

Ram Mohan Comments on DNSSEC at IGF, Vilnius

DNSSEC is considered by many to be the biggest structural improvement to the Internet in 20 years.

If you spend any time on the Internet browsing web pages, sending email or using social networks, you are using the Domain Name System (DNS) without even knowing it. The DNS translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. In other words, the Domain Name System (DNS) acts as the Internet's phone book associating human readable strings with various machine readable values, using a system of DNS servers that talk to each other.

Many of the protocols used on the Internet were developed during a period when the number of infrastructure providers was limited and trust between each of these providers could be assumed. Hence, communication with the various DNS servers was done "in the clear" with limited authenticity checking leaving it vulnerable to substitution or man in the middle attacks. This means that a user who clicks on a website link today is vulnerable to hijack to another website altogether, without the ability to control such a hijack. Worse, the user may click on a link or use email, and it is possible that access to their email is directed via a malicious server which listens in on their conversations – called a "man in the middle" attack.

DNS Security Extensions (DNSSEC) addresses this vulnerability by adding digital signature technology to the DNS hierarchy making substitution/redirection/man-in-the-middle attacks nearly impossible. This digital signature technology ensures that information returned from the DNS has not been modified while in transit from its authoritative source.

DNSSEC has been designed and implemented by the Internet community for the Internet community. In the same bottom-up, cooperative fashion that created the Internet, the Internet community has developed and is deploying DNSSEC at an aggressive rate.

DNSSEC is the result of almost two decades of cooperative development by the Internet Engineering Task Force (IETF). The result is a secure and efficient protocol with support and buy-in from the community.

Security researchers recently discovered improved exploits of the cache poisoning vulnerability, which resulted in a coordinated community-wide response to patch vulnerable systems, and eventually leading to accelerated DNSSEC deployment efforts.

DNSSEC deployment is a major milestone for the Internet, and is a significant success for the IETF, for ICANN and for the community of Internet users.

The DNS root was signed 15 July 2010. ICANN played a significant coordinating role in this effort, in association with VeriSign and the NTIA. This was a cooperative effort that incorporated direct involvement of the global Internet community in the management of the root key through regular key ceremonies.

The signing of the DNS root now allows Top Level Domain registries, registrars and domain name users to deploy DNSSEC with the surety that the chain of trust will be ensured from the top of the domain name system hierarchy.

DNSSEC Deployment has been faster than expected. With just a few trailblazing TLDs a year ago, now 20 TLDs have deployed DNSSEC and at least 14 others in preparation.

Once fully deployed, and with continued collaboration between the IETF, registries, registrars, network service providers and the community, DNSSEC is poised to become a cornerstone for Internet security as a common source of authentication and allows the continued use of the Internet as a secure platform for innovation, new product development and access to knowledge worldwide.