The Internet Protocol Journal

July 2019 Volume 22, Number 2

*A Quarterly Technical Publication for Internet and Intranet Professionals*

## In This Issue



You can download IPJ back issues and find subscription information at:
**www.protocoljournal.org**

**ISSN 1944-1134**

## From The Editor

Security and privacy have received much attention and treatment in this journal over the years. The original ARPANET protocol suite had few if any security features, but over time a great deal of effort has gone into retrofitting existing protocols with security and privacy features, and adding new technologies such as encryption and authentication mechanisms. In this issue we look at two areas of protocol development related to security and privacy.

The *Domain Name System* (DNS) provides a vital function for everything we do on the Internet, namely translating human-friendly names such as **google.com** to machine-friendly numbers such as **17.172.224.47** or **2001:4860:4860::8888**. A typical DNS entry not only contains the IP address for the server you are trying to reach, but also tells you how to send e-mail to that server. If you tried to contact us between May 31st and June 14th using any of our e-mail addresses such as **ipj@protocoljournal.org**, your message did not get delivered or was delayed. This happened because the DNS registrar for **protocoljournal.org** was changed and the corresponding *Mail Exchange* (MX) records were not updated accordingly. We apologize for this glitch; service has now been restored.

The topic of *DNS Privacy,* originally discussed in this journal in our March 2017 issue, has recently sparked considerable debate following the specification and deployment of *DNS over Hypertext Transfer Protocol Secure* (DoH). In our first article, Geoff Huston explains the motivations for DoH and explores its wider implications.

Routing Security is also an important component for a stable and reliable Internet. The *Mutually Agreed Norms for Routing Security* (MANRS) are a set of "best practice" operational agreements as explained in our second article, by Andrei Robachevsky.

We welcome two new sponsors of IPJ: Akamai and PKNIC. Publication of this journal is made possible by the generous support of numerous individuals and organizations. If you would like to help support IPJ, please contact us for further details. Comments, suggestions, book reviews, and articles are always welcome.

Send your messages to **ipj@protocoljournal.org**

*—Ole J. Jacobsen, Editor and Publisher*
**ole@protocoljournal.org**

# DNS Privacy and the IETF

*by Geoff Huston, APNIC*

From time to time the *Internet Engineering Task Force* (IETF) seriously grapples with its role with respect to technology relating to users' privacy. Should the IETF publish standard specifications of technologies that facilitate third-party eavesdropping on communications, or should it refrain from working on such technologies? Should the IETF take a further step and publish standard specifications of technologies that directly impede various forms of third-party eavesdropping on communications? Is a consistent position from the IETF on personal privacy preferred? Or should the IETF be as agnostic as possible and publish protocol specifications based solely on technical coherency and interoperability without particular regard to issues of personal privacy?

These are not new questions for the IETF. Going back some twenty years, the IETF was working on a standardization of a suite of media gateway protocols when the request was raised to make the protocols compliant with the US *Communications Assistance for Law Enforcement Act* (CALEA)[16]. This situation excited passions both within the IETF and in the broader circle of observers and commentators. The *Electronic Privacy Information Center* (EPIC) communicated to the IETF its position, which resonated with many IETF participants at the time: "We are writing to urge the IETF not to adopt new protocols or modify existing protocols to facilitate eavesdropping. [...] we believe that such a development would harm network security, result in more illegal activities, diminish users' privacy, stifle innovation, and impose significant costs on developers of communications."[0]. After much angst and debate, the IETF refused to act on this request, and published its position in RFC 2804: "The IETF has decided not to consider requirements for wiretapping as part of the process for creating and maintaining IETF standards."[1].

To put this situation into some context, the telephone networks that preceded the Internet typically operated under a framework of interception capability, and this capability was a mandatory requirement for licensed service operators for both their voice and data services. For the IETF to place interception capabilities out of scope for their standards work was not only a strong break from an established public carriage function, but it also threw into some confusion how vendors and operators could define an interoperable standard for interception requests. The *European Telecommunications Standards Institute* (ETSI) has evidently filled this gap with a set of standards for lawful interception[2]. However, this set of standards still presents real issues to both network operators and law enforcement agencies. One interesting approach in the New Zealand networking community was to support the development of a tool called *OpenLI*, an open source implementation of the ETSI protocols[13] for use by local network operators.

The IETF's position of refusal to standardize surveillance-enabling architecture modifications twenty years ago did not settle the matter then and hasn't settled it now. Code and standard specifications of network protocols do not necessarily usurp our laws, and code, law, and markets are all elements in a political tussle over what ultimately determines social policies and practices.

The time following the CALEA matter saw an uneasy stand-off between the IETF, as the most visible body associated with the Internet code base, and various public bodies wanting to undertake various forms of surveillance on the Internet. The situation changed in response to the revelations in the documents leaked by Edward Snowden in 2013. Snowden's disclosures of mass surveillance by the US *National Security Agency* (NSA)—evidently working in close cooperation with related agencies in Australia, the United Kingdom, and Canada—prompted the IETF to take a very strong public position in RFC 7258: "Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible."[3] This position means that the IETF has crossed into the second of the previous questions. Rather than simply refusing to work on interception technologies, as espoused in RFC 2804, this later RFC advocates that the IETF should publish standard specifications of technologies that directly impede third-party eavesdropping on communications.

It's a noble position that the IETF has taken, but it is perhaps a rather unworldly one in the light of subsequent concerns about the extent of corporate activities in this same area, activities that now have their own name: *surveillance capitalism*. The world of the Internet is now a world where surveillance dominates every aspect of its environment. The online market for goods and services is distorted by the presence of "free" products and services that are funded through a back flow of advertising revenue based on a thorough and comprehensive knowledge of individual users, gained only by using thorough and comprehensive surveillance frameworks that target every user.

The Internet is largely dominated, and indeed driven, by surveillance, and pervasive monitoring is a feature of this network, not a bug. Indeed, perhaps the only debate left today is one over the respective merits and risks of surveillance undertaken by private actors and surveillance by state-sponsored actors. The pronouncement of the IETF denouncing state-sponsored surveillance can only generate a wry smile in retrospect. Sadly, pervasive monitoring is what generates the revenue that propels today's Internet, and the IETF is a coerced fellow traveler, despite the occasional bursts of sometimes hysterical rhetoric that attempts to disavow any such relationship. We have come a very long way from this lofty moral stance on personal privacy into a somewhat tawdry and corrupted digital world, where "do no evil!" has become "don't get caught!"

It has been five years since RFC 7258 was published, and the privacy issue refuses to go away. It seems that the IETF is heading into this turgid and complex field of privacy once more, this time because of the *Domain Name System* (DNS).

## DNS Privacy

The DNS has always been a fertile field of opportunity for both surveillance and access control. The basic DNS name-resolution protocol has always worked in a totally unencrypted mode, so that queries and responses are available to any party who can see these transactions on the wire. The wire protocol has no authentication, so network actors can intercept DNS queries addressed to any IP address and provide a response in their name, while the querier may be none the wiser that this substitution has occurred. This idea may sound somewhat esoteric, but every Internet transaction starts with a DNS name-resolution query. The DNS is a timely and accurate indicator of everything we do online, and it's an entirely unprotected and open protocol. What a rich environment for a network eavesdropper! Little wonder that many service operators, and many nation states for that matter, use the DNS for all kinds of purposes relating to both surveillance and access control.

The intersection of RFC 7258 and the DNS has generated the topic of *DNS Privacy,* complete with an IETF Working Group and a worthy collection of drafts of ideas of how to improve the privacy aspects of the DNS.

The first steps in this activity were to look at the interaction between *end clients* and their chosen recursive *resolver*. This element is a critical one of the larger picture, because it is the only part of the DNS resolution service where the IP address of the end client is contained in the query. Once the query is passed within the DNS infrastructure, the query contains no direct identifying link to the client.

## Client Subnet

As an aside it is worth mentioning the *Client Subnet* extension to DNS queries and the tension between privacy and performance levers that are accessible with such end-user information leakage (RFC 7871)[4].

