Date: June 28, 2006

To: DNSTransition@ntia.doc.gov

Fiona Alexander
Office of International Affairs
National Telecommunications and Information Administration
1401 Constitution Avenue, NW., Room 4701,
Washington, DC 20230
USA

Subject: DNS Transition Notice of Inquiry Contribution -- re DNSSEC Deployment at the DNS Root

From: Thierry Moreau
thierry.moreau@connotech.com

CONNOTECH Experts-conseils, inc.
9130 Place de Montgolfier
Montreal, Qc
Canada H2M 2A1

Tel.: (514)385-5691

Dear Ms Alexander:

In response to the NTIA Notice of Inquiry on the Internet Technical Coordination Transition, I submit the following contribution, not addressing a specific question. I notice the strong commitment of the US Government to its role in the ICANN institutional framework, which the following contribution abstain from questioning directly. Instead, I present an analysis of a specific aspect of Internet evolution, with the humble hope to assist policy development and governance in an environment of increased reliance on the DNS data for ever more critical applications.

Best Regards,

Thierry Moreau

1. Introduction

The DNS governance NoI (Notice of Inquiry) from NTIA is a welcome initiative. I use this opportunity to discuss the DNS integrity vulnerability that was not a significant concern in 1998, and the DNSSEC protocol development project which addresses this integrity vulnerability. The DNSSEC emerging technology deserves explanations, hence the extensiveness of the present NoI contribution. In these explanations, I attempt to reflect views prevailing in specialized circles, but I also present personal opinions generally based on forward looking analysis of DNS governance issues created by the attempt to fix the DNS integrity vulnerability. However, the present NoI contribution is not written as a tutorial: a text portion may be based on notions discussed in greater details later in the document.

2. The DNS Integrity Vulnerability

It is well known that data retrieved from the DNS is not protected by any integrity mechanism that would prevent data tampering between zone data publication by the DNS zone administrator and Internet user reliance on this data. I refer to this as the DNS integrity vulnerability. DNS cache poisoning is a type of IT security attack that exploits the DNS integrity vulnerability.

Does the DNS integrity vulnerability really matter? In discussing this question, we get a sense of the demand for IT security technology, i.e. an intriguing paradox between the ever increasing set of attacks on e-commerce operators (including e-government and online banking) and the limited effectiveness of any workable IT security mechanism. A magic fix of the DNS integrity vulnerability would directly solve a limited set of attacks (reference [1]), but it is doubtful that any encompassing approach to e-commerce security can be drafted without addressing the DNS integrity vulnerability. While the DNS integrity vulnerability definitely needs to be addressed from the perspective of an educated observer of Internet security, the application use of any DNS integrity mechanism is currently absent, and the impact on human factors still needs attention. In summary, some latent demand exists for improving DNS integrity as an e-commerce strengthening measure; the timing is as soon as possible; but the measurable benefits are indirect and contingent on application support of DNS services not currently available.

Some niche applications would benefit from a fix for the DNS integrity vulnerability. Here is some explanation on their generic relationship to the DNS vulnerability. The primary use of the global DNS database is the translation of domain names to host addresses. But the DNS has other uses, based on its distributed database arrangement, providing on-line access to “resource records” indexed by domain names. Some of these DNS alternate uses may benefit from a solution to the DNS integrity vulnerability, notably the distribution of cryptographic keys associated with domain

names. There are current developments for two applications which would rely on DNS distributed cryptographic keys: unsolicited bulk e-mail prevention or filtering, and message encryption. These two emerging Internet security schemes would clearly benefit from a solution to the DNS integrity vulnerability, but would still provide security with the current DNS, at a reduced level.

It is not a purpose of the present NoI contribution to comprehensively review the security schemes which depend of a solution to the DNS integrity vulnerability, but a list of references certainly supports the emergence of a recurring pattern. In the case of unsolicited bulk e-mail filtering, two protocol development initiatives can be cited:

- DKIM (DomainKeys Identified Mail Signatures) (reference [2]), and
- SPF (Sender Policy Framework) (references [3], [4], [5], [6], and [7]).

