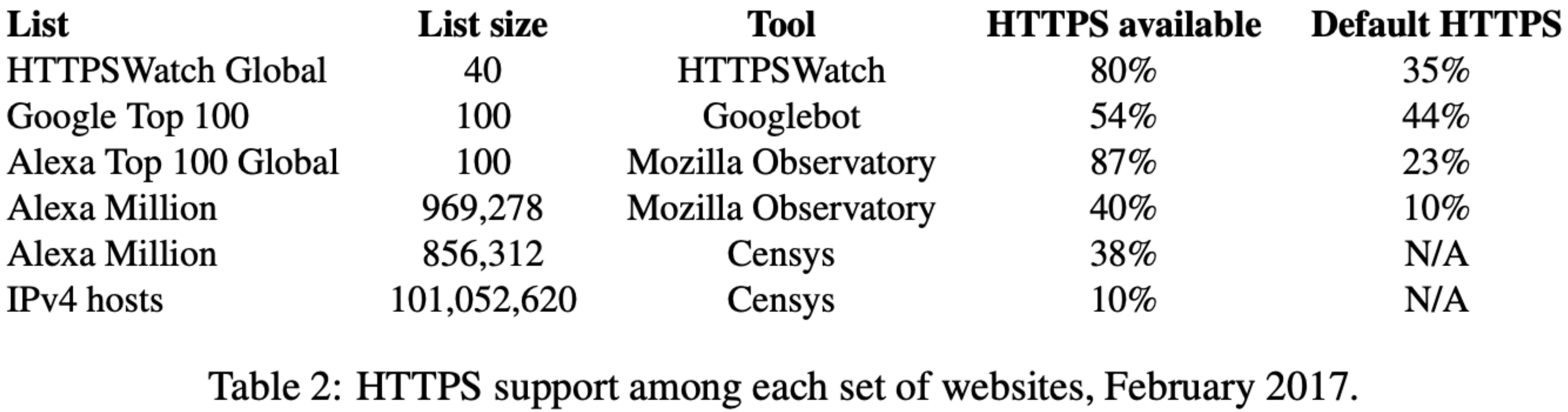
Conclusions

- Security and trust imply the generalized adoption of security open standards
- Fully deploying these standards add burden, increase operational costs and do not immediately improve revenues (or impact in the public perception of a brand)
- This may explain their slowly adoption rate
- Public ignorance of the real adoption status may also help to increase the rate of adoption
- Allowing users to have a more informed picture of the situation may improve the rate of adoption

Some University Sites

Site	Score	IPv6	DNS-SEC	HTTPS redirect	HSTS	HTTPS characteristics	HTTP security headers	DANE	Validity of the certificate	OCSP stapling
UMINHO.PT	71%	X	Yes	Yes	Yes	Partial	Partial	X	Yes	X
UP.PT	47%	X	X	X	Yes	Partial	Partial	X	Yes	Yes
UNL.PT	29%	X	X	Yes	X	Partial	X	X	Yes	X
UC.PT	26%	X	X	X	X	Partial	X	X	Yes	X
UEVORA.PT	94%	Yes	Yes	Yes	X	Partial	X	X	Yes	X
ULISBOA.PT	40%	X	Yes	Yes	X	Partial	X	X	X	X

The Long Tail – HTTPS Penetration as of 2017



List	List size	Tool	HTTPS available	Default HTTPS
HTTPSWatch Global	40	HTTPSWatch	80%	35%
Google Top 100	100	Googlebot	54%	44%
Alexa Top 100 Global	100	Mozilla Observatory	87%	23%
Alexa Million	969,278	Mozilla Observatory	40%	10%
Alexa Million	856,312	Censys	38%	N/A
IPv4 hosts	101,052,620	Censys	10%	N/A

Table 2: HTTPS support among each set of websites, February 2017.

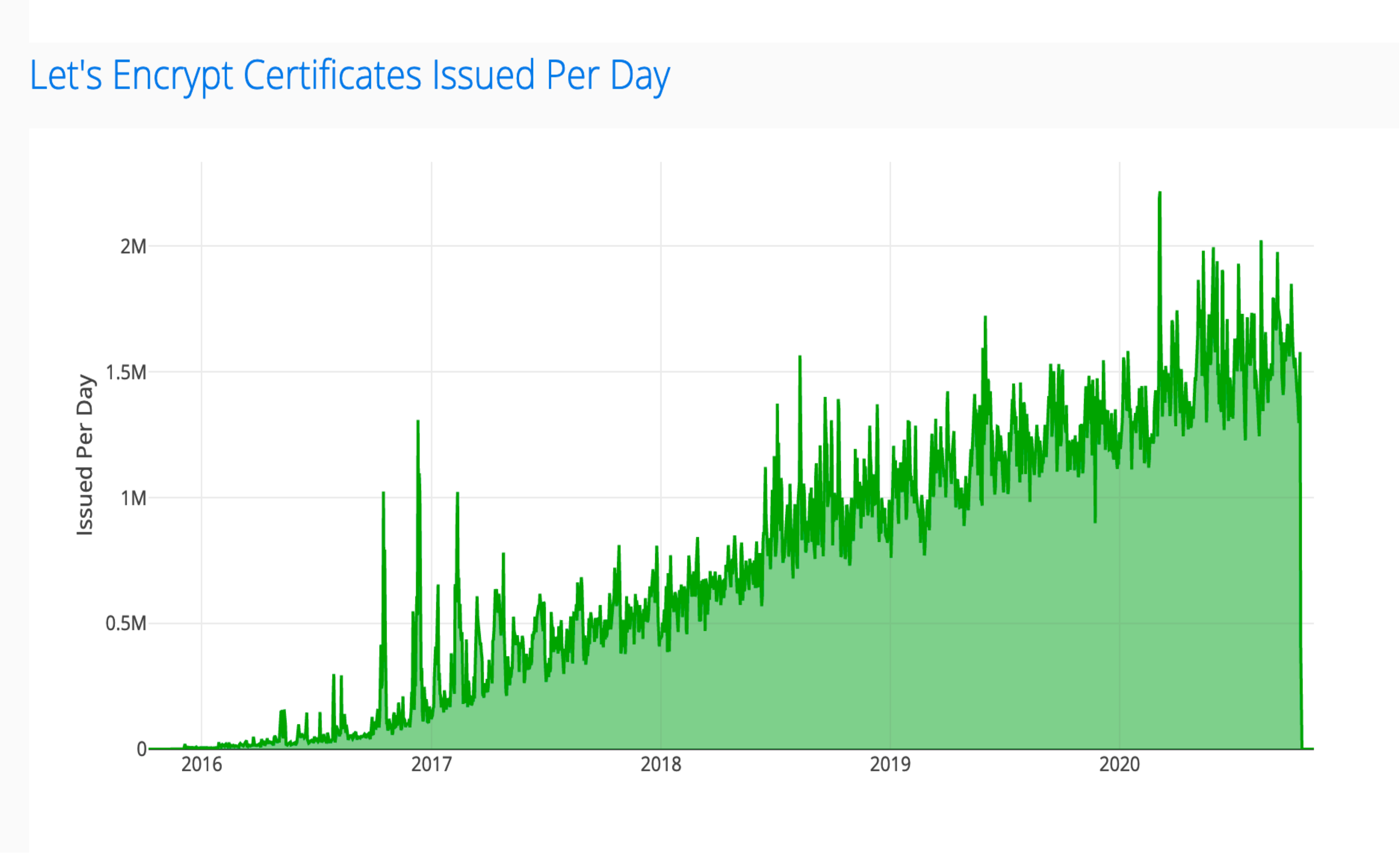
Milestones of HTTPS Adoption Progress

- By the end of 2014, most Big Names of the WEB already had support for HTTPS
- At the same time most technical details were also sorted out
- The price and complexity of getting a certificate was one of the main barriers for adoption, but Let's Encrypt (and certbot from EFF) removed that last hurdle
- From 2018 on major browsers started marking "HTTP" sites as "Not Secure"
- HTTP/2 and HTTP/3 introduce encryption by default

https://www.jefftk.com/p/history-of-https-usage

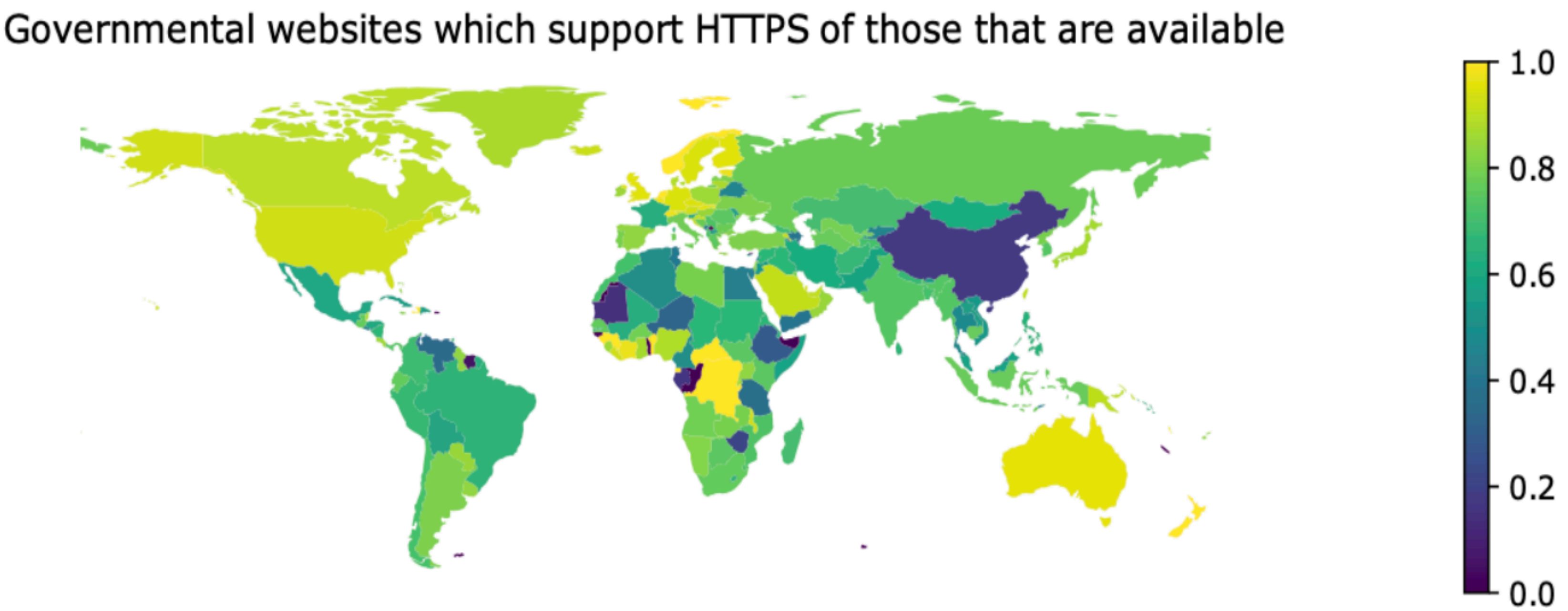
Let's Encrypt Impact

- Let's Encrypt is a fully automated Certificate Authority that issues free short-lived site certificates.
- Some researchers think that the proof of possession of such certificates may be more easily circumvented.



Example of the Long Tail – Governmental Sites

Percentage of visible governmental websites which support HTTPS of those that are available (made using a hand crafted set of governmental sites)

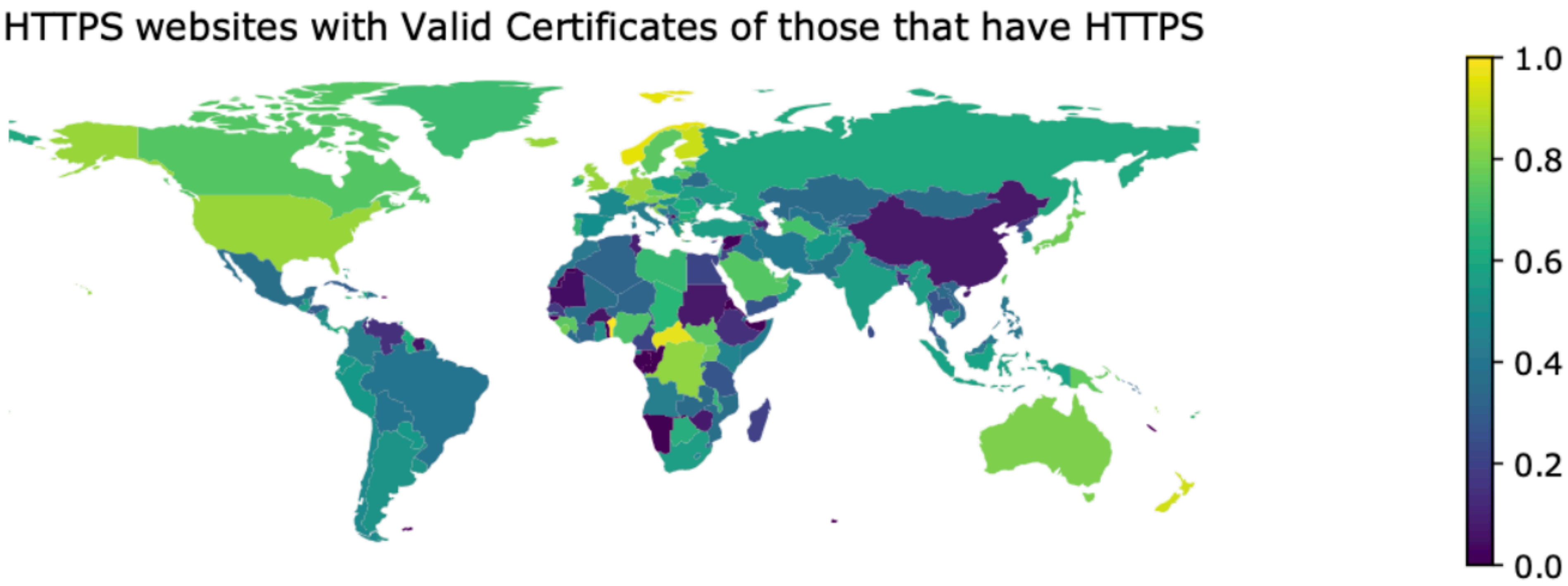


Governmental websites which support HTTPS of those that are available
1.0
0.8
0.6
0.4
0.2
0.0