The rise of *Content Distribution Networks* (CDNs) and multiple points of presence has led to a technique, commonly used by Akamai today as well as some others, where the assumed geolocation of the DNS resolver posing the question is a reasonable facsimile to the location of the end client. The concurrent rise of the use of open DNS resolvers, most notably the `8.8.8.8` service from Google, negated this assumption.

In response to the frustrations on the CDN side of misdirected users and woefully inefficient content delivery, the IETF standardized a mechanism to attach the subnet of the end client to the query, RFC 7871[4].

The attachment of the client's credentials was made by using the *Extension Mechanisms for DNS* (EDNS)[17], and the idea was to put the IP address of the end client making the query (or an IP prefix) into the query that both survived recursive resolver hand-offs and could be used as a distinguishing label in local cache lookups to perform content steering via the DNS.

Semantically a bridge is being crossed here. Previously the DNS could be thought of as an invariant distributed database. No matter who posed a name query, the response was always the same. Client Subnet is an overt admission that some folks want the DNS to be inconstant, such that the value of the response may depend on the identity of the querier. More importantly, a major privacy bridge is also being crossed. Previously, authoritative name servers were not exposed to the identity of the original client making the query, because they were masked by the intermediary recursive resolvers. With Client Subnet, the authoritative server is aware of the original client. Interception and eavesdropping undertaken at the server end will enjoy a richer view of the end clients that are expressing some level of interest in the names served by this authoritative server.

Perhaps in deference to RFC 7258 it should be noted that the IETF appeared to be reluctant to reference it when specifying this Client Subnet extension, but nevertheless the organization ended up doing it! I quote here Section 2 of RFC 7871, which is a good description of the level of compromise and discomfort that lies just beneath the surface of this DNS privacy debate in the IETF:

> "If we were just beginning to design this mechanism, and not documenting existing protocol, it is unlikely that we would have done things exactly this way.
>
> The IETF is actively working on enhancing DNS privacy and the reinjection of metadata has been identified as a problematic design pattern.
>
> As noted above however, this document primarily describes existing behavior of a deployed method to further the understanding of the Internet community.
>
> We recommend that the feature be turned off by default in all nameserver software, and that operators only enable it explicitly in those circumstances where it provides a clear benefit for their clients. We also encourage the deployment of means to allow users to make use of the opt-out provided. Finally, we recommend that others avoid techniques that may introduce additional metadata in future work, as it may damage user trust.
>
> Regrettably, support for the opt-out provisions of this specification are currently limited. Only one stub resolver, *getdns*, is known to be able to originate queries with anonymity requested, and as yet no applications are known to be able to indicate that user preference to the stub resolver."[4]

### DNS over TLS

The *Transport Layer Security* (TLS) protocol can both encrypt the communication between a client and a server and provide some assurance to the client that the server is operated under the authority of the named entity that the client intended to connect to. In much the same manner as TLS is used to protect HTTP sessions and provide some assurance that the service point is an authorized agent of the named service, this protocol can also be used in the DNS context between end users' client stub resolver and their chosen recursive resolver service.

The IETF *DNS PRIVate Exchange* (DPRIVE) Working Group[12] has worked on *DNS over TLS* (DoT)[9, 10] and we are now seeing numerous DNS recursive resolver services that support DoT. Resolver code for Unbound, PowerDNS, and Knot exists, and BIND can be configured with TLS use through a *stunnel* configuration. So if you are prepared to set up your own DNS-resolution environment on your device, you can bypass the open DNS-resolution system provided by your ISP and use a DoT service that will hide your DNS queries and responses from your ISP, and any interested onlookers.

However, it has to be said that using DoT constitutes a highly qualified form of privacy. It's not a solution for everyone. Adding DoT support to your platform may require the installation of a third-party app on your device (which may or may not be possible on your device), and in any case the number of users who are willing to alter the DNS configuration of their device is very limited. Even when the packing of the TLS service is quite seamless, such as in Android Pie's DNS privacy option, it probably still will not be broadly used. In Android's case it is an esoteric feature buried a few levels deep in menus, it is not necessarily supported on all Android platforms, and unless you already know about it you will probably never stumble over it when poking around in your device.

But configuring the client is only half the story. Whom are you going to talk to? Which recursive resolvers support client connections using DoT?

It's an important question. While you are stopping others from looking over your shoulder at your online DNS activity, you are still telling your chosen DNS recursive resolver your complete DNS profile. Today, Google, Cloudflare, and Quad9 all provide open DNS resolver servers.

Sharing your secrets with Google may sound a bit like dancing with the devil. Google's advertising platform generates comprehensive user profiles and its ad support systems are certainly expert and capable practitioners of the art of surveillance capitalism!

In their defense, I must note that Google clearly states that it does not use its public DNS service to reap user profile data and it exercises strict controls over access to DNS data, but that itself raises the question of how such unilateral undertakings are enforced within the company. Google does not open itself up for any form of third-party compliance inspection. Although its DNS practice statement is an excellent statement of noble intent, how can a user be assured that Google is thoroughly and completely committed to every detail in the practice statement?

Let's look at it from the user's perspective. When you configure your system to use a third-party open DNS resolver, you may also be leaving aside your local national regulatory framework. It's a mixed package, because you may be circumventing what you might think of as onerous national content controls, including DNS censorship, but at the same time you may also be circumventing any rights and protections you may have under these same national regulatory structures. When you are outside of any national jurisdiction, then who is left to ensure that service providers adhere to their stated practices in providing the service?

It's not just trust in the service provider at the other end of the TLS connection. Even accessing such a privacy-oriented service may present a problem. In its wisdom, the IETF's DPRIVE Working Group standardized DoT over TCP port 853. This port is not port 443 as used by TLS in supporting HTTP. Any network operator can prevent users from applying this DNS overlay service by simply blocking all traffic to TCP port 853.

DNS over TLS represents a specialized service accessible to just a few. It's a service that is readily blocked. It's a service that may prevent surveillance on the wire, but still ends up sharing your DNS activity with the DoT service provider of your choice. You may well still be compromised in terms of assured privacy protection, but does it make you feel better having a choice as to which service operator you choose to expose yourself to?

### DNS over HTTPS

What caused all the current fuss in the IETF was a variant of this DoT approach, termed *DNS over Hypertext Transfer Protocol Secure* (DoH).

In terms of the carriage of DNS on the wire there is almost nothing that differs between DoT and DoH. Both take wire format DNS messages, encrypt them using TLS, and use a TCP session between the client and resolver. In protocol terms of packets on the wire the only difference between the two approaches is that DoH uses the same TCP port number as HTTPS, namely port 443. It may sound like a cosmetic change, but two very fundamental differences transcend this simple protocol tweak.

Firstly, DoH is very difficult to detect. It looks like HTTPS traffic and uses the same port as HTTPS traffic. One could make assumptions in the opening TLS handshake where the name of the server is carried in the clear, but work on encrypted *Server Name Indication* (SNI) in TLS 1.3 is proceeding, and it is reasonable to believe that even this small aperture of visibility will be sealed up in the near future. If you also add TLS padding to the mix, then even traffic profile analysis would not necessarily reveal that it is a DNS session within the TLS stream.

If privacy is the goal, then what's to complain about with this picture? Surely DoH offers the end user a package of encryption, mimicry, and obfuscation that hides the DNS to all but the endpoints of the session.

The answer to this question leads to the second fundamental difference between DoT and DoH. We are no longer talking about an esoteric feature knob that requires a knowledgeable, or even foolhardy, user to turn it on. The DNS session may look like just another HTTPS session to the network, but it also looks like just another HTTPS session to the host platform. In other words, a browser may just turn on DoH all by itself. It's not the user turning it on, nor the platform turning it on, but the browser itself. No special configuration needs to be in place by the platform of the local network to support the operation of DoH. If a browser chooses to use DoH, then there is little that the platform or the network can do to prevent it. If a browser has installed DoH support, then control over the DNS name-resolution function has passed from the user to the browser provider, and rather than being an esoteric function enabled by a handful of users, it becomes a "mainstream" service used by potentially billions of end users. For example, it appears that Google's Chrome browser enjoys a 60% market share of browsers[5]. If Chrome enabled DoH by default, then what would that mean for the entire DNS? Would it literally disappear from sight?

The second concern is the choice of DoH server. Instead of using a locally configured DNS-resolver service provided by the ISP, DoH switches the situation to use a service configured by the browser. The early implementation of this service in Firefox requires the explicit configuration of a trusted recursive resolver, in a manner similar to the configuration of the DoT server in Android Pie. What if the DoH resolver is configured by the browser by default?

Let's just pause for a second to think about this notion. DoH can place the control of the privacy setting for DNS queries into the hands of the browser, bypassing both the user and the local internet infrastructure, and can do so in a way that intertwines secure web services with secure DNS service. In privacy terms it sounds very enticing.

The downside is that the user's browser is now sharing all of its local activity with the configured DoH server. To put it a different way, what part of "sharing your entire personal profile with the browser-selected DoH server" is consistent with our traditional concepts of personal privacy and informed choice?

Consider a second concern here as well. This ability for a browser and a DoH resolver to combine and thereby effectively dominate the Internet namespace is a legitimate concern. Few companies are in such a position, but there are few companies left in the Internet ecosystem. A very small number of digital behemoths inhabits the core of the Internet, and these entities could potentially take advantage of such an opportunity, were it offered to them. Google is the dominant provider of the platform in Android, the browser in Chrome, and the DNS resolver in the `8.8.8.8` service. Would this scenario be a case of a single corporate entity being in a position of overarching control of the entire namespace of the Internet? Netflix already fielded an app that used its own DNS resolution mechanism independent of the platform upon which the app was running. What if the Facebook app included DoH? What if Apple's iOS used a DoH-resolution mechanism to bypass local DNS resolution and steer all DNS queries from Apple's platforms to a set of Apple-operated name resolvers?

We'll find out some answers to these questions in the near future. On April 9, 2019, Mozilla announced its plan to enable DoH by default in the Firefox browser[6], committing to an earlier informal description of its plans that were outlined by Mozilla's Eric Rescorla at the end of March 2019[7].

To place this announcement into a broader perspective, it should be noted that the market share of Mozilla's Firefox browser, while large, is by no means dominant. The StatCounter site reported a market share of 4.69% for Firefox in March 2019[5], so these moves by Mozilla are not intrinsically all that significant in terms of the profile of the larger Internet and the average Internet user. A major concern with this announcement is that the move by the Firefox browser to make DoH the default means of DNS name resolution is a precursor for similar changes to the Chrome browser. Chrome is definitely the dominant browser in today's Internet ecosystem, with some 62.63% market share according to StatCounter. If Chrome were to use a default setting that pushed all its DNS name-resolution activities to a Chrome-selected DoH server, then the implications for the DNS are very significant.

Will the other browsers follow Mozilla's lead with DoH enabled by default? The experience so far would support a "yes" answer. Browser vendors have been enthusiastic to integrate changes to their platform that decrease page load times, and they are equally keen to integrate changes that protect the browser activity against various forms of surveillance.

DoH does not necessarily make DNS resolution quicker, although it does put the browser in more control over its use of the DNS and allows the browser to control its own local DNS cache. But, of course, DoH plugs a critical DNS information leak in the current browser architecture. Third-party observers can infer browser activity by looking at the browser DNS query stream. DoH prevents any such observation in both the user's platform and the local network. So "yes" is a likely answer to this question.

Can such positions be regulated? How can we be assured that transactions that now have disappeared from sight, and from any meaningful form of oversight, are still conducted with all due integrity? We have already seen many national regimes struggle with very real questions concerning the limitations of imposing constraints on the actions of these entities. Have the concerns of the U.S. Supreme Court's Louis Brandeis in the first half of the twentieth century over the rise of industrial and financial behemoths that in his view were too big to effectively regulate at all come full circle?

### What Does DoH Mean?

Here is the core of the collective angst and disquiet in the IETF when considering the implications of DoH and the "centrality" of Internet infrastructure.

We are attempting to actively withhold the DNS from the traditional forms of inspection and interception using access carriers and wire-based mechanisms. In so doing we are looking to counter what was perceived as a state-based surveillance operation that had assumed too much capability.

But in the case of the DNS have we over-achieved? In withholding our DNS secrets from one party, have we instead handed the entire plate to another? Have we now provided the private surveillance framework with a whole new trove of personal data to mine by ruthlessly exploiting the DNS in a manner that is entirely out of sight? When the browsers and even the apps direct their name queries through encrypted channels to resolvers operated by the same browser and app providers, then have we dealt a body blow to any efforts to safeguard personal privacy on the Internet?

At least RFC 7871 on Client Subnet included an admonition to operators to turn it off and a tacit apology for specifying a tool that had serious issues relating to erosion of user privacy in the DNS infrastructure. The DoH specification in RFC 8484[11] contains no such considerations. It fails to mention the security and privacy issues if a browser invisibly co-opted the name-resolution function and passed all its DNS traffic in a secure encrypted tunnel to a cooperating resolver using DoH that faithfully mimics conventional content transactions. It fails to mention the risks of increasing the "centrality" of the Internet when the DNS name resolution is forcibly sucked into the browser and application space and then concealed behind a veil of strong encryption.

It's incredibly challenging to make the case that DoH enhances personal privacy. It probably doesn't. It's easier to sustain a case that DoH has the potential to change the parties whom you bring into your trust circle by virtue of their being privy to your private profile, and not necessarily in a good way. In and of itself such a substitution of trust should not necessarily be of concern. But now it's your browser that can make the decision as to whom you are trusting with your personal data, not you. And the parties who are looking to be your DoH trust partner are the same parties who have a direct and overbearing interest in selling you to the highest bidding advertiser.

### Privacy Undertakings

These open DNS providers appear to have a clear view of user concerns over personal privacy. Their privacy policies implicitly acknowledge that the DNS query stream could be used to provide insights into the personal profile of users and assert that they have no such intent to do so. Such noble intentions to operate a free public service and refrain from any form of monetization of the service are entirely laudable.

However, from an historical perspective these undertakings appear to be unrealistic and unsustainable. We should remember the events of a century ago with Theodore Vail and the *Kingsbury Commitment* in 1913 in the United States. His key commitment was a profession of noble intent to enrich the public space. AT&T was to be an "enlightened monopoly" that served the public in close cooperation with the state while at the same time serving the interests of AT&T shareholders. His view of the telephone service as a privately operated public utility is, to quote Tim Wu in his treatise on Vail and AT&T, "...at once the most sympathetic and scariest element of his vision. Vail saw no harm in, and indeed believed in, giants, so long as they be friendly giants. He believed power should be beneficently concentrated, and that with great power came great responsibility."[8]

As we observe the aggregation of this critical part of the Internet infrastructure in the centralization of the DNS, it cannot be ignored that these grand statements of respect for the public interest and undertakings that safeguard personal privacy sound scarily similar to the espoused public benefactor vision of AT&T in 1913 as it embarked on a course of establishing a national monopoly. But it is perhaps not today's operators and today's commitments that should concern us, but where this condition may lead. Again, quoting Tim Wu: "[Theodore Vail] presents us therefore with a challenging figure: an unabashed monopolist, but a benign one, who lived up to his own ideals of enlightened despotism. The fault in this arrangement therefore lay not so much with Theodore Vail as with the men who would succeed him."[8].

Perhaps the same is true of these current undertakings relating to protection of personal privacy and their perception of the greater public interest.

Over time these earnest undertakings in the provision of free services may well be eroded by the inevitable pressures that every private enterprise is prone to, namely those of paying the bills and maximizing shareholder value. After the DNS is placed under an all-encompassing shroud of deep encryption, then both good and dark deeds will be both indistinguishable and undetectable.

It appears that the original disquiet on the part of the IETF was not that state-sponsored intelligence agencies collected intelligence, because, after all, that is their role, but a perception that the public accountability of some of these agencies had, in the IETF's view, failed. It is ironic that the IETF's response appears to literally hand the keys to an encrypted DNS over to a handful of private sector entities that appear to have no enduring public accountability whatsoever.

### References and Further Reading

[0] Electronic Privacy Information Center (EPIC), "An Open Letter to the Internet Engineering Task Force," November 8, 1999. **https://www.epic.org/privacy/internet/letter_to_ietf.html**

[1] IAB and IESG, "IETF Policy on Wiretapping," RFC 2804, May 2000.

[2] ETSI, "Lawful Interception (LI)," **https://www.etsi.org/technologies/lawful-interception**

[3] Stephen Farrell and Hannes Tschofenig, "Pervasive Monitoring Is an Attack," RFC 7258, May 2014.

[4] Wilmer van der Gaast, Carlo Contavalli, and Warren Kumari, "Client Subnet in DNS Queries," RFC 7871, May 2016.

[5] StatCounter, "Browser Market Share Worldwide," **http://gs.statcounter.com/browser-market-share**

[6] Marshall Erwin, "DNS-over-HTTPS Policy Requirements for Resolvers," Mozilla Security Blog, April 9, 2019. **https://blog.mozilla.org/security/2019/04/09/dns-over-https-policy-requirements-for-resolvers/**

[7] Eric Rescorla, "Mozilla's plans re: DoH," IETF Mailing List Archive, March 27, 2019. **https://mailarchive.ietf.org/arch/msg/doh/po6GCAJ52BAKuyL-dZiU91v6hLw**

[8] Tim Wu, *The Master Switch: The Rise and Fall of Information Empires*, Borsoi Books, ISBN-13: 978-0307269935, 2010.

[9] John Heidemann, Duane Wessels, Allison Mankin, Paul Hoffman, and Liang Zhu, "Specification for DNS over Transport Layer Security (TLS)," RFC 7858, May 2016.

[10] Sara Dickinson, Tirumaleswar Reddy, and Daniel Gillmor, "Usage Profiles for DNS over TLS and DNS over DTLS," RFC 8310, March 2018.

[11] Patrick McManus and Paul Hoffman, "DNS Queries over HTTPS (DoH)," RFC 8484, October 2018.

[12] IETF DNS PRIVate Exchange (DPRIVE) Working Group: **https://datatracker.ietf.org/wg/dprive/charter/**

[13] The OpenLI Project: **https://openli.nz/**

[14] Dan Wing, Tirumaleswar Reddy, and Prashanth Patil, "DNS over Datagram Transport Layer Security (DTLS)," RFC 8094, February 2017.

[15] Stephane Bortzmeyer, "DNS Query Name Minimisation to Improve Privacy," RFC 7816, March 2016.

[16] CALEA: **https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance**

[17] Paul Vixie, Joao Damas, and Michael Graff, "Extension Mechanisms for DNS (EDNS(0))," RFC 6891, April 2013.

[18] Geoff Huston and Joao Luis Silva Dama, "DNS Privacy," *The Internet Protocol Journal*, Volume 20, No. 1, March 2017.

[19] Patrick McManus and Paul E. Hoffman, "DNS-over-HTTPS (DoH) Operational and Privacy Issues," IETF Blog, **https://www.ietf.org/blog/doh-operational-and-privacy-issues/**

[20] Catalin Cimpanu, "First-ever malware strain spotted abusing new DoH (DNS over HTTPS) protocol," *ZDNet,* July 3, 2019. **https://www.zdnet.com/article/first-ever-malware-strain-spotted-abusing-new-doh-dns-over-https-protocol/**

[21] Catalin Cimpanu, "UK ISP group names Mozilla 'Internet Villain' for supporting 'DNS-over-HTTPS'," *ZDNet,* July 4, 2019. **https://www.zdnet.com/article/uk-isp-group-names-mozilla-internet-villain-for-supporting-dns-over-https/**

GEOFF HUSTON, B.Sc., M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region. He has been closely involved with the development of the Internet for many years, particularly within Australia, where he was responsible for building the Internet within the Australian academic and research sector in the early 1990s. He is author of numerous Internet-related books, and was a member of the Internet Architecture Board from 1999 until 2005. He served on the Board of Trustees of the Internet Society from 1992 until 2001. At various times Geoff has worked as an Internet researcher, an ISP systems architect, and a network operator. E-mail: **gih@apnic.net**

# Improving Routing Security

*by Andrei Robachevsky, The Internet Society*

Not a single day goes by without dozens of incidents affecting the routing system of the Internet. Route hijacking, route leaks, IP address spoofing, and other harmful activities can lead to *Denial of Service* (DoS) attacks, traffic inspection and surveillance, lost revenue, reputational damage, and more.

According to our analysis based on BGPStream[0] data, the following numbers indicate the scale of the problem along with the comparison to data from 2017:

- In 2017, there were 12,600 (a 9.6% decrease) incidents (either outages or attacks such as route leaks and hijacks). Figure 1 shows the number of routing incidents by type in 2018.
- Although the overall number of incidents was reduced, the ratio of outages vs. routing security incidents remained unchanged — 62/38.
- About 4.4% (a decrease of 1%) of all Autonomous Systems on the Internet were affected.
- 2,737 (a decrease of 12%) Autonomous Systems experienced at least one routing incident.
- 1,294 (a 17% decrease!) networks were responsible for 4,739 routing incidents (a 10.6% decrease).

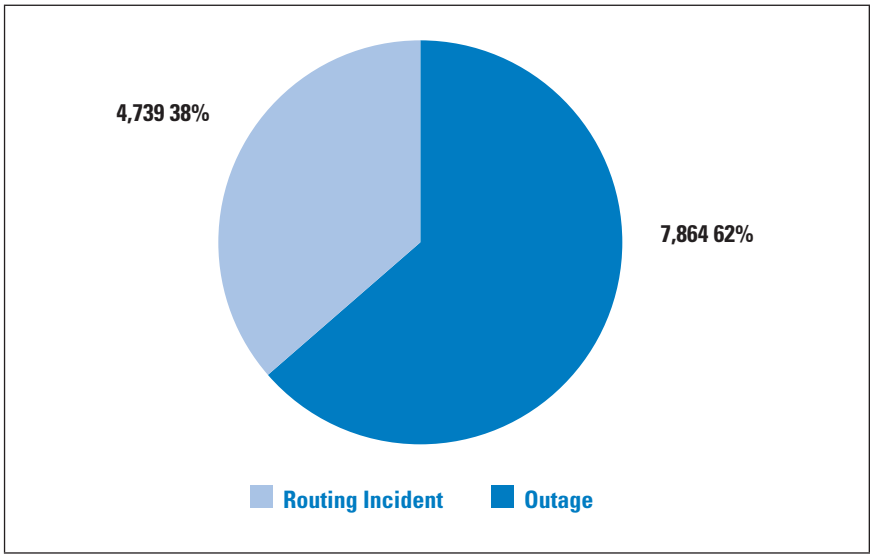
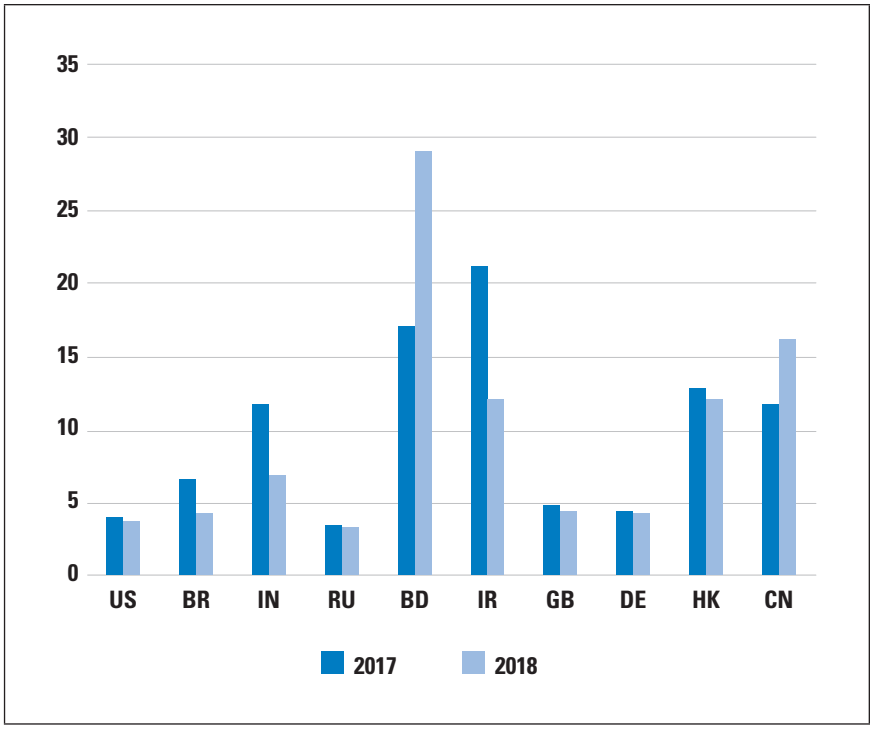