In the case of message encryption supported by DNS distribution of cryptographic keys, some of the current protocol developments can be cited:

- an update to a general purpose specification for storing cryptographic keys in the DNS, intended notably to support OpenPGP public encryption keys (reference [8]),
- the opportunistic encryption protocol development, which appears as a comprehensive application development initiative (references [9] and [10]),
- an enhancement to the SSH (Secure SHell) that uses the DNS as a trust distribution mechanism for public encryption keys (reference [11]), and
- the current HIP (Host Identity Protocol) architecture development also relies on the DNS for trusted public key distribution (reference [12]).

It remains to be seen whether any subset of these initiatives will drive sufficient demand for fixing the DNS integrity vulnerability in the scope of the global DNS.

3. Impact of DNS Support for IT Security Schemes

There are possible policy implications in the distribution of trusted public encryption keys in the global DNS in which the integrity vulnerability would have been addressed. These policy implications are linked to government imposed controls on encryption technologies. Network traffic encryption technologies are readily available nowadays; however, one can argue that ubiquitous trusted encryption key distribution does not exist yet, based on the ease with which end-users can be deceived by browser X.509 certificate spoofing, including tampering with self-signed certificate configuration. The emergence of a different strategy for large-scale distribution of encryption public keys is likely to trigger questioning in some of the government offices having a “national security” mandate. In this regard, the relaxation of export controls on encryption items by the United States (back in year 2000) should not be mistaken as a global elimination of government imposed controls on encryption technologies.

It is obvious that if the above suspected encryption controls concerns are real, they

would inextricably relate to the international nature of the global DNS. This is compounded by fact that the *application uses* of the DNS would be targeted by the government control scrutiny, while DNS technical coordination and policy development has historically focused on the *name registration* aspect of the DNS.

4. The DNSSEC Protocol Extension

Up to now, I didn't mention DNSSEC a solution to the DNS integrity vulnerability. Indeed, DNSSEC is the only proposal that addresses this vulnerability, originated from a decade-long protocol development effort in the IETF (references [13], [14], and [15]), notably with the bind software supplier as a flagship open source implementation (reference [16]). It is not a purpose of the present NoI contribution to explain the DNSSEC security technology besides what is relevant to identify current and potential stakeholders and policy implications of the technology.

The DNSSEC security architecture is both conceptually simple and intricate at the implementation level. In a nutshell, the DNS security services are provided with the public key digital signature technology applied in batch mode, i.e. the DNS data is digitally signed when it is changed in the distributed database, and not when it is requested in a DNS query. Moreover, the DNSSEC chains of digital signatures are structured along the DNS tree structured name space: this superimposes a trust model over a delegation scheme that was originally intended for database maintenance operational duties. The DNS technical coordination burden associated with DNSSEC deployment is thus closely linked to the DNS root zone administration, and the term "DNS root zone singing" is understood among specialized forums as referring to the necessary procedures and operations for DNSSEC support at the DNS root, within the institutional framework subject to the NTIA NoI.

Currently, DNSSEC is deployed operationally in at least one TLD, namely the Swedish .se TLD (reference [17]). Another noteworthy deployment effort occurs at RIPE NCC (Reséaux IP Européens Network Coordination Center) (reference [18]), with a coverage limited to portions of the DNS hierarchy but with a rich set of support documentation and software utilities. There are other limited-scope experiments, and a few TLD administrations are planning DNSSEC deployment. DNSSEC adoption signals from US government comes through a few NIST publications, including a detailed guidelines document (reference [19]), and a formal designation as a recommended security control in an IT security standard applicable to the US government (reference [20]), where secure name lookup service is referred under acronyms SC-20 and SC-21, respectively for DNS authoritative source and DNS resolution. None of these DNSSEC deployment initiatives cover the trust anchor key management issues to be explained shortly.

There is still on-going work on DNSSEC protocols. Progress is being made on the

NSEC3 work item, a privacy enhancement mechanism, more specifically a countermeasure against unauthorized collection of every domain name in a given DNS zone, a possibility inadvertently introduced in the DNSSEC protocol ("privacy" is not to be confused with "confidentiality" in the context of NSEC3). Progress is less clear for the issue called "trust anchor key management," (an alternate term is "automated trust anchor key rollover," focusing on the required technical functionality). Trust anchor key management refers to the security procedures surrounding the DNS root signature key (the trust "anchor" is tied to the "end of the chain" of digital signatures along the DNS name hierarchy). It is thus an IETF work item related to the institutional framework subject to the NTIA NoI. As the promoter of a patent-pending solution for automated trust anchor key rollover, I am an interested observer of any initiative which might ease the DNSSEC deployment at the DNS root and TLDs, including sensible trust anchor key management procedures.

