

## Workshop: DNS and Root Zone File Management

**Date:** November 1, 2006

**Time:** 17:30-19:00

**Location:** Workshop Room II, Divani Apollon Hotel and Spa

### Panel Participants:

Brian Cute, VP Government Relations, VeriSign

Frederico Neves, Member, SSAC; Director of Services and Technology, Registro.br

Lars-Johan Liman, Autonomica.se

Marilyn Cade, Member, ICANN GNSO

Milton Mueller, Partner, Internet Governance Project

Riaz Tayoub, Third World Network

Thierry Moreau, Connotech

### Sponsored by:

The Third World Network

Government of Brazil

Internet Governance Project

The Domain Name System (DNS) is a critical part of the Internet's infrastructure. The DNS has served Internet users well, but it has some well-known vulnerabilities.<sup>1</sup> These problems can be exploited to redirect requests to bogus servers and engage in disruptive or criminal acts which can threaten commerce, reputation, or security.

In response to these threats, the IETF proposed the Domain Name System Security Extensions (DNSSEC). DNSSEC introduces public-key cryptographic signatures into the DNS infrastructure to ensure the integrity and authenticity of information retrieved by DNS resolver queries. Proper implementation of DNSSEC requires procedures to securely manage the cryptographic keys.

DNSSEC would address an increasingly common threat on the Internet today, website spoofing used for data phishing. Also, widespread adoption of DNSSEC would create a globally accessible, authenticatable infrastructure for the secure distribution of other information. As such, it could contribute to resolving problems in email based SPAM (e.g., DKIM), identity management (e.g., OpenID), and public-key and certificate management for encrypted communications systems (e.g., SSH).

To be universally secure, DNSSEC imposes a top-down model of trust following the DNS name hierarchy. Resolvers would rely on a cryptographically-signed root zone as a "trust anchor" to authenticate zones for top-level domains, second-level domains, etc., using digital signature chains similar to certificate chains. The model assumes that lower-level zones are securely delegated by their inclusion in their parent zone file.

Will the root be signed? If so, who and how will the keys be managed? Who will decide if and how zones are delegated from the root? The security policy choices (e.g., key generation, signing, rollover) and operational procedures (e.g., transparency, accountability) governing the root zone will impact all root server operators, all domain name registries (including ccTLDs), as well as DNS name server operators, resolver software and application developers, and end users. If the root zone doesn't solve this problem, TLDs and second-level domains will be "islands of trust" and will have to come up with their own solutions on how to distribute and rollover their own public keys securely.

In short, **DNSSEC is not simply a technical issue but a major governance problem.** It significantly expands the technical requirements, difficulty and costs of running the DNS. It also increases the importance of the procedures for Root Zone File (RZF) management. This critical issue needs to be discussed openly and the issues more widely understood.

<sup>1</sup> See *Signposts in Cyberspace*, National Research Council (2005).