March 2019
Geoff Huston

# The State of DNSSEC Validation

Many aspects of technology adoption in the Internet over time show simple "up and to the right" curves. There are many examples, so to pick a classic curve Google's measurement of IPv6 use is a good example (https://www.google.com/intl/en/ipv6/statistics.html). What lies behind these curves is the theory that once a decision is made to deploy a technology the decision is not subsequently "unmade." When we observe an adoption curve fall rather than rise, then it's reasonable to ask what is going on.

The level of DNSSEC validation of DNS responses in the Internet is an example where the curve is not "up and to the right." We observe that the level of use of DNSSEC validation has fallen for an extended period across 2017 and 2018 and has only regained its momentum in the most recent six months. In this article let's look into this data in further detail to see what is going on.

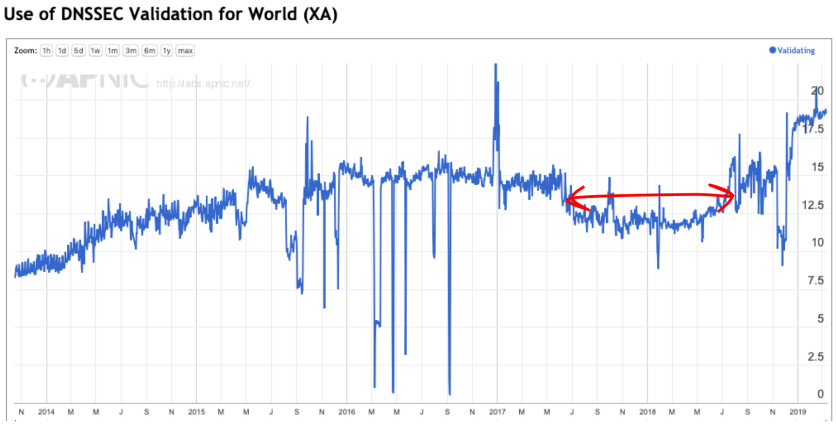


*Figure 1 – DNSSEC Validation rate (https://stats.labs.apnic.net/dnssec/XA)*

Google's Public DNS service (8.8.8.8) is undoubtedly the most popular DNS resolution service in the Internet, and some 15% of the world's users pass their queries through this service. Google's Public DNS service performs DNSSEC validation, and for some years it appeared that the growth in uptake of DNSSEC validation and the growth in uptake of the use of Google's public DNS resolver service were largely a reflection of each other.

The drop in the level of DNSSEC validation in 2017 - 2018 coincides with a drop in the level of the use of Google's DNS service over the same period, which again appears to support the supposition that Google's PDNS service is the major driving factor behind the general use of DNSSEC validation. However, we're seeing in late 2018 and early 2019 a divergence in these two metrics: the level of use of Google PDNS service is steady at around 13%-15% while the level of DNSSEC validation is now approaching 20% of the Internet's user population.

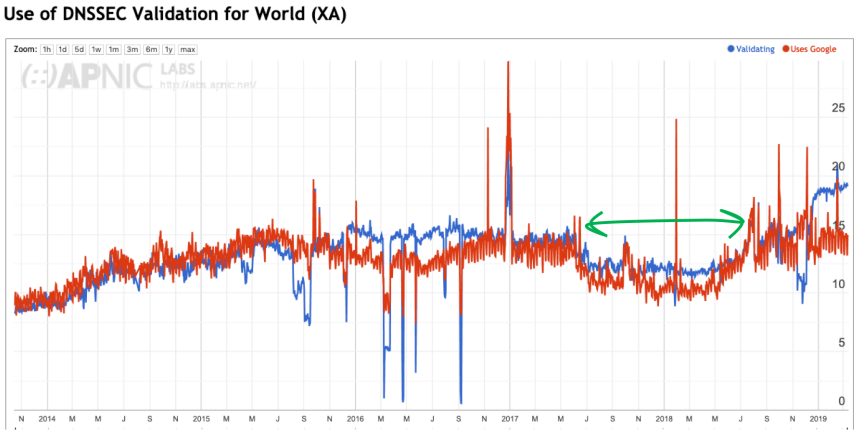


*Figure 2 – DNSSEC Validation rate and use of Google's DNS service (https://stats.labs.apnic.net/dnssec/XA?g=1)*

This consideration of "the Internet" in this context is somewhat misleading. The Internet is not homogenous, and while we can talk about "Internet-wide" metrics, it does not necessarily mean that all regions of the Internet show the same behaviours. Of the five major geographic regions of the world only two regions show a noticeable decrease in the level of DNSSEC validation in 2017 and 2018, namely Africa and Asia. The other regions show a pausing of growth across 2017 and 2018, but not necessarily a decline.