There are also important issues for deployment. The DNSSEC operational burden on registries and registrars can hardly be ignored, and a DNSSEC business model for the highly price competitive registrar market is yet to emerge. Moreover, DNSSEC, as a global service upgrade in the Internet, faces the chicken-and-egg acceptance paradox, where the end-user benefits seems to materialize only when some critical mass of DNS nameserver support is reached. Other important issues for effectiveness in providing DNS data assurance include application software support, and an unbounded security awareness campaign: after all, it is the end-user who makes the ultimate decision to rely on computer results based on DNS provided data. Some of these issues are relevant to the institutional framework subject to the NTIA NoI.

5. The Policy Implications of DNSSEC

The DNSSEC security technology is "almost ready for field deployment," but this assessment has been made for years, with repeated postponements. As the list of outstanding issues slowly shortens, the toughest issues remain, including the policy implications at the DNS root and TLD levels. The intricacies of "DNS root signing politics" are often mentioned, but seldom described. In the present contribution to the NoI, I attempt to describe these DNSSEC policy implications at a greater level of details than in other public accounts (in this regard, reference [21] is a presentation which I find the most comprehensive).

The DNSSEC deployment has implications at the DNS root level, including:

- signing the root zone file whenever it is edited (which implies defining technological and organizational controls of the signature private key),
- adding secure delegations in the DNS root zone file as TLDs introduce DNSSEC support in their operations, and
- periodically following the procedures implied by an automated trust anchor key rollover scheme to be adopted (in this context "automation" applies to the

validating resolver side of the DNS data distribution process, and not to the DNS root authoritative server side).

These are new operational requirements tainted by the incremental security provided by the DNSSEC technology architecture. Some observers expressed the desire to see these operational requirements to be fulfilled without any impact on DNS root administration policy debates. Indeed, such a course of events would allow smooth introduction of DNSSEC, in a timely manner at the DNS root and, in the global Internet, at the pace of the emerging demand for fixing the DNS integrity vulnerability.

However, my understanding of the DNSSEC deployment within the institutional framework subject to the NTIA NoI let me identify some governance issues:

- the mere novelty of meeting increasing expectations of cryptographic assurance for the DNS, given the criticalness of DNS root administration,
- the above question on encryption key distribution, and
- specific characteristics of the end-to-end data assurance built-in the DNSSEC protocols, including
  - cost recovery for operational duties that can not entirely disappear through the on-going cost decline for IT hardware and network connectivity,
  - possible increased liability for DNS zone content errors,
  - a novel dependency on DNS resolver software distribution for proper initial trust anchor key configuration, and
  - the expectations of transparency and auditability for DNSSEC root signature key procedures, while a private signature key is, by definition, a concealed data element.

This list is just mine; I can't predict how DNSSEC adoption and deployment requirements will be handled by the organizations involved in the DNS root support.

6. DNSSEC Deployment Efforts in Current Institutional Framework

We can make an historical review of ICANN reaction to the DNSSEC development activities. The first mention of DNSSEC in the ICANN activity reports to the US DoC are in March 2003 (reference [22]), as an area of attention for the SSAC (Security and Stability Advisory Committee). In October 2005, the ICANN actual involvement with DNSSEC amounted to little more than taking note of progress made in other Internet organizations: “ICANN has provided opportunities to promote DNSSEC to its constituents [...]. Many of the developers of DNSSEC are directly involved in the ICANN process[...]” (references [23] and [24]). I see no sign of any work actually done within ICANN, or under the auspices of ICANN.

