DNSSEC vs DNS-over-HTTPS: who do you trust?

ICANN 64 DNSSEC Workshop

Vittorio Bertola, Head of Policy & Innovation
Kobe, 13 March 2019

Stay Open. OX

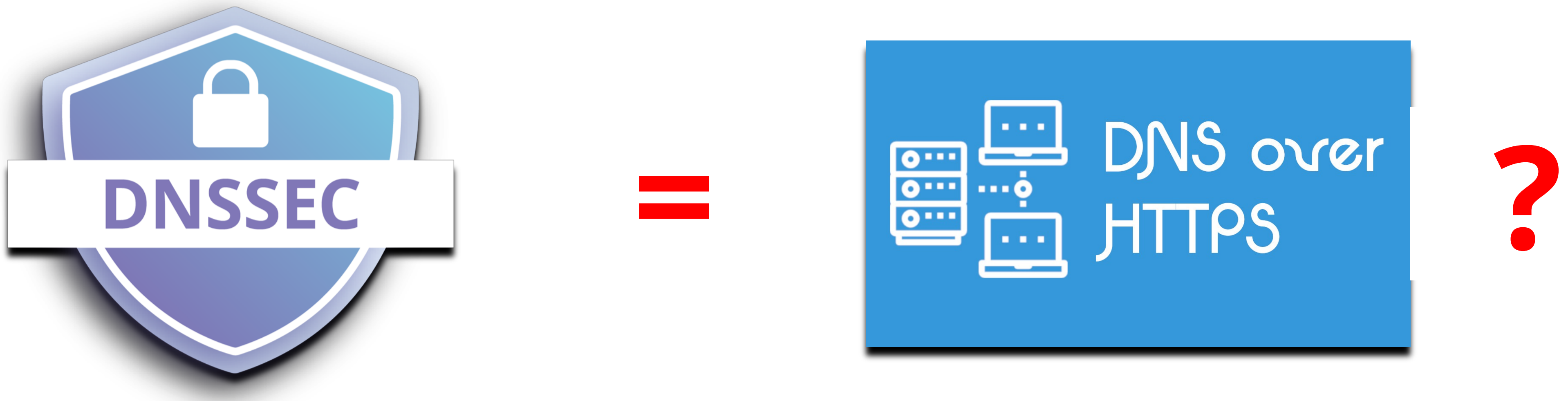
DNSSEC: the concept

- Adds **cryptographic signatures** to the replies
- **The communication is still unencrypted**, and everyone on the network can see your traffic
- Lower computational cost (signatures are pre-calculated)
- The [stub] resolver can verify the integrity of the reply by checking the signatures
- Provides **data security**
- Even if it is still possible to alter the reply during transport, if verification succeeds, **you can trust that the reply was not altered**

DNS-over-HTTPS: the concept

- **Encapsulates DNS** in HTTP and HTTP in TLS
- **The communication is encrypted**, and no one on the network can see your traffic
- Higher computational cost (everything is encrypted on the fly)
- The stub resolver cannot verify the integrity of the reply, but the reply can't be altered anyway
- Provides **channel security**
- It is not possible to alter the reply during transport, so **you can trust that the reply was not altered**

So someone might have an idea…



Ok, the two security mechanisms are different, but in the end,
they both ensure that the reply was not altered during its journey to the final user, so…

*…**why can’t we use DNS-over-HTTPS in place of DNSSEC?***

Hey, it’s a great idea!

<

!

DNS-over-HTTPS is actually better, because:

- *DNS-over-HTTPS gives you the same security on data that DNSSEC gives*
- *But DNS-over-HTTPS also makes your queries private!*
- *And it even authenticates the server you talk to, via PKI!*
- *And it is much easier to implement – look, no one could really make DNSSEC work in 20 years, but everyone already speaks HTTPS!*

The fallacy in this idea

You can trust that the reply was not altered!

…in respect to **the information provided by all the authoritative name servers** in the chain of DNS delegations.

You can trust that the reply was not altered!

…in respect to **the information provided by the recursive resolver**.

But wait! It’s just a matter of who you trust…

The oracle (the source of truth) is

the root server system

The oracle (the source of truth) is

your resolver

And what’s the truth, anyway?

- For some reason, the DNS people (and the ICANN leadership) seem to think that the DNS is still a single distributed ledger that gives you objective information
  - *«Ok, sometimes resolvers will mess with your replies, but these are dirty shortcuts that we admit for practical reasons»*
- Reality is that **DNS replies have been highly subjective for quite a while**, depending both on who is the client and which resolver is used
- Each resolver will give you a significant amount of replies that differ from those of another resolver (a factual survey would be interesting)
  - CDNs and geodistribution of content, DNS firewalls, voluntary content filters, government-mandated content filters, split horizons, local-only names…

Is there still truth in DNS?

A new DNS trust model

- Today, you are already expected to take whatever your resolver tells you as the truth
  - Including DNSSEC verification results!
- So if you just accept that **truth = what my resolver tells me** then using DNS-over-HTTPS in place of DNSSEC is perfectly fine, and it is actually simpler and better
- This could be done in a non-disruptive way
  - The stub resolver uses DoH to authenticate the recursive resolver and connect to it securely
  - The recursive resolver uses DNSSEC to make sure that it gets true replies from the authoritatives
- But this could also be done in a disruptive way
  - The resolver operator becomes the namespace owner and policymaker for all of its users
  - It could or could not use the root server system – it could answer queries however it likes
  - And if an operator controlled the broad majority of the global market…

Questions of the day

Who would users trust more, ICANN or the maker of their favourite browser?

Why should browsers implement DNSSEC, if they can just implement DoH and take over the DNS resolution in the meantime?

Thank you!

vittorio.bertola@open-xchange.com

Stay Open.