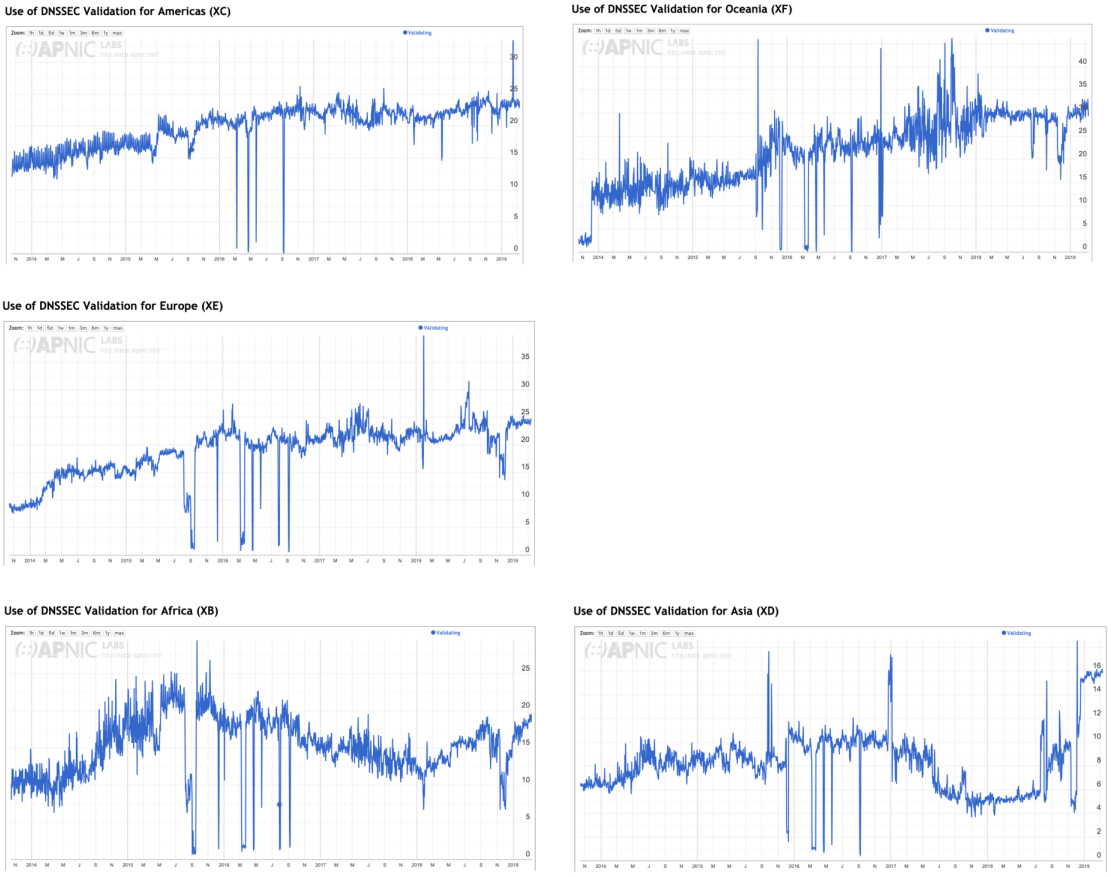


*Figure 3 – DNSSEC Validation by Region*

It seems that Africa and Asia both saw a decline in DNSSEC validation rates across 2017 and 2018. Let's look at these two regions in a little more detail.

## DNSSEC Validation in Africa

Let's first look in a bit more detail into Africa. DNSSEC validation use peaked at 22% of users in mid-2016 and declined to 12% by early 2018 and has shifted back to 18% in early 2019. ISP's in this region have been relatively enthusiastic users of Google's Public DNS services, and over the past 5 years the use of Google's DNS services has been between 20% to 35% of the entire African user population. Interestingly, the period over 2016 – 2017 saw the use of Google's service increase, but the level of DNSSEC validation decline. The most logical explanation is that ISPs increasingly used local non-validating DNS resolvers to complement their use of Google's service.

