DNSSEC One Pager

Introduction

Since the Internet was developed in an era where trust between the relatively small handful of players was assumed, legacy DNS has little in the way of built in security – you ask a question, you get an answer – with only a few checks that a response corresponds to a particular question. Not surprisingly, with increased bandwidth and computational resources bad actors have found ways to effect a redirection of web, email, etc., traffic by lying to the DNS. Since DNS remembers or caches the lie, this can effect a large number of users. This attack is referred to as cache poisoning and was a call to action for the Internet community to "fix" the DNS. The result was DNS Security Extensions (DNSSEC). DNSSEC adds cryptographic records alongside existing DNS records that the DNS can use to verify that records have not been modified. This can guarantee that what a domain name holder puts into the DNS (e.g., an IP address) is what the end user gets unchanged.

Talking Points:

- All devices on the Internet have Internet Protocol (IP) addresses. Connections are established and data transferred between a pair of IP addresses. To ease use by humans these IP addresses are associated with domain names. The Domain Name System (DNS) was developed in 1983 to convert between domain names and IP addresses.

- The increase in bandwidth and computational speed since the DNS was originally developed has allowed attackers to easily exploit vulnerabilities. These vulnerabilities allow attackers to insert modified responses that redirect users to malicious web sites and services.

- When such an attack is carried out on the element of the DNS infrastructure typically performing the domain name to IP address lookup (referred to as a "resolver"), it effects all who rely on this service. This is called cache poisoning.

- DNS Security Extensions (DNSSEC) was developed by the IETF (same body that created the core Internet protocols themselves, e.g., TCP/IP) to addresses this problem. DNSSEC works by adding digital signatures to DNS responses that the resolver can use to validate good responses and discard surreptitiously modified ones.

- DNSSEC is the biggest security upgrade to Internet infrastructure in over 20 years. But it is important to note that DNSSEC does not fix all the security ills of the Internet. It is just one step that has potential to secure much more than only DNS.

- ICANN's role in DNSSEC is as evangelist and manager of DNSSEC root key alongside historical root zone management duties. To address any political sensitivities, root key management is carried out with the direct participation of 21 trusted community representatives in 4 "key ceremonies" per year held in our key management facilities in El Segundo, CA and Culpepper, VA.

- The ubiquitous reliance on DNS in all aspects of on-line transactions (much more than just web browsing) make securing the DNS of critical importance. Furthermore, the cross-organizational and trans-national nature of a secured DNS make it a platform for delivery of other data to support innovative security solutions. This is exemplified by developments in the IETF that rely on DNSSEC to secure web and email (e.g., DANE), to supporting Smart-Grid efforts, and helping secure the Internet of things.

- The Internet's infrastructure is well on its way to fully supporting DNSSEC (deployed on +85% TLDs). However, for DNSSEC to be effective individual domain names must be signed as well. This has been a difficult goal to achieve with only approximately 3% of names currently signed. It is therefore important for us to continue DNSSEC awareness raising efforts.