However, there is now consideration of a DNSSEC deployment at the management level at ICANN. A foremost sign is the root transition agreement (reference [25]) which is part of the ICANN-Verisign lawsuit settlement agreement currently pending

DoC approval. The root transition agreement appears as a contractual arrangement for DNSSEC deployment at the DNS root by ICANN, Verisign, and the US DoC, with input from the IAB. But the vagueness of this document wording let me qualify it as an "agreement to agree," which I believe is dubious practice in contract negotiations, even more so when the negotiations are in the context of a pending dispute resolution. In any event, the root transition agreement seemed to be echoed in the latest ICANN operational plan (reference [26]) where the DNSSEC deployment activity is described as "Determine timetable, coordination requirements and costs for full deployment."

In summary, there has been little actual ICANN involvement in the DNSSEC deployment initiative, and certainly no leadership in either policy development, or assertion that DNSSEC deployment is devoid of policy implications.

The other institutional angle to DNSSEC is focused on the protocol development, mainly with the IETF, as a consensus-based engineering organization, and the IAB, as a liaison between IETF/IESG protocol development and the operational perspective of ICANN. There is a cultural gap between the voluntary-participation-based IETF working groups, including the DNSEXT working group mandated for DNSSEC protocol development, and the operational accountability demands on the more formal ICANN processes. I personally see this cultural gap impeding progress towards adoption of a good automated trust anchor key rollover solution for the DNS root signature key.

7. Summary Observation and Recommendations

My foremost summary observation is that DNSSEC deployment adds specific technical coordination issues to the list of ICANN coordination functions, and to the extent that the prior functions were not performed as originally intended and/or to the expectations of Internet community participants, there is little chance for the current institutional framework to be effective in providing DNSSEC support at the root.

According to the DoC statement of June 2005, DoC maintains its "historic role in authorizing changes or modifications to the authoritative root zone file." (reference [27]) Irrespective of which organization has formal authority over ICANN, I may state recommendations for guidance from such an organization to ICANN (or successor) about DNSSEC deployment.

7.1 Don't Use DNSSEC Support at Root Level for to Control Encryption Key Distribution

The recommendation reads as follows:

> Whichever organization has formal authority over ICANN should make a statement to the effect that the decision to include a DNSSEC secure delegation in the authoritative root zone file shall not be dependent on any

regulations (or other form of control) governing the encryption key distribution in the TLD and/or its second level domains and below.

7.2 Help the Emergence of a "DNSSEC Business Model"

The recommendation reads as follows:

> Whichever organization has formal authority over ICANN should provide a directive to ICANN to timely establish a price regulation policy for DNSSEC, i.e. applicable to second-level domain name registrations that are targeted by a DNSSEC secure delegation in addition to their plain DNS name registration.

A policy formulation is desirable even if it boils down to a zero price for the DNSSEC secure delegation option at the TLD registry level.

7.3 Avoid Contractual Restrictions on DNSSEC Secure Delegations from the Root

The recommendation reads as follows:

> Whichever organization has formal authority over ICANN should provide a directive to ICANN to timely establish a DNSSEC technical coordination policy with the objective of minimal preconditions for DNSSEC secure delegations in the DNS authoritative root zone file.

E.g. the precondition might be limited to a provision where the TLD administrator acknowledges that DNSSEC private signature keys deserve protection by commercially acceptable security procedures. Another way to see this recommendation is that the DNSSEC secure delegation option from the root should be provided almost automatically, and not contingent upon a formal contractual relationship where one does not exist prior to DNSSEC support by the TLD.

Note that the above three recommendations focus on DNS governance, while ICANN is expected to develop the required operational procedures (e.g. for implementation characteristics of the digital signature technology -- who controls the root signature key) as part of its technical coordination functions.

In the absence of such guidance from whichever organization has formal authority over ICANN, uncertainty will remain in these three aspects of DNSSEC deployment at the root, and a realistic deployment timetable is unlikely to emerge. For Internet participants wishing to see an end to the DNS integrity vulnerability, lack of progress at DNSSEC deployment at the root due to ICANN inefficiency in policy development is perhaps an hopeless circumstance. Conversely, the stakeholders questioning the current ICANN institutional framework for limited actual support of Internet evolution would see the DNSSEC deployment delays as yet another argument for radical change.

The above is my attempt to make a structured analysis of DNSSEC for policy

development and governance purposes, with focus at the DNS root. At the TLD administration level, there appears diverse environments which might shape diverse approaches to DNSSEC deployment. If the DNS root administration is seen as a service to a federation of TLD administrations, attention should be paid to a TLD administration perspective, which I did not address. Moreover, it should be noted that ICANN inaction is used as a justification for at least one initiative that circumvent the lack of DNSSEC support at the root.

In summary, DNSSEC deployment somehow rests on whichever organization has formal authority over ICANN, e.g. with respect to the three above recommendations. Otherwise, many of the above issues deserve to be addressed in forums organized by ICANN for to achieve meaningful participation and representation of key stakeholders through this significant Internet evolution. This is obviously not occurring as it should.

References

[1] Aaron Emigh, "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures", Radix Labs, October 3, 2005, available at http://www.antiphishing.org/Phishing-dhs-report.pdf -- note that some experts involved in the preparation of this report acknowledged the editorial oversight of omitting DNSSEC as a countermeasure for the DNS integrity vulnerability.

[2] E. Allman, J. Callas, M. Delany, M. Libbey, J. Fenton, M. Thomas, "DomainKeys Identified Mail Signatures (DKIM)", May 22, 2006, draft-ietf-dkim-base-02, http://www.ietf.org/internet-drafts/draft-ietf-dkim-base-02.txt, see also http://www.ietf.org/html.charters/dkim-charter.html

[3] Mark Delany, "Domain-based Email Authentication Using Public-Keys Advertised in the DNS (DomainKeys)", 27 March 2006, http://www.ietf.org/internet-drafts/draft-delany-domainkeys-base-04.txt

[4] E. Allman, H. Katz, "SMTP Service Extension for Indicating the Responsible Submitter of an E-Mail Message", RFC4405, April 2006.

[5] J. Lyon, M. Wong, "Sender ID: Authenticating E-Mail", RFC4406, April 2006.

[6] J. Lyon, "Purported Responsible Address in E-Mail Messages", RFC4407, April 2006.

[7] M. Wong, W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", RFC4408, April 2006.

[8] S. Josefsson, "Storing Certificates in the Domain Name System (DNS)", RFC4398, March 2006

[9] M. Richardson, "A Method for Storing IPsec Keying Material in DNS", RFC4025, March 2005

[10] M. Richardson, D.H. Redelmeier, "Opportunistic Encryption using the Internet Key Exchange (IKE)", RFC4322, December 2005

[11] J. Schlyter, W. Griffin, "Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints", RFC4255, January 2006

[12] P. Nikander, J. Laganier, "Host Identity Protocol (HIP) Domain Name System (DNS) Extensions", February 24, 2006, http://www.ietf.org/internet-drafts/draft-ietf-hip-dns-06.txt

[13] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005

[14] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005

[15] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005

[16] Internet Systems Consortium, ISC BIND, http://www.isc.org/index.pl

[17] DNSSEC(.se) -- signed since 13th September 2005, http://dnssec.nic.se/

[18] DNSSEC Deployment at the RIPE NCC, https://www.ripe.net/rs/reverse/dnssec/index.html

[19] NIST Special Publication 800-81, Secure Domain Name System (DNS) Deployment Guide, http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf

[20] NIST Special Publication 800-53, Revision 1, Recommended Security Controls for Federal Information Systems, public draft, March 2006, http://csrc.nist.gov/publications/drafts/800-53-rev1-ipd-clean.pdf

[21] Jim Reid, DNS-MODA, TLD Registry Considerations for Secure DNS (DNSSEC), presentation to APTLD (Asia Pacific Top Level Domain Association) meeting in Aman, Jordan, October 2005, http://www.aptld.org/meeting/2005/10_Amman/file/Jim-Reid-Secure-DNS.pdf

[22] Sixth Status Report Under ICANN/US Government Memorandum of Understanding, 31 March 2003, http://www.icann.org/general/status-report-31mar03.htm

[23] Twelfth Status Report under ICANN/US Government Memorandum of Understanding Quarter ending 30 September 2005, http://www.icann.org/general/mou-status-report-07oct05.pdf

[24] Thirteenth Status Report under ICANN/US Government Memorandum of Understanding Quarter ending 30 March 2006, http://www.icann.org/general/mou-status-report-07apr06.pdf

[25] Root Server Management Transition Completion Agreement, http://www.icann.org/topics/vrsn-settlