An overview of signing and DNSSEC deployment

João Damas
ISC
Overview

• Yes, let’s do it
• ...but, what does it mean to sign a zone?
• Administrative aspects of signing
• Operational aspects of signing
What does DNSSEC signing give you?

DNSSEC
• does not encrypt data
• does not identify the servers
• protects data against tampering while travelling the net

The equivalent of the green label is provided by the registrar checking the customer
Administrative aspects of signing

• Cost (making it smaller)
  – how big is the zone?
  – expected initial uptake?
  – where to keep the keys?

• From the above follow some operational consequences
Operational aspects

• Choosing keys
  – just follow widespread advice. Don’t be creative where you don’t need to be.

• Where to store the keys
  – HSMs
  – Offline machines
  – USB keys

• Document and publish your approach
  – there are models out there to be used [1]
Signing

One thing affects most operational considerations with DNSSEC

Signatures are BIG

www.isc.org  600 IN A 149.20.64.42
www.isc.org  581 IN RRSIG A 5 3 600 20101227233208 20101127233208 14457 isc.org. pBzL/ulDgwebXk46zGuFOzc49wPefgH8MfaCsMoyS3I GibJwv7V1/EguqENHUz7Q8a0plRhHPVh0+9bnDhPE0qvTBcHQUnfVqPrj6umAfqdyht1/vRqLYGvXcosPLcEHw84RJHFFIFTGw7C1Ohg9PI9UDNwvkMI1ChPuE5PmAs=
Signing

• a small detail

– Delegations and glue do **NOT** get **SIGNED**
– wonderful for a TLD
Signing - proof of $\exists$

- Proof of non-existence
  - A nameserver’s ability to tell you that there is no data for the question being asked and to prove it by signing the no-data answer
- Need to pre-compute
- NSEC (next secure)

```
dig mail2.isc.org +dnssec
```
```
mail.isc.org. 3600 IN NSEC manx.isc.org. A AAAA RRSIG NSEC
```
Signing - proof of ≠

- Duplicates the size of the zone (and then you add the size of the signatures)
  - zones become 4-7 times bigger
- to the rescue...
Signing - proof of NSEC3

- really stands for “you loose some, you gain some”
- Official excuse reason: privacy
- Real benefit: opt-out
  - allows a zone administrator to designate intervals in the zone for which no NSEC3 are generated
  - In a delegation heavy zone (e.g. a TLD), reduces the increase in size dramatically
Signing - proof of \( \notin \)

- Example
  .org has \( \approx 5000 \) NSEC3 records
    - mostly from A records that are not glue
    - Only these (and the .org records themselves) get signed
    - increment in size is minimal
Signing - proof of $\exists$

- What do you lose?
  - the proof of $\exists$ in the gaps
Operational impact

- Need to be careful with those keys
- Don’t let signatures expire (!)
- Estimate signing time - do it offline
- Check your available bandwidth
- Check the RAM (and disk) in your servers
- Publish your policy
- DO NOT FORGET THE REGISTRY
Conclusion

• It is doable
• There are various automation tools
• Understand what is being done
  – even if you outsource
• Go through the checklist
• Ask for assistance. We have all made mistakes
Questions?

Just ask now (DNSSEC is much more of a beast than we are)
Grab me (or us)
Send email 👉 joao@isc.org
References

• [1] draft-ietf-dnsop-dnssec-dps-framework-03.txt or successors
• http://www.dnssec.net/
• DNSSEC in 6 minutes