*Figure 1: Routing incidents by type in 2018; almost 40% of all incidents were due to routing security issues.*

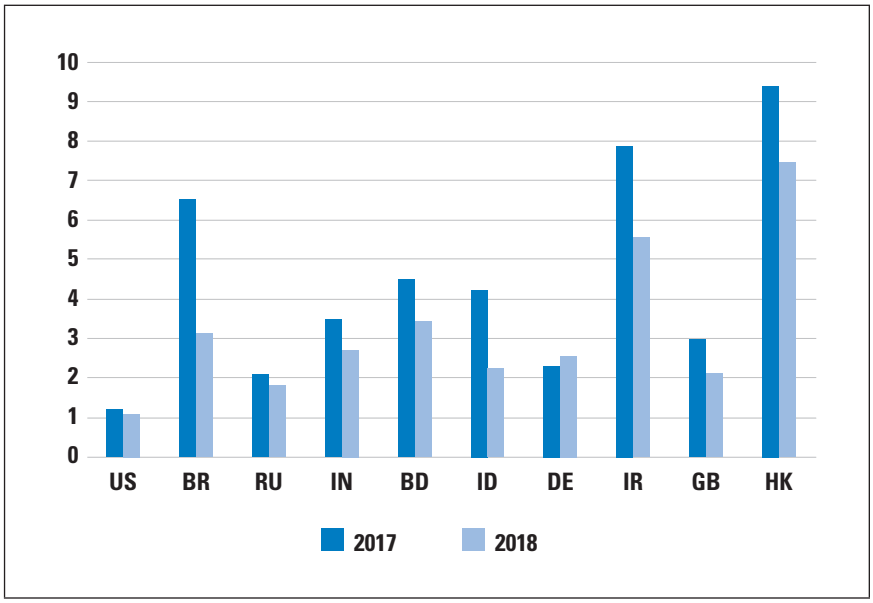
Looking further at the dynamics of the evolution of routing security from the perspective of affected networks (Figure 2), we can see that Bangladesh, mainland China, and Hong Kong appear to be the most vulnerable, with up to 30% of all networks affected by a routing mishap. We can also see positive dynamics in countries like Brazil, India, and Iran, where the percentage of "victimized" networks decreased significantly.

*Figure 2: Changes in the percentage of affected networks in a country. Top-10 most affected countries.*




Let's look at networks whose configuration mistakes or intentional acts caused these incidents. In absolute numbers, 36% of all "culprits" operate in the US, Brazil, and Russia, but if we normalize this number by the total number of networks in a country, mainland China and Hong Kong are at the top (see Figure 3). On a positive side, the situation has improved in most of the top-10 countries with the highest number of culprits. For instance, in Brazil the number of misbehaving networks has been cut by more than half.

*Figure 3: Changes in the percentage of networks in a country responsible for a routing incident, top 10 with most incidents detected.*



### Why Is Routing Security Hard?

Despite the positive trend, it is too early to celebrate victory; vulnerabilities still exist, and too many networks are not applying required controls to prevent incidents from happening. What is holding the networks from resolving this problem once and forever?

There are several reasons. In the Internet, as a decentralized system, the overall level of routing security depends on the individual actions of all network operators, and incidents in most cases are impossible to address by your own operator. The economics favor insecurity, as the impacts of routing incidents are often felt by others and not by the culprit, and security has not yet emerged as a market differentiator. To put it another way—the controls that are necessary to reduce routing incidents, and that the operator should apply, improve the overall security, and to a much lesser extent they offer protection to their own networks. In other words, the security of your network is in the hands of other network operators, with whom you may not have any relation-ship. Therefore, addressing security issues in the Internet routing system requires a collective action.

Another challenge is related to the fact that security in general is not a state, but a process. Implementing security requires a systemic approach, and that is why corporate security relies on frameworks and established processes. How is it possible to apply such a systemic approach in a decentralized system with more than 60K independent networks?

MANRS[1], *Mutually Agreed Norms for Routing Security,* attempts to address both challenges.

### How MANRS Can Help

MANRS, a global initiative driven by network operators and *Internet Exchange Points* (IXPs) all over the globe and supported by the Internet Society, outlines simple but concrete actions that different types of network operators should take. The actions are limited in scope, and backed up by a growing community they have a good chance to become true norms of security in network operations.

Norms are often seen as possible solutions to a so-called *Collective Action Problem*. The name of this social phenomenon, known for centuries, was coined by Mancur Olson in 1965 in his book *The Logic of Collective Action*[2]. Not really a problem in small communities, it becomes a real challenge as the number of entities grows, resulting in the failure to cooperate because of conflicting interests, despite a clear common benefit. That phenomenon is exactly what we observe in the area of routing security in the Internet.

Let's look at a set of actions that MANRS offers. Four actions are defined for *Internet Service Providers* (ISPs):

- *Action 1. Filtering:* Ensure the correctness of your own routing announcements and of announcements from your customers to adjacent networks with prefix and *Autonomous System (AS)-path granularity.*
- *Action 2. Anti-spoofing:* Enable source address validation for at least single-homed stub customer networks, your own end users, and infrastructure.
- *Action 3. Coordination:* Maintain globally accessible up-to-date contact information.
- *Action 4. Global Validation:* Publish your routing policy, including the intended announcements, so others can validate routing information on a global scale.

These actions represent a minimum baseline that yields significant improvements to the routing system with relatively little effort from individual players. The actions also provide a global reference that other initiatives or corporate improvement projects can use as a starting building block. This process can help focus various efforts in the area of routing security for steady and continuous improvement on a global scale.

Another aspect of MANRS is related to the interdependency and the fact that only a collective solution is possible. Not only does MANRS serve as a recommendation of what to do, but it also builds a community of security-minded operators committed to the common cause. The community is crucial in reinforcing the baseline and transforming it into norms of operational behavior.

Network operators join MANRS not out of pure altruism. Many understand that a stable and secure communication fabric is an essential component for their growing business. Many of the operators that joined MANRS were already implementing good routing security and even exceeding the requirements of the actions. However, MANRS, as a global reference point, provides them an opportunity to signal their security posture to customers and regulators. Moreover, the growing MANRS community is a clear demonstration that the industry is taking action to address these complex security issues.

### IXPs Onboard

ISPs are not the only players that affect routing security. For instance, IXPs form local communities of ISPs with a common operational objective. They are in an excellent position to support the reciprocity of network protection that routing security requires and create a "safe neighborhood" at the exchange. To take advantage of the impact IXPs can have in the area of routing security, the MANRS community set the goal to get IXPs on board.