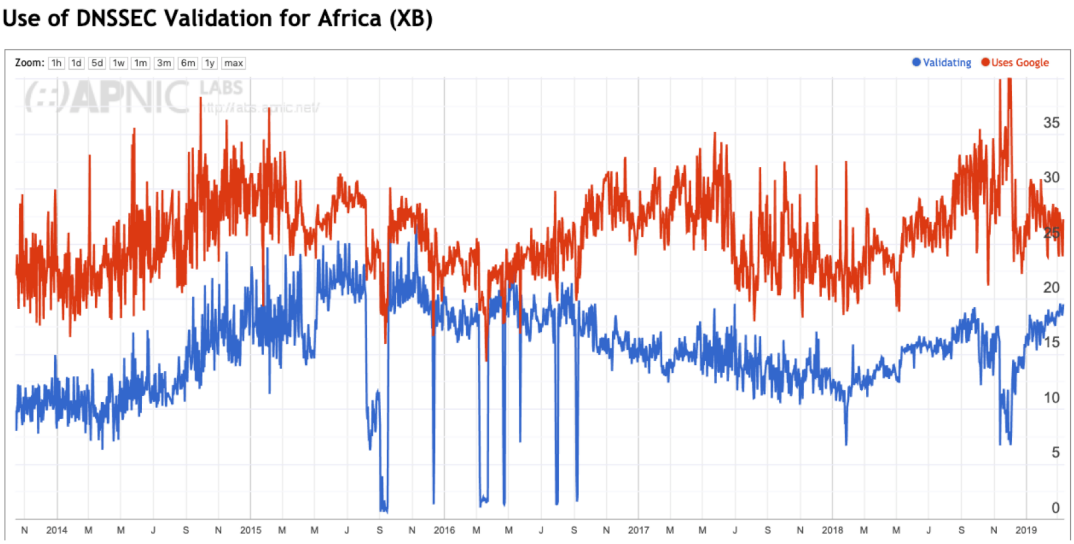


*Figure 4 – DNSSEC validation and Google DNS use in Africa*

The largest pools of Internet users in Africa are to be found in Nigeria, Egypt, South Africa, Kenya, and Morocco. These five countries contain two thirds of the region's Internet user population.

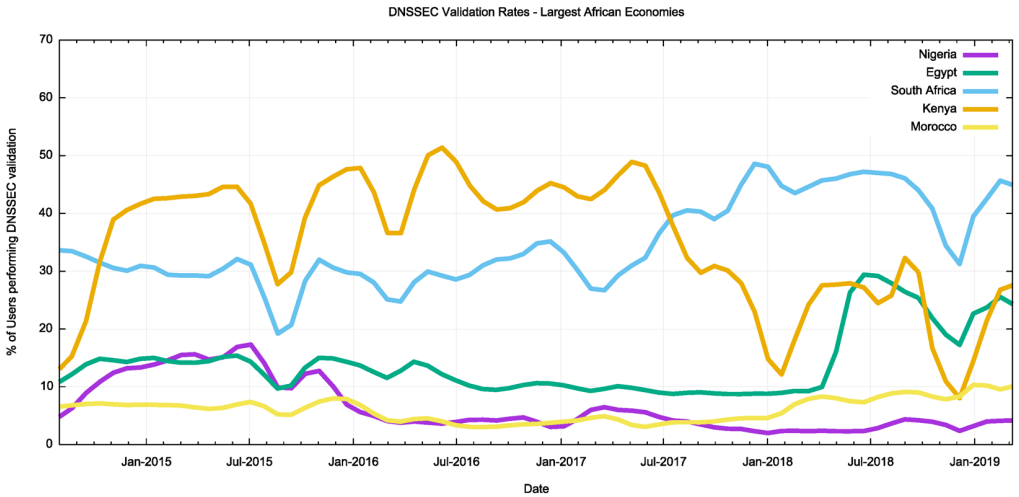


*Figure 5 – DNSSEC validation in the 5 largest African Economies*

In Nigeria AS 36873 (Celtel Nigeria) used Google's DNS service almost exclusively across 2015, and then transitioned to use other non-validating resolvers in 2016. In 2018 they have resumed the use of Google DNS service, but in conjunction with a local resolver (https://stats.labs.apnic.net/dnssec/AS36873). Another major ISP in Nigeria, AS37076 (EMTS) also used Google's DNS service up until the start of 2016, but since then they have used other non-DNSSEC-validating DNS resolvers (https://stats.labs.apnic.net/dnssec/AS37076).

