DNSSEC Updates

Icann 42, October 26th, 2011

About AFNIC

- ✓ Non-profit association founded in 1998.
- ✓ Operates 6 ccTLD (.fr/.re/.pm/.tf/.yt/.wf).
- ✓ More than 2 millions domain names.
- ✓ About 800 registrars (portfolio size varies from 1 to 640 000 domain names).
- ✓ DNSSEC was introduced in september 2010.

DNS publishing process in brief

- ✓ Zones dynamically updated (RFC 2136) every hour.
- ✓ NSEC3+Opt-Out.
- ✓ Use of OpenDNSSEC for key management, Bind+AEP Keyper HSM for math and signing stuff, homemade scripts to synchronize the whole thing and validate data.
- ✓ Zone signing keys (ZSK) of each zone are rolled over every 2 months.
- ✓ No Key Signing Key (KSK) rolled over yet… Planned for next year.

Rocky start…

- ✓ 3 outages during the first 6 months of operating of signed zones… ☹
- ✓ Each time noticeable, each time on .fr zone, each time at the worst possible time (it never happened on working-day when the whole technical team is at the office…).
- ✓ Each outage, while the bugs found were of different kind, happended during the key deletion process.
- ✓ The good news for the community is that we were able to find bugs in all applications we were using. They are now patched.
- ✓ At that point, we were close to decide to remove our ccTLDs DS records from the root zone.
- ✓ We had no problems with our small zones, and in this case, we can say that « size does matter » ☺

… but Proxy rocks

- ✓ No visibles outages since we have added our proxy system (6 months ago).
- ✓ Increase complexity of publication process while adding better control over zone changes.
- ✓ Add more complete DNSSEC validation step in the process.
- ✓ Improve monitoring system since.
- ✓ New plans to add new features to improve again and again the security of this mechanism.
- ✓ Work still in progress…

Where are the registrars ?

- ✓ 6 months ago, we launched our DNSSEC-aware version of Zonecheck as well as a new version of EPP server (RFC 5910/DS Data interface).

- ✓ In the same time we updated our web based registration system to deal with DNSSEC data.

- ✓ … but, there are only 30 domain names with DS records in our database as of October 11, 2011.

- ✓ … 1% of registrars have signed delegations.

- ✓ … and no DS was registered through our EPP server…

- ✓ We have just started a training program to educate our community. Too early to measure the impact.

- ✓ If we believe in social networks, some registrars should propose DNSSEC features to there clients in the next few months…

But are we ready for a DNSSEC rush ?

- ✓ In the same time, we decided to conduct some load tests to have an idea of our signing capabilities.
- ✓ We registered, during hours, DS records, at the maximum rate the system could handle them.
- ✓ We obtain mixed results.
- ✓ Incremental publishing process (Dynamic Update) used in normal operation works fine. Overhead is not significative.
- ✓ But, complete zone file generation, we use in case of emergency would take hours instead of minutes if we had DS records for all domain names.
- ✓ We plan to improve this mechanism in the next few months (fortunately, we have good tracks to drastically lower the process time).

Thank you !

www.afnic.fr
Vincent.Levigneron@afnic.fr