But IXPs are not exactly ISPs. And since MANRS membership requires demonstration of commitment with a tangible contribution, the community has created a related but separate set of MANRS actions for participating IXPs:

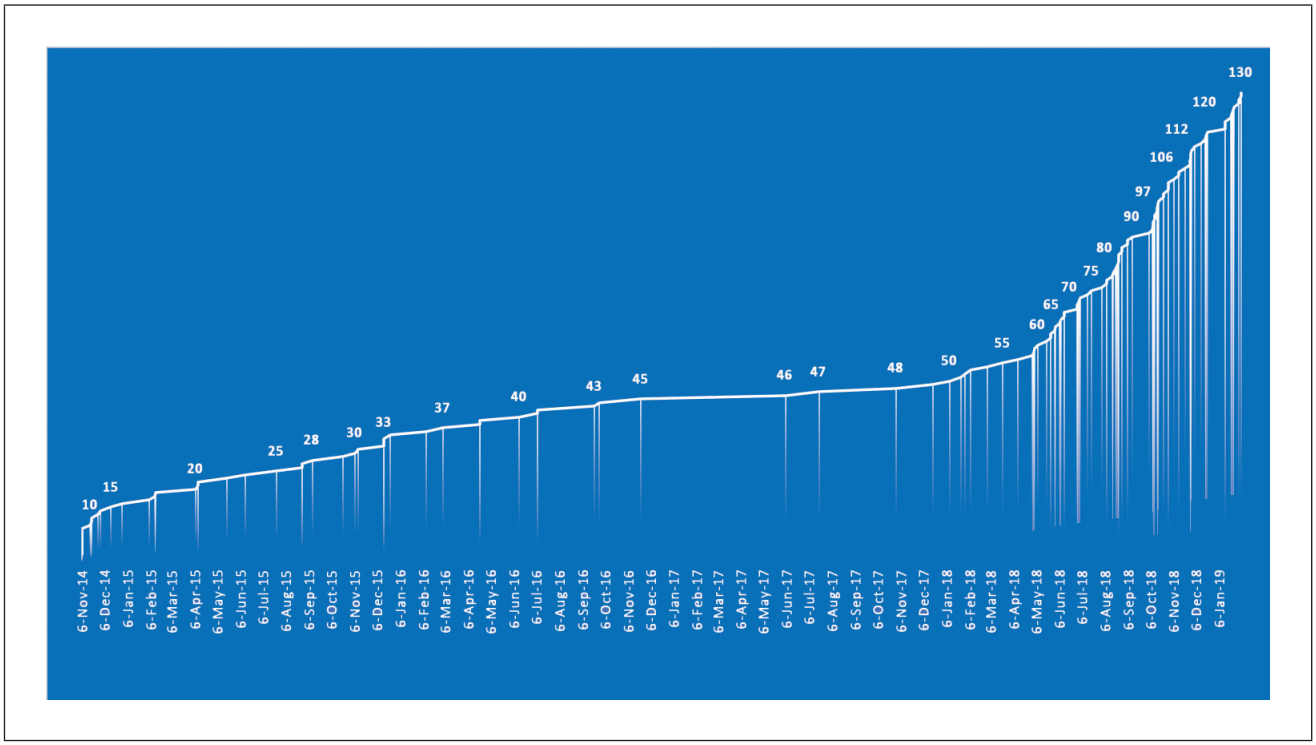
- *Action 1. Prevent propagation of incorrect routing information:* This mandatory action requires IXPs to implement filtering of route announcements at the Route Server based on routing information data (*Internet Routing Registry* [IRR] and/or *Resource Public Key Infrastructure* [RPKI]). A Route Server is a proxy network used to facilitate multilateral peering between the operators. Instead of setting up multiple *Border Gateway Protocol* (BGP) peering sessions with various operators at the exchange, an operator can peer with only the Route Server to accomplish this goal.
- *Action 2. Promote MANRS to the IXP membership:* IXPs joining MANRS are expected to provide encouragement or assistance for their members to implement MANRS actions.
- *Action 3. Protect the peering platform:* This action requires that the IXP have a published policy of traffic not allowed on the peering fabric and perform filtering of such traffic.
- *Action 4. Facilitate global operational communication and coordination among its members by providing necessary mailing lists and member directories.*
- *Action 5. Provide monitoring and debugging tools, such as the Looking Glass (LG)*[3]*:* BGP LG servers are computers on the Internet running one of a variety of publicly available Looking Glass software implementations. A LG server is accessed remotely for the purpose of viewing routing information. Essentially, the server acts as a limited, read-only portal to routers of whatever organization is running the LG server. Typically, publicly accessible LG servers are run by ISPs or *Network Operations Centers* (NOCs).

### Membership Growth

MANRS has seen a steady growth of its membership since its launch in November 2014. At the time of this writing, 130 operators cover more than 250 ASNs. Since the launch of the IXP Programme[4] in April 2018, the number of participating IXPs has reached 30 (Figure 4).

MANRS needs partners to scale up adoption. IXPs are a great example of such collaboration. MANRS also partners with organizations such as APNIC, *Latin America and Caribbean Network Information Centre* (LACNIC), *Latin American and Caribbean Internet Exchange Association* (LAC-IX), the *Brazilian Network Information Center* (NIC.BR), Internet2, GÉANT, and RedCLARA to reach out to regional communities to grow the MANRS membership.

*Figure 4: MANRS membership growth, ISPs.*




Education and training play a very important role helping to lower the threshold for adoption. Based on the "Implementation Guide" developed by the community, MANRS Online Training[5] contains six modules to help engineers understand the implementation details of the actions. These online modules can be completed either individually or as part of a moderated class, earning a certificate of completion from the Internet Society.

Next step in the capacity-building program is the release of the online hands-on lab; its development is being finalized.

In the area of capacity building, MANRS partners with training organizations such as the *Network Startup Resource Center* (NSRC) and the *Asia Pacific Network Information Centre* (APNIC)—reaching out to hundreds of network engineers.

As the awareness grows, more and more organizations are evaluating their readiness for MANRS actions, making necessary adjustments and joining the effort. The capacity-building efforts help networks that lack necessary expertise to implement the actions quickly.

It is our collective responsibility as participants of the Internet global routing system to ensure the reliability and security of the Internet. Help us make the Internet a safer place. Only together can we protect the core.

### References and Further Reading

[0] BGPStream: **https://bgpstream.com/**

[1] MANRS: **https://www.manrs.org/**

[2] Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups,* Harvard University Press, ISBN 0-674-53751-3, 1971.

[3] BGP: the Border Gateway Protocol Advanced Internet Routing Resources: **http://www.bgp4.as/looking-glasses**

[4] MANRS IXP Programme: **https://www.manrs.org/ixps/**

[5] MANRS Tutorials: **https://www.manrs.org/tutorials/**

[6] Salam Yamout, "Improving Routing Security: Microsoft Joins MANRS," Internet Society Blog, May 22, 2019. **https://www.internetsociety.org/blog/2019/05/improving-routing-security-microsoft-joins-manrs/**

[7] Dan Goodin, "Google goes down after major BGP mishap routes traffic through China," Ars Technica, November 12, 2018. **https://arstechnica.com/information-technology/2018/11/major-bgp-mishap-takes-down-google-as-traffic-improperly-travels-to-china/**

[8] "Routing Security for Policymakers," An Internet Society White Paper, October 2018. **https://www.internetsociety.org/resources/doc/2018/routing-security-for-policymakers/**

[9] Matthew Lepinski, "BGPsec Protocol Specification," RFC 8205, September 2017.

[10] Wesley George and Sandra Murphy, "BGPsec Considerations for Autonomous System (AS) Migration," RFC 8206, September 2017.

[11] Randy Bush and Geoff Huston, "Securing BGP with BGPsec," *The Internet Protocol Journal,* Volume 14, No. 2, June 2011.

[12] Stephen Kent, "Securing the Border Gateway Protocol," *The Internet Protocol Journal,* Volume 6, No. 3, September 2003.

ANDREI ROBACHEVSKY is the Senior Technology Programme Manager for the Internet Society. Andrei's primary area of interest is security and resilience of the Internet infrastructure. This work is based on active engagement with the operator, research, and policy communities. Prior to joining ISOC, Andrei was Chief Technical Officer of the RIPE NCC, leading the development of the company's IT strategy, external and internal IT services, and work of the engineering departments. He was responsible for the deployment of DNSSEC for the reverse DNS tree and deployment of anycast instances of the K-root DNS server. Andrei brings to the Internet Society more than 10 years of experience in the Internet technical community. For more than a decade he has been actively following Regional Internet Registry (RIR) and Internet Engineering Task Force (IETF) activities. He was Chair of the Number Resource Organization's (NRO) Engineering Coordination Group (ECG), which is responsible for various technical inter-RIR activities and projects. In 2010–2012 Andrei was a member of the Internet Architecture Board (IAB). Andrei is based in Amsterdam, The Netherlands. E-mail: **robachevsky@isoc.org**

# Fragments

### ISOC Signs Letter Opposing GCHQ Proposal for Weakening Encryption

In late 2018, The British *Government Communications Headquarters* (GCHQ) published an essay[1] on *Lawfare* outlining its principles for "exceptional" or "lawful" access to encrypted information, alongside a proposed use case—the "ghost proposal." (Generally, when people speak of lawful or exceptional access they refer to some means of allowing law enforcement the ability to lawfully access the content of encrypted communications and encrypted data in an unencrypted form. For example, by asking companies to have the technical ability to access encrypted content.)

The GCHQ proposal would add a silent (or ghost) user to end-to-end encrypted messaging services, such as *WhatsApp*, and allow the government to listen in to ongoing encrypted conversations secretly for law enforcement or national security purposes. The *Internet Society* is pleased to add its name to an open letter[2] outlining the dangers that this proposal, and techniques like it, pose to the Internet and to users everywhere.

All exceptional or lawful access proposals put users, the economy, the services we depend on and the Internet itself at greater risk to security threats. GCHQ's "ghost proposal" is no exception. As stated in the open letter, the ghost proposal would:

> "...introduce potential unintentional vulnerabilities, and increase risks that communications systems could be abused or misused ... [and] mean that users cannot trust that their communications are secure."

Protected communications are a matter of security. Whether they are used to keep critical infrastructure running, safeguard our financial information, or keep personal information from those who would use it to do us harm, protected communications keep us all safe. All of these rely on encryption and other digital security tools.

The ISOC is proud to add its voice to a diverse group of stakeholders from civil society, industry and academia calling on GCHQ to abandon the ghost proposal and avoid any alternate approaches that would similarly threaten digital security and human rights. We must strengthen, not weaken encryption. By whatever name, any point of entry to a secure service is a weakness.

[1] Ian Levy and Crispin Robinson, "Principles for a More Informed Exceptional Access Debate," *Lawfare*, November 2018. **https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate**

[2] Open Letter to GCHQ: **https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_to_GCHQ_on_Ghost_Proposal_-_May_22_2019.pdf**

### ICANN Publishes Updated Domain Name Marketplace Indicators

The *Internet Corporation for Names and Numbers* (ICANN) recently announced publication of the first wave of the *Domain Name Marketplace Indicators* report, which presents statistics related to *generic top-level domains* (gTLDs) and *country code top-level domains* (ccTLDs).[1]

This report is an evolution of the previous *gTLD Marketplace Health Index* report (Beta), which was first published in July 2016 with twice annual reports through June 2018. This report includes expanded coverage to include ccTLD data. ICANN plans to further expand its coverage of shortlisted indicators and continue to publish these statistics twice a year to track progress against its goal of supporting the evolution of the domain name marketplace to be robust, stable and trusted.

A community Advisory Panel worked with ICANN to refine these indicators in preparation for publishing this version. Concurrent to the release of these Version 1.0 marketplace indicators, ICANN org will continue to work with the community and the Advisory Panel to evaluate additional enhancements that might be incorporated into this initiative in the future.

ICANN's mission is to help ensure a stable, secure and unified global Internet. To reach another person on the Internet, you need to type an address—a name or a number—into your computer or other device. That address must be unique so computers know where to find each other. ICANN helps coordinate and support these unique identifiers across the world. ICANN was formed in 1998 as a not-for-profit public-benefit corporation with a community of participants from all over the world.

[1] **https://www.icann.org/resources/pages/metrics-gdd-2015-01-30-en**

### Check your Subscription Details!

If you have a print subscription to this journal, you will find an expiration date printed on the back cover. For the last couple of years, we have "auto-renewed" your subscription, but now we ask you to log in to our subscription system and perform this simple task yourself. The subscription portal is here: **https://www.ipjsubscription.org/** This process will ensure that we have your current contact information as well as delivery preference (print edition or download). For any questions, contact us by e-mail at: **ipj@protocoljournal.org**

# Thank You!

Publication of IPJ is made possible by organizations and individuals around the world dedicated to the design, growth, evolution, and operation of the global Internet and private networks built on the Internet Protocol. The following individuals have provided support to IPJ. You can join them by visiting **http://tinyurl.com/IPJ-donate**

Fabrizio Accatino
Michael Achola
Martin Adkins
Christopher Affleck
Scott Aitken
Jacobus Akkerhuis
Antonio Cuñat Alario
Nicola Altan
Matteo D'Ambrosio
Jens Andersson
Danish Ansari
Tim Armstrong
Richard Artes
David Atkins
Jaime Badua
Eric Baker
Santosh Balagopalan
David Belson
Hidde Beumer
Pier Paolo Biagi
John Bigrow
Orvar Ari Bjarnason
Axel Boeger
Keith Bogart
Mirko Bonadei
Roberto Bonalumi
Julie Bottorff Photography
Gerry Boudreaux
L de Braal
Kevin Breit
Thomas Bridge
Ilia Bromberg
Václav Brožík
Christophe Brun
Gareth Bryan
Stefan Buckmann
Caner Budakoglu
Darrell Budic
Scott Burleigh
Jon Harald Bøvre
Olivier Cahagne
Antoine Camerlo
Tracy Camp
Ignacio Soto Campos
Fabio Caneparo
Roberto Canonico
David Cardwell
John Cavanaugh
Lj Cemeras
Dave Chapman
Stefanos Charchalakis
Greg Chisholm
David Chosrova
Marcin Cieslak
Brad Clark
Narelle Clark
Steve Corbató
Brian Courtney
Dave Crocker
Kevin Croes
John Curran
André Danthine
Morgan Davis
Jeff Day
Freek Dijkstra
Geert Van Dijk
David Dillow
Richard Dodsworth
Ernesto Doelling
Eugene Doroniuk
Karlheinz Dölger
Joshua Dreier
Lutz Drink
Andrew Dul
Holger Durer
Mark Eanes
Peter Robert Egli
George Ehlers
Peter Eisses
Torbjörn Eklöv
Y Ertur
ERNW GmbH
ESdatCo
Steve Esquivel
Jay Etchings
Mikhail Evstiounin
Paul Ferguson
Kent Fichtner
The Flirble Organisation
Gary Ford
Jean-Pierre Forcioli
Christopher Forsyth
Andrew Fox
Craig Fox
Fausto Franceschini
Tomislav Futivic
Edward Gallagher
Andrew Gallo
Chris Gamboni
Xosé Bravo Garcia
Kevin Gee
John Gilbert
Serge Van Ginderachter
Greg Goddard
Octavio Alfageme Gorostiaga
Barry Greene
Richard Gregor
Martijn Groenleer
Geert Jan de Groot
Christopher Guemez
Gulf Coast Shots
Sheryll de Guzman
James Hamilton
Stephen Hanna
Martin Hannigan
John Hardin
David Harper
Edward Hauser
David Hauweele
Marilyn Hay
Headcrafts SRLS
Hidde van der Heide
Johan Helsingius
Robert Hinden
Asbjorn Hojmark
Damien Holloway
Alain Van Hoof
Edward Hotard
Bill Huber
Hagen Hultzsch
Kevin Iddles
Mika Ilvesmaki
Karsten Iwen
David Jaffe
Ashford Jaggernauth
Martijn Jansen
Jozef Janitor
John Jarvis
Dennis Jennings
Edward Jennings
Aart Jochem
Brian Johnson
Curtis Johnson
Richard Johnson
Jim Johnston
Jonatan Jonasson
Daniel Jones
Gary Jones
Jerry Jones
Amar Joshi
Merike Kaeo
Andrew Kaiser
Christos Karayiannis
David Kekar
Jithin Kesavan
Jubal Kessler
Shan Ali Khan
Nabeel Khatri
Dae Young Kim
Anthony Klopp
Henry Kluge
Michael Kluk
Andrew Koch
Ia Kochiashvili
Carsten Koempe
Alexader Kogan
Antonin Kral
Mathias Körber
John Kristoff
Terje Krogdahl
Bobby Krupczak
Murray Kucherawy
Dirk Kurfuerst
Warren Kumari
Darrell Lack
Yan Landriault
Sig Lange
Markus Langenmair
Fred Langham
Andrew Lamb
Richard Lamb
Tracy LaQuey Parker
Rick van Leeuwen

Simon Leinen
Robert Lewis
Martin Lillepuu
Roger Lindholm
Sergio Loreti
Eric Louie
Guillermo a Loyola
Hannes Lubich
Dan Lynch
Miroslav Madić
Alexis Madriz
Carl Malamud
Michael Malik
Yogesh Mangar
Bill Manning
Harold March
Vincent Marchand
David Martin
Jim Martin
Ruben Tripiana Martin
Timothy Martin
Gabriel Marroquin
Carles Mateu
Juan Jose Marin Martinez
Ioan Maxim
David Mazel
Miles McCredie
Brian McCullough
Joe McEachern
Jay McMaster
Mark Mc Nicholas
Carsten Melberg
Kevin Menezes
Bart Jan Menkveld
William Mills
David Millsom
Desiree Miloshevic
Joost van der Minnen
Thomas Mino
Wijnand Modderman
Mohammad Moghaddas
Charles Monson
Andrea Montefusco
Fernando Montenegro
Joel Moore
Maurizio Moroni
Brian Mort
Soenke Mumm
Tariq Mustafa
Stuart Nadin
Michel Nakhla
Mazdak Rajabi Nasab
Krishna Natarajan
Darryl Newman
Thomas Nikolajsen
Paul Nikolich
Travis Northrup
Marijana Novakovic
David Oates
Ovidiu Obersterescu
Tim O'Brien
Mike O'Connor
Mike O'Dell
Jim Oplotnik
Carlos Astor Araujo Palmeira
Alexis Panagopoulos
Gaurav Panwar
Manuel Uruena Pascual
Ricardo Patara
Dipesh Patel
Alex Parkinson
Craig Partridge
Dan Paynter
Leif Eric Pedersen
Rui Sao Pedro
Juan Pena
Chris Perkins
David Phelan
Derrell Piper
Rob Pirnie
Marc Vives Piza
Jorge Ivan Pincay Ponce
Victoria Poncini
Blahoslav Popela
Eduard Llull Pou
Tim Pozar
David Raistrick
Priyan R Rajeevan
Balaji Rajendran
Paul Rathbone
William Rawlings
Bill Reid
Rodrigo Ribeiro
Glenn Ricart
Justin Richards
Mark Risinger
Ron Rockrohr
Carlos Rodrigues
Magnus Romedahl
Lex Van Roon
William Ross
Boudhayan Roychowdhury
Carlos Rubio
Timo Ruiter
RustedMusic
Babak Saberi
George Sadowsky
Scott Sandefur
Sachin Sapkal
Arturas Satkovskis
PS Saunders
John Sayer
Phil Scarr
Elizabeth Scheid
Jeroen Van Ingen Schenau
Carsten Scherb
Ernest Schirmer
Dan Schrenk
Richard Schultz
Roger Schwartz
SeenThere
Scott Seifel
Yury Shefer
Yaron Sheffer
Doron Shikmoni
Tj Shumway
Jeffrey Sicuranza
Thorsten Sideboard
Andrew Simmons
Pradeep Singh
Henry Sinnreich
Geoff Sisson
Helge Skrivervik
Darren Sleeth
Richard Smit
Bob Smith
Courtney Smith
Mark Smith
Job Snijders
Ronald Solano
Asit Som
Ignacio Soto Campos
Peter Spekreijse
Thayumanavan Sridhar
Paul Stancik
Ralf Stempfer
Matthew Stenberg
Adrian Stevens
Clinton Stevens
John Streck
Viktor Sudakov
Edward-W. Suor
Vincent Surillo
T2Group
Roman Tarasov
David Theese
Douglas Thompson
Lorin J Thompson
Joseph Toste
Rey Tucker
Sandro Tumini
Angelo Turetta
Phil Tweedie
Steve Ulrich
Unitek Engineering AG
John Urbanek
Martin Urwaleck
Betsy Vanderpool
Surendran Vangadasalam
Buddy Venne
Alejandro Vennera
Luca Ventura
Tom Vest
Dario Vitali
Lakhinder Walia
Laurence Walker
Randy Watts
Andrew Webster
Tim Weil
Jd Wegner
Westmoreland Engineering Inc.
Rick Wesson
Peter Whimp
Russ White
Jurrien Wijlhuizen
Derick Winkworth
Pindar Wong
Romeo Zwart
Bernd Zeimetz
廖 明沂.


**Follow us on Twitter and Facebook** `@protocoljournal` `https://www.facebook.com/newipj`

# Call for Papers

The *Internet Protocol Journal* (IPJ) is a quarterly technical publication containing tutorial articles ("What is...?") as well as implementation/operation articles ("How to..."). The journal provides articles about all aspects of Internet technology. IPJ is not intended to promote any specific products or services, but rather is intended to serve as an informational and educational resource for engineering professionals involved in the design, development, and operation of public and private internets and intranets. In addition to feature-length articles, IPJ contains technical updates, book reviews, announcements, opinion columns, and letters to the Editor. Topics include but are not limited to:

- Access and infrastructure technologies such as: Wi-Fi, Gigabit Ethernet, SONET, xDSL, cable, fiber optics, satellite, and mobile wireless.
- Transport and interconnection functions such as: switching, routing, tunneling, protocol transition, multicast, and performance.
- Network management, administration, and security issues, including: authentication, privacy, encryption, monitoring, firewalls, troubleshooting, and mapping.
- Value-added systems and services such as: Virtual Private Networks, resource location, caching, client/server systems, distributed systems, cloud computing, and quality of service.
- Application and end-user issues such as: E-mail, Web authoring, server technologies and systems, electronic commerce, and application management.
- Legal, policy, regulatory and governance topics such as: copyright, content control, content liability, settlement charges, resource allocation, and trademark disputes in the context of internetworking.

IPJ will pay a stipend of US$1000 for published, feature-length articles. For further information regarding article submissions, please contact Ole J. Jacobsen, Editor and Publisher. Ole can be reached at **ole@protocoljournal.org** or **olejacobsen@me.com**

# Supporters and Sponsors

*Supporters*

Internet Society

cisco

*Diamond Sponsors*

Google

ICANN

*Ruby Sponsors*

Your logo here!

*Sapphire Sponsors*

Your logo here!

*Emerald Sponsors*

Afilias

Akamai

APNIC

APRICOT Asia Pacific Regional Internet Conference on Operational Technologies

COMCAST

DE-CIX

EQUINIX

JPRS Japan Registry Services

Juniper Networks

lacnic

LinkedIn

linx

NSRC Network Startup Resource Center

NTT Communications

RIPE NCC RIPE Network Coordination Centre

TEAM CYMRU

VERISIGN

WIDE PROJECT

*Corporate Subscriptions*

AFRINIC The Internet Numbers Registry for Africa

amsix amsterdam internet exchange

DNS-OARC

IWL

ISC Internet Systems Consortium

Limelight Networks

PKNIC

qa cafe

SIDN

For more information about sponsorship, please contact `sponsor@protocoljournal.org`

The Internet Protocol Journal
NMS
535 Brennan Street
San Jose, CA 95131

CHANGE SERVICE REQUESTED



*The Internet Protocol Journal is published quarterly and supported by the Internet Society and other organizations and individuals around the world dedicated to the design, growth, evolution, and operation of the global Internet and private networks built on the Internet Protocol.*

*Email: ipj@protocoljournal.org*
*Web: www.protocoljournal.org*