Source: https://blog.sudheesh.info/docs/2020-10-06-measuring-the-adoption-https-governments/

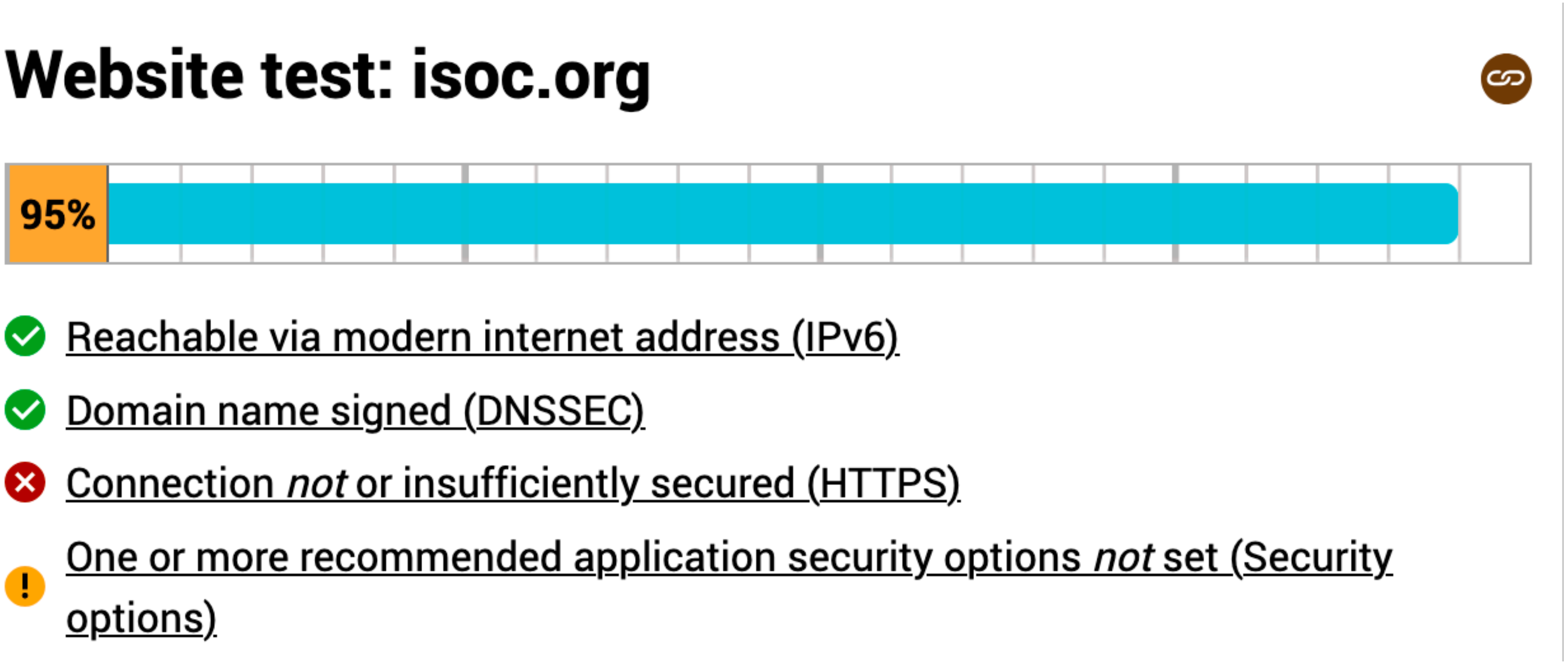
Support of Basic HTTPS is Not Enough

Percentage of governmental websites with valid certificates of those that have HTTPS


HTTPS websites with Valid Certificates of those that have HTTPS
1.0
0.8
0.6
0.4
0.2
0.0

Source: https://blog.sudheesh.info/docs/2020-10-06-measuring-the-adoption-https-governments/

By Contrast



Website test: isoc.org

95%

✓ Reachable via modern internet address (IPv6)

✓ Domain name signed (DNSSEC)

✗ Connection *not* or insufficiently secured (HTTPS)

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

https://blog.sudheesh.info/docs/2020-10-06-measuring-the-adoption-https-governments/