The picture in Egypt is somewhat different and DNSSEC validation has been constant at around 10% until mid 2018, when one of the larger service providers, AS8452 (TE Data) switched to use Google's DNS service and DNSSEC validation rates rose accordingly (https://stats.labs.apnic.net/dnssec/AS8452)

In Kenya one of the larger service providers, AS36926 (Celtel) appears to have turned on DNSSEC validation in its local DNS resolver infrastructure in 2016, but then reverted to a non-validating configuration in September 2016 (https://stats.labs.apnic.net/dnssec/AS36926).

## DNSSEC Validation in Asia

The picture of DNSSEC validation in Asia is similar to that seen in Africa. Many ISPs in Asia appear to direct their user's DNS queries to Google's service..

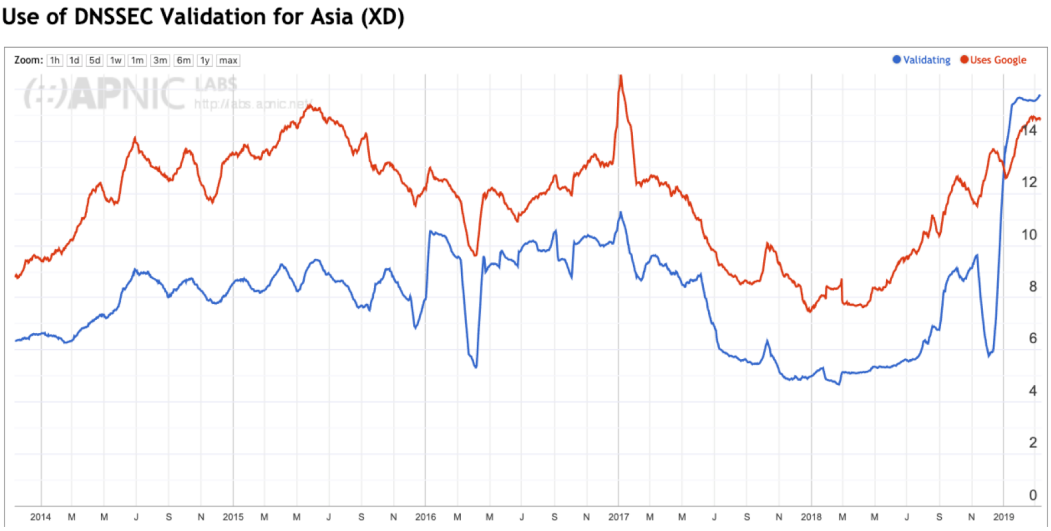


*Figure 6 – DNSSEC validation and Google DNS use in Asia*

Some 80% of the region's considerable user population can be found in China, India, Japan, Indonesia, Vietnam and Turkey

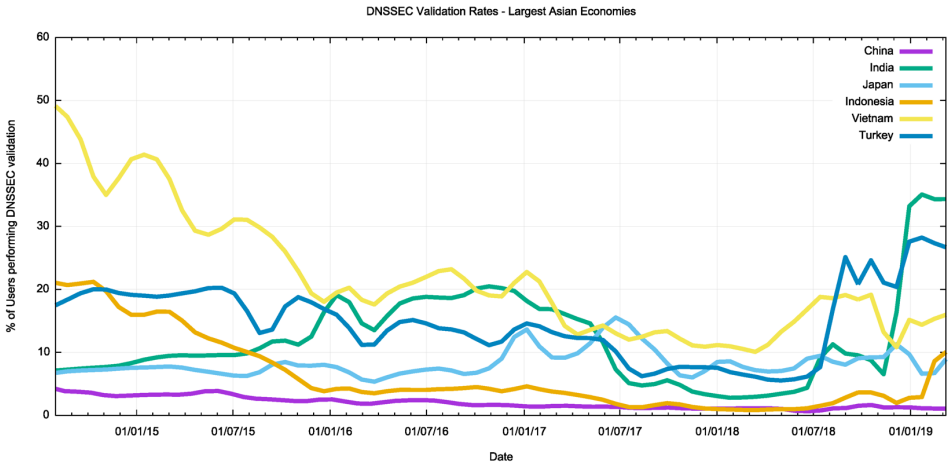


*Figure 7 – DNSSEC validation in the 6 largest Asian Economies*

The picture in China is one of a relatively small user base that use DNSSEC validating resolvers. Somewhat surprisingly there is a considerable level of use of Google's Public DNS services, and these days some 7% of Chinese uses have their DNS queries resolved through Google's DNS service.

