The Business Case for DNSSEC

Date: 27 Sep 2017

Organisation: The Internet Corporation for Assigned Names and Numbers (ICANN)

Author: Dr. Richard Lamb, Senior Program Manager of ICANN

Ever since Dan Kaminsky rang the alarm bell (DEFCON 2008) showing how the Internet's phone book could be manipulated to redirect users en masse to attacker sites, scrutiny on the Domain Name System (DNS) has intensified. In particular a technology called DNSSEC (DNS Security Extensions) has enjoyed brisk deployment[1] and received attention (press[2] and even Hollywood[3]).

Parties responsible for the Internet's core infrastructure such as ICANN, HKIRC (.HK), and VeriSign (.COM) have deployed comprehensive DNSSEC implementations to secure the top level of the Internet's phone book. All this to enable that a lookup for say, www.hkirc.hk (for techies[4]), returns the unmodified, cryptographic verified address corresponding to that web server (203.119.87.14) regardless of any man-in-the-middle attack. At the time of writing, over 90% of domain names such as hkirc.hk can lock down their DNS by deploying DNSSEC. Support at the validation end of DNSSEC has also shown steady progress[5] with services like 8.8.8.8/Google and large ISPs (e.g., COMCAST, PCCW) enabling DNSSEC.

However, deployment at the second level, e.g., google.com, has been disappointing (approximately 3-4%). Without deployment on popular sites, the full benefits of DNSSEC cannot be realized. Reasons range from perceived difficulty to deploy to lack of a "killer app". The author believes this lack of broad deployment for a nascent technology like DNSSEC, with wide

[1] Stats on DNSSEC deployment at the top https://rick.eng.br/dnssecstat/
[2] Guardian article on DNSSEC key management. Press does not get everything right but does help draw attention to cyber security https://www.theguardian.com/technology/2014/feb/28/seven-people-keys-worldwide-internet-security-web
[3] Hollywood takes notice. Nice write-up by my colleague. Like above, not quite right but helpful overall. http://kim.id.au/key-ceremony-primer/
[4] Shows the “chain of keys” and organizations used to build the “chain of trust” http://dnsviz.net/d/www.hkirc.hk/dnssec/
[5] Stats on DNSSEC validation in HK using novel analysis techniques. https://stats.labs.apnic.net/dnssec/HK?o=cXAw1x1g1r1

deployment at the Internet's core infrastructure but little at the edges, can be seen as a business opportunity[6].

Cursory inspection of DNS use reveals it is relied on for much more than just converting web site names into machine addresses. DNS look ups fall within the critical path for email, VOIP, and various authentication mechanisms as well, making securing it an important step toward helping stem cybercrime. Securing the DNS protects both business and customer. But most intriguing fact is that with DNSSEC the DNS turns into a global database for delivering content securely such as digital certificates (creating a global "PKI"), key material, and configuration data.

Many engineers have discovered this and new protocols and systems built on DNSSEC are being developed, published (e.g., DANE[7], XMPP[8], SMTP[9], SMIME[10]), and patented. Such a secure cross-organizational, transnational publication platform is a boon for innovative new security solutions (much needed in the Internet of Things world) and even that next "killer app".

Conclusion

The Internet has matured and along with it so has abuse. Built in a time of trust, new tools are now needed to combat this abuse.

DNSSEC is a step in upgrading the core infrastructure of the Internet to reinforce trust with cryptography. DNSSEC has thus far enjoyed steady deployment and the flow of innovative ideas to secure other parts of the Internet based on DNSSEC have just begun.

However, we need to do more. Without wider deployment onto popular services, the advantage now and in the future of a secured DNS will not be realized. It is the hope that thought leaders will help raise awareness to take advantage of the opportunities DNSSEC presents.

[6] https://www.co.tt/eeint/dnssecwhyee.pptx
[7] https://tools.ietf.org/pdf/rfc6698.pdf
[8] https://tools.ietf.org/pdf/rfc7673.pdf
[9] https://tools.ietf.org/pdf/rfc7672.pdf
[10] https://tools.ietf.org/pdf/rfc8162.pdf