DNS Security Extensions (DNSSEC)

DNS Security Extensions (DNSSEC) was first introduced in the mid-1990s as an additional security measure to protect the DNS from cache poisoning exploits (recently referred to as the Kaminsky bug) which can allow a bad actor to get in the middle of an Internet users' request to access a Web site without their knowledge. DNSSEC introduces digital signatures to the DNS infrastructure, allowing end users to more securely navigate the Internet. It can provide users with effective verification that their applications, such as Web or email, are using the correct addresses for servers they want to reach.

What does DNSSEC do?

The DNS system is hierarchical and works like a collection of phone books with the address of each "zone" or site you can access on the Internet. Each level of this hierarchy is "authoritative" for the level just below it. For instance, the "Root" that is maintained by the IANA contains information about all of the TLDs (e.g.: .com, .org, .info) and who is responsible for them. The .info registry will contain information about all .info Web sites e.g.: afilias.info. But Afilias is authoritative for afilias.info and it is the only party who knows all of the subzones assigned to that domain name, such as www for the public Web site or "mail" for staff members to access email.

When an Internet user wants to get to www.afilias.info a DNS resolver embedded into their operating system on their computer automatically knows to ask for the address of this site, and that request is sent through this entire chain to get to the IP address where www.afilias.info lives ultimately displaying the Web site in your Web browser.

At each step in the process only simple yes/no responses are given and there is no authentication of who is actually saying "yes" this is the address for www.afilias.info . So if a bad actor where to get into the middle of the user's request and say "yes I have the address," they could point the user to another site entirely. The long term potential risk is that that bad actor will point the user to somewhere that will damage your brand, or damage the user by infecting them with malware or conduct a phishing scheme.

DNSSEC secures this process by establishing a "chain of trust" that effectively asks for a secret password or "key" in order to exchange the information at each level. DNSSEC-based authentication is the key to identifying potential risks and providing a distributed, secure naming mechanism that can be leveraged for new services.

Key signing

To implement DNSSEC a pair of public-private keys are used to sign a zone (e.g.: www.afilias.info, or mail.afilias.info) digitally. Either the person responsible for administering that zone or their DNS service provider then must host signed zones with a DNSSEC-compliant name server. When the zone has been signed, applications like Web browsers and email can use the digital signatures to provide secure services to those requesting to access that signed zone.

In order to manage DNSSEC keys, including continually rotating keys (a.k.a. Key Rollover), the zone administrator must use specialized DNSSEC software and hardware. Additional these “keys” must be distributed to the proper “trust anchors” through the Internet so validation can be completed. These can be standalone tools or add-ons to your existing DNS software. Some vendors sell dedicated "DNSSEC Appliances", which acts as an automated DNS signer for DNS zones and managing keys.

DNSSEC adoption

One of the key stumbling blocks to DNSSEC adoption has been that the implementation of new DNSSEC hardware and software to sign zones is complicated and time consuming. In addition, the continual management of keys and ensuring their security is an added task that many organizations do not have the skill set or budget to accommodate. Afilias' 1-Click DNSSEC™ solution, solves this problem by providing both a world class DNS service to manage traffic to your zones, and enabling DNSSEC with just one click.

Current DNSSEC developments

The Public Interest Registry has publicly announced that the .org registry will be signed in 2009. The United States Office of Management and Budget also issued a mandate in 2008 that .gov be signed in 2009. The NTIA is also considering the implications of signing the Root.