It is in India that we see the best correlation of the Internet-wide DNSSEC validation numbers with national numbers. By late 2016 India had reached a significant milestone of 20% of users performing DNSSEC validation. However, across 2017 this number plummeted to 3% by the end of 2017. It is only

in the past 3 months has this situation reversed, and now the DNSSEC validation rate in India is some 33%.

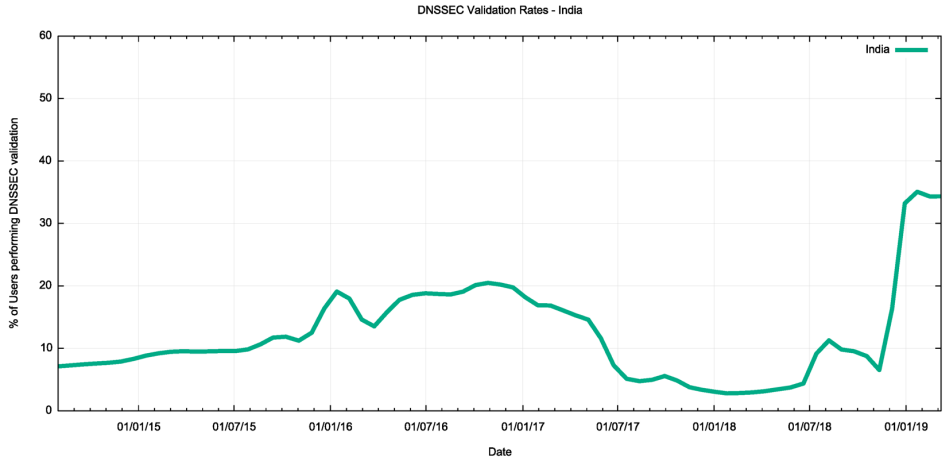


*Figure 8 – DNSSEC validation in India*

The recent rise in DNSSEC validation rates in India is largely due to measures taken within India's largest retail ISP, Reliance Jio (AS55836). This network made extensive use of Google's Public DNS service in 2014 and 2015 but turned to use its own resolvers in 2016. In recent months there is an observed rise in the use of Google's DNS service, but not at the same level as the rise in DNSSEC validation within that service provider (https://stats.labs.apnic.net/dnssec/AS55836).

A similar picture is visible for AS38266 (Vodaphone India), where deployment of DNSSEC-validating resolvers commenced in early 2018 in that network (https://stats.labs.apnic.net/dnssec/AS38266).

The picture of DNSSEC validation in Japan in a more conventional one., The level of adoption is still relatively low at some 8%-10% of the national user population, but the rise is consistent with a conventional "up and to the right" curve. Interestingly, this curve is consistent with the use of Google's DNS.

The opposite picture is the case in Indonesia, where a 25% use of DNSSEC validation in 2014 dropped to 1% in 2018. A more positive uptake trend is only visible in Indonesia in recent weeks. This profile is largely due to the state of DNSSEC validation within Telekomunikasi Indonesia (AS 17974), where a significant set of DNS queries were being directed to Google's service in 2014, and this was effectively turned off in 2015. The most significant recent change in Indonesia is the adoption of DNSSEC validation by Hutchinson (AS45727) (https://stats.labs.apnic.net/dnssec/AS45727).

## Why the fall in DNSSEC Validation in 2017 and 2018?

It's probably not coincidental that the roll of the root zone Key-Signing Key was originally scheduled to occur in October 2017. A significant effort was put into pushing out a message that DNSSEC-aware DNS resolvers needed to be tracking the roll of the KSK, and if they failed to follow the progress of the incoming key then the resolver would fail to answer any queries. The diagnostic tools for resolvers are pretty woeful., and it is a challenge even for operators of these resolvers to get the resolver to report on its trusted key state. It is quite conceivable that a number of resolver operators took the conservative option in 2017 and turned off DNSSEC validation as a way of avoiding potential service problems with the KSK roll.

In the case of the Indian DNS resolver operators DNSSEC validation was switched on again in late 2018, well after the 2018 KSK roll. There are no substantiated reports from these service operators as to why DNSSEC validation was switched off in 2017 and why it was resumed late in 2018, so the linking of this data with the KSK roll is simply supposition on my part. But in my opinion the hiatus in DNSSEC validation across the entire Internet was directly related to the extended period of the KSK roll. It seems entirely logical that many operators who were contemplating turning on validation in their resolver

infrastructure delayed the process until the KSK had been rolled and DNSSEC was once more considered to be "stable".

