POWERDNS

Getting DNSSEC deployed: costs and benefits[1]

Abstract

Three country code top-level domains have succeeded in getting a sizeable number of delegations DNSSEC secured. This document discusses how and why it happened in these three countries. Furthermore, it is examined if this experience can help us in understanding why access providers might or might not want to turn on validation. Finally, we present how PowerDNS will attempt to make DNSSEC acceptable for service providers.

Acknowledgements

We would like to thank Jason Livingood (Comcast), Daniel Federer (SIDN) and Rudolf van der Berg for their constructive comments and data points.

DNSSEC today

DNSSEC has been a tough sell. So tough that it has been ascribed properties it does not actually have, all in an effort to get people to deploy it.

DNSSEC does not stop spam, it does not prevent phishing, it does not prevent malware attacks. As a technology by itself, it is remarkably incapable of solving immediate problems.

However, DNSSEC does provide a source of authenticated and authentic data. This can be used to improve the robustness of DNS, protecting it from future attacks.

In addition, having a high speed, cached and resilient source of authentic data immediately spawns new possibilities. For example, details of certificates underlying the SSL protocol can be locked down via DNSSEC, preventing rogue operators from using working but fraudulently issued certificates.

Host public key details can similarly be published securely now, allowing for authenticated remote control of servers without blindly having to accept the initial new host key.

So even though it took a lot of work to deploy DNSSEC in a world that did not derive an immediate benefit, we are today in a situation where the infrastructure is out there, and we must now make sure that end-users will actually use our wonderfully fast authenticated data source.

This document outlines how we think we can achieve this.

[1] For more information, please contact bert.hubert@netherlabs.nl, or +31-622-440-095

How we got here

Initially, massive government sponsored efforts were exerted to get DNSSEC developed and to get the very root of the DNS signed, allowing for the rest of the top level domains to follow. This process has now nearly run its course, and every (cc)TLD of importance is now secured. Many of them are now also providing signed delegations through registrars, although not many registrars actually enable that feature for domain holders.

In several countries, significant success has been achieved. In the Czech republic, 37% of all .CZ domains are now signed and delegated securely. The Netherlands has achieved around 20%, and a record total of around 1.3 million signed delegations. Sweden has likewise seen high levels of DNSSEC deployment.

Why did that happen, and why in these three countries and not elsewhere? Three things are worthy of note:

- The Czech Republic, Sweden and The Netherlands all offered their registrars a credible incentive per signed delegation.
- In all these countries, the bulk of the signing has been performed using software that is fully automated and makes DNSSEC low maintenance
- All bulk signing activities happened in a close-knit community with the involvement of software developers, registrars and importantly the registry

To reproduce the successes of .CZ, .SE and .NL, it appears wise to make sure these three conditions are met.

Delving a little bit deeper, the country that saw the most spectacular speed of adoption (The Netherlands) had a number of things going for it:

- It was the third country, Sweden and the Czech Republic had shown that it could be done
- The incentive was aligned with the existing registry billing cycle, so registrars would not have to finance the migration for 12 months down the road.
- The registry was in good contact with its members, and made sure all knew about the program.
- Through strong outreach, including courses for technical and managerial staff of registrars, a lot of the fear surrounding DNSSEC was mitigated.
- Sweden's large deployments had made PowerDNS capable as a bulk DNSSEC server
- PowerDNS is a Dutch company with a lot of local contacts in the community

A similar thing occurred in the Czech Republic, where locally developed software was also used.

It is important to note that Sweden had had an incentive program in place long before secure signing really took off there. It is hypothesized that this is significant in terms of cost/benefit analyses.

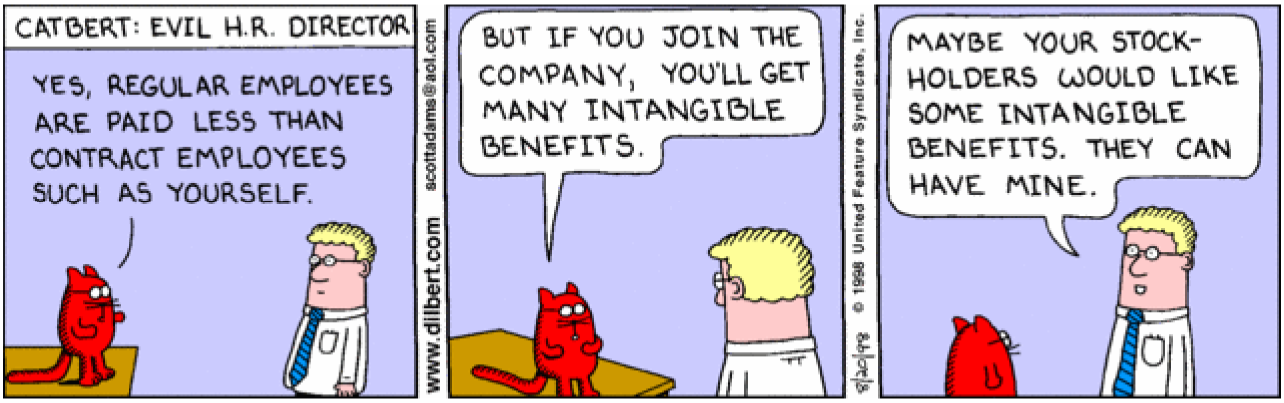
An open issue is that although many domains are now signed, the lack of validation means that misconfigurations remain undiscovered.

Finally, now that we've achieved '30%' levels in these ccTLDs, it is assumed that out of the remaining 70% we stand a chance of convincing the high-profile and security relevant domains to move to DNSSEC as well. It would be a tough sell for a bank to not do DNSSEC when the technology has in fact already been deployed by local restaurants!

Cost of deployment versus level of incentive

While commercial organizations are not as rational as economists often postulate, it is rare for a company to engage in activities that it thinks will continue to lose them money.

While early deployment of DNSSEC might come with intangible benefits, these are less compelling than their tangible brothers:


CATBERT: EVIL H.R. DIRECTOR
YES, REGULAR EMPLOYEES ARE PAID LESS THAN CONTRACT EMPLOYEES SUCH AS YOURSELF.
scottadams@aol.com
www.dilbert.com
BUT IF YOU JOIN THE COMPANY, YOU'LL GET MANY INTANGIBLE BENEFITS.
© 1998 United Feature Syndicate, Inc.
8/20/98
MAYBE YOUR STOCK-HOLDERS WOULD LIKE SOME INTANGIBLE BENEFITS. THEY CAN HAVE MINE.

From the three large scale countries referenced above, it can be observed that the incentives supplied were sufficient to motivate registrars to sign, but ONLY if they could do so with software specifically designed to make this easy and not increase their maintenance costs.

The Czech Republic had early success using homegrown tailor made software. Sweden did not initially have success until, together with PowerDNS they helped work out the bugs in that software. The Netherlands had instant success after instituting the ‘rapid satisfaction’ incentive program, because the required software was known and available.

Replicating this for the access providers

Access providers initially had little interest in deploying DNSSEC ‘since there were no DNSSEC signed domains to validate’. It is always easy to find a reason not to do something, and a reason that sounds good need not be the exclusive or ultimate reason.

Now that there is a lot to validate, we find that there still is very limited interest within the access provider community to start validating domains. The notable exception is the giant deployment of Comcast, as spearheaded by Jason Livingood. Comcast consciously decided to be competitive on security, as well as on the latest technology (IPv6 for example) in general.

Large access providers have revenues in the many billions of dollars and are therefore effectively out of reach for the registry community to incentivize them. Even a million dollars of ‘net incentive’ does not register at the decision making level of a nation-wide service provider.

From the registrar & hosting communities, it is clear however that success will only be achieved once the cost/benefit is at least not ‘obviously negative’. And for an access provider, it will never become ‘obviously positive’ through incentivization, unless billions are supplied.

So what CAN we do?

ARPU, customer service costs, churn

In the world of access providers a lot of decisions are based on the ARPU: Average Revenue Per User, or, how much money each customer brings in. The ARPU is generally well established, and not under tight control of the service providers. Trying to raise the ARPU scares off customers, and there is not typically a lot of room to lower it.

Given a semi-static ARPU, there is tremendous focus on its counterpart, the average expenses per user. Such expenses consist of hardware depreciation, Subscriber Acquisition Cost (SAC), customer support and (systems administration) staff. Like the ARPU, most of the costs are rather static - hardware can't be replaced overnight by cheaper variants, and firing significant amounts of your administration staff also comes with eventual downsides (see below on 'churn').

The only easily variable part in this equation is the cost of customer support. In short, if customers report fewer issues, it costs less to support them. A widely accepted number in the industry is that each support call costs over $25 (!).

So here is the access provider's dilemma - ARPU is reasonably static, and the total revenues consist of the number of users multiplied by the ARPU. The costs of the business however do go up when new customers arrive, but don't rapidly go down if they leave (for example, the hardware does not depreciate slower if it is used less).

This brings us to another component of service provider life: churn. Churn is how many of your customers depart, leaving you with having to earn back the 'Subscriber Acquisition Cost', and the hardware you'd had to buy to support the customer who has now left. Churn is therefore typically top of mind in the decision making process of a service provider.

Summarizing, for an access provider to control its short term profits, the two big knobs to twist are the **prevention of churn** and the **prevention of customer service calls**. All other effects are of a longer term nature.

DNSSEC, customer support costs & churn

As stated earlier, we can't make DNSSEC profitable for an access provider by giving them money. Also, if there is only the slightest hint of a suspicion that DNSSEC will lead to increased support costs, it immediately becomes unacceptable. If customers are confronted with important domain names that no longer work, this has the twin effects of increased number of support calls and potentially churn: "my domains DO work with your competitor [that does not do DNSSEC.]"

The obvious thing is then to make sure that DNSSEC will not increase support costs, but that only removes the initial barrier towards deploying DNSSEC. It still does not make it attractive, since no (tangible!) business benefit will be derived of it.

In order to make DNSSEC attractive, its deployment must be said to have the potential to **lower** customer dissatisfaction, which in turn will lead to less support calls and reduced churn. But how to make that happen?

DNS: the thing that always works except when it doesn't

DNS typically works well. DNS servers are monitored in bulk, and most service providers do measure (for example) average response times and failure rates. However, the rise of Google Public DNS and OpenDNS happened for a reason.

Typically these external DNS suppliers offer improved service compared to the service provider's own efforts. The external provider can afford lots more stringent monitoring of their DNS since it is their main business, and because they **need** to compete on DNS quality[2].

Most service providers currently do not have good non-bulk monitoring of DNS in place. If there are obvious disruptions, these get detected, but even a very high profile domain going out of service (for example, facebook.com) is typically discovered only after a spike in support calls.

And even if such a failure is detected, which usually has its origin in a temporary third party malfunction, it is tricky to wipe the faulty data from all servers, and such efforts will usually only be undertaken for very high profile domain names. We recall this happening for Facebook and the German national railways domains, for example.

But if service providers were to gain non-bulk ('domain specific') monitoring and easy service restoration, they could improve the customer experience measurably, both by proactively detecting problems and quickly instituting workarounds.

The offer: the realtime DNS console

What we at PowerDNS will be doing is to vastly improve the amount of statistics on failing domain names, concurrently with turning on DNSSEC. We are calling this the DNSSEC Console, which can be accessed via an HTML5 based web application. It talks to an entire PowerDNS Recursor constellation.

- A realtime overview of all domain names that are failing to resolve, and why
- For the top-1000 domains (for example), it will raise alerts if these fail to resolve, and take automatic measures to improve the situation
- It will allow operators to signal with one click to all their PowerDNS Recursors to forget bad data, or perhaps to replace it by old 'know good' IP addresses.
- For DNSSEC enabled domains, a single click will configure the acceptance of outdated (expired) cryptographic signatures for a selectable time period (default, one week).
- If DNSSEC for a domain is truly broken, again with a single click, the domain can be configured to forego DNSSEC validation for a selectable period of time.
    - This can also be configured for entire (cc)TLDs
- Such insight will correspond to a 'rolling window' of traffic, allowing for the quick resolution even of historic incidents ('I couldn't access cnn.com, but now it works all of a sudden').
- In addition, the recent increase in DNS reflection attacks will similarly be amenable to prevention and detection using the new console

This console is tied closely to DNSSEC, and the thinly veiled goal is to present the console as 'part of

[2] For service providers, having their customers 'defect' to such external DNS services represents bad news. For one thing, customers that call in with problems might in fact be reporting issues in third party infrastructure. Such calls still cost money.

Secondly, DNS is also typically used as internal infrastructure, for example to connect VoIP handsets to IP addresses that are nearby instead of at the other end of the country. This ability disappears once DNS is being provided by an external party.

DNSSEC validation'.

Through this console we think we can turn the 'net cost' of DNSSEC into a net advantage by virtue of reducing customer churn and the volume of support calls.

Some details

This console will be part of the mainline PowerDNS Recursor software and will, like all our software, be 100% open source. We want to move quickly to co-develop the console and DNSSEC in the recursor, so we can make sure we have a 'foot in the door' in the upgrade cycles.

All PowerDNS Recursor nodes will emit statistics to the central console; all nodes can be controlled from this console. The DNSSEC Console will automatically derive the 1000-10000 most requested domains that actually have been known to resolve. This is the 'active list', and it would include 'facebook.com', 'google.com' etc, but not include 'PRINTER.OFFICE' etc.

The 'active list' is treated specially - any issues on there lead to an alert status.

The performance impact of the DNSSEC Console is limited because Recursor nodes ship off their statistics to the console, and spend relatively little time working on the stats themselves. Being a nameserver is hard enough work!

The console is accessed via a command line, but also has a pretty HTML5 based frontend, probably built on top of one of the modern MVC JavaScript frameworks (backbone.js for example).