But this raises a more fundamental question about this technology. If operators feel that it is entirely reasonable to defer, or even turn off, a technology for more than a year then why turn it on at all? Its it not perceived as being a necessary or vital part of the DNS service portfolio then why bother? Let's take a look at exactly this question.

## Is DNSSEC worth it?

It seems that there is much uncertainty over the use of DNSSEC validation. Some resolver operators appear to have embraced DNSSEC and use it as a point of principle, including the large open resolver networks operated by Google and Cloudflare. On the other hand, there are resolver operator who do not perform DNSSEC validation. While DNSSEC validation is now being used by some 20% of the world's users, the other 80% are not.

So who's right? Is DNSSEC validation a good idea? Or is it a whole lot of effort with little in the way of tangible benefit?

There is no clear answer to this question. DNSSEC offers a more resilient and trustable DNS where users can trust that the DNS answers that they receive exactly match the authoritative zone contents. But this comes at a cost, and the issue is whether the benefits are worth the incremental costs of adding DNSSEC signatures in DNS zones and validating these signatures in DNS responses. Let's look at both sides of the issue.

### The Case for "No!"

It's easy to see DNSSEC as a case of one more thing to go wrong in the DNS. For DNS zone administrators it's another element to the zone administration tasks, adding key management, regular key updates, zone signing, key rollover, and coordination of keys with the parent zone and delegated zones. Even the simple elements of zone delegation and zone contents are mis-configured in much of the DNS and adding the elements of cryptographic keys and digital signatures only adds to the probability of zone failure for those who choose to sign their zone.

DNSSEC adds to the size of DNS responses, and this creates potential issues with the DNS. DNS over UDP is meant to fit responses within 512 bytes. Adding DNSSEC digital signatures generally causes the response size to exceed this limit. DNS queriers need to use EDNS extensions to specify their capability to handle large UDP responses and for larger responses there is the issue of IP packet fragmentation and the subtle differences between IPv4 and IPv6 in terms of IP packet fragmentation. The backstop of reversion to TCP adds additional time and additional unreliability as DNS over TCP is not universally supported in all DNS resolvers.

DNSSEC validation takes additional time. The need to assemble the DNSKEY and DS records of all of the parent zones without resolver caching would present an insurmountable time penalty. The use of resolver caches partly mitigates this additional penalty in resolution time, but in a world where every millisecond matters DNSSEC is an extravagant time waster!

Most end systems do not perform DNSSEC validation directly. They rely on their DNS resolver to perform DNSSEC validation on their behalf, and they implicitly trust in the resolver to perform this with appropriate levels of integrity. Of course, the issue here is that a man-in-the-middle attack between the end host and the validating resolver is still potentially effective: the end host is not validating the DNS response and cannot detect if a response is genuine or if it has been tampered with.

DNSSEC validation outcome signalling is inefficient. Validation failure re-uses the SERVFAIL response code, which acts as an invitation to the recursive resolver to spend more time performing re-queries using

different authoritative servers for the zone (which, admittedly, is an improvement on an earlier behaviour when the resolver would exhaustively check every possible delegation path!).

DNSSEC validation is variable. When and how do resolvers perform validation? Do they perform all the queries for DNSKEY and DS records before attempting validation? Do they serialize these DNS queries or perform them in parallel? What about CNAME records? Is the first name validated before following the CNAME or is the CNAME record followed and then both names validated? How do these additional tasks and the time taken to complete them interact with existing timers in the DNS? It appears that DNSSEC causes additional query load in the DNS because of this interaction between aggressive timers in the client and time to complete validation functions that need to be performed by resolvers.

Of course, there is also the really tough question: What threat is DNSSEC protecting you against? The textbook answer is to protect resolvers against the so-called "Kaminsky attack" that injects bad data into a recursive recover's cache. DNSSEC can certainly provide this protection, but only in a limited context. It can protect the recursive resolver, but the non-validating client stub is still as vulnerable as ever. Therefore, this is not a comprehensive solution to the problem. It's a step in the direction of threat mitigation by potentially protecting recursive resolvers against man-in-the middle attacks. But is the cost of this DNSSEC response commensurate with the nature of the threat? This particular DNS attack appears to be a rather esoteric attack vector and the use of randomised source ports in resolvers already adds sufficient randomness to make the Kaminsky guessing attack somewhat ineffective in any case.

The overall impression from this perspective is that DNSSEC is half-cooked and the costs far outweigh the potential benefit of risk mitigation.

## The Case for "Yes!"

The overall picture of security in the Internet is pretty woeful. The path between recognising a URL on a screen and clicking on it and believing that the presented result is actually the genuine article requires a fair amount of blind trust. We are trusting that the DNS mapping of the name to an IP address is genuine, trusting that the routing system is passing the IP packets to the 'correct' endpoint, trusting that the representation of the name on your screen is actually the name of the service you intended to go to, and trusting that the TLS connection is genuine, to name but a few.

That's a lot of trust and many would argue it's just too much trust. As we place more and more personal and social functions into a world of connected computers, we place more and more reliance on the integrity of the Internet. If an adversary can subvert the Internet's functions, then there is considerable potential for disruption and damage. The experience from repeated attacks so far is that adversaries, whether its talented hackers, criminal enterprises or state actors, can subvert the Internet's operation and infrastructure and can create considerable damage. And with the much-touted Internet of Things on the way we are about to over-populate this already compromised environment with even more devices, and place even greater levels of reliance on a foundation that is simply incapable of withstanding the pressure.

There is no single cure here and no single measure that will make it all better for the Internet's infrastructure. We need to improve the resilience of the addressing and routing infrastructure and we need to harden the DNS and make it more resistant to attempts to compromise it. DNSSEC may be a work in progress but as far as the DNS is concerned DNSSEC is all we have.

But let's not underestimate the value of a robust trustable name infrastructure. The trust infrastructure of the Web is hopelessly corrupted and the efforts on certificate transparency, HPKP records and CAA records are desperate and largely ineffectual measures that fail even when using a limited objective of palliative mitigation. If we want to provide essential web security then it appears that domain keys in the DNS are the best response we have to the issue (DANE), and that means we need to have a trustable DNS where users can verify DNS data as being authentic. And DNSSEC is the only way we know how to achieve that.

Work is going on with addressing some of the more obvious shortcomings of DNSSEC validated name resolution. A shift to use elliptical curve cryptography can reduce the size of digital signatures and reduce DNS packet sizes to avoid some of the issues related to IP packet fragmentation. The use of DNSSEC chained responses could improve the efficiency of DNSSEC validation, but at the expense of larger responses, which implies that such a move to use DNSSEC chain extensions in responses would make a lot of sense in a context of DNS-over-TLS or DNS-over-HTTPs, or as a stapled attribute in a TLS certificate exchange to facilitate the use of DANE as a CA-pinning measure. A refinement of the DNS error codes to explicitly signal DNSSEC validation failure would prevent the resolver re-query behaviour that we see with SERVFAIL signalling. Work is also underway to equip end hosts with DNSSEC validation capability, so that end hosts are not reliant on an untrusted (and vulnerable) connection between the host and their DNS resolver. And let's not forget that caching in the DNS is incredibly effective. The digital signatures in DNSSEC are cached in the same way as delegation and address records are held in the cache, so there will be no real time penalty for validated resolution of a signed DNS name if the relevant resource records are already held in the local cache.

Without a secure and trustable name infrastructure for the Internet, the prospects for the Internet look pretty bleak. DNSSEC is not the complete answer here, but it sure looks as if it's an essential element of a secure and trustable Internet. And maybe that's sufficient reason for us to adopt it. We can and should put in the technical effort to make DNSSEC more efficient and make it easier and faster to use. But we shouldn't let the perfect be the enemy of the good. There is no point in waiting for a "better" DNSSEC. We'll be waiting indefinitely, and the problems associated with a compromised digital infrastructure will persist. The alternative is to simply use what we have at hand with DNSSEC and use our ongoing experience to shape our further efforts to harden up both the DNS and the larger Internet infrastructure.

For securing the DNS there is no Plan B beyond DNSSEC. Any story relating to improving the security of the Internet necessarily entails securing the name system and that inevitably involves the use of DNSSEC.

The overall impression from this perspective is that DNSSEC is already deployable. But "deployable" is not the same as "completed", and the work is not finished by any means. Operational experience will guide the further refinement of DNSSEC tools and techniques.

## Disclaimer

The above views do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.

## Author

*Geoff Huston* B.Sc., M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region.

*www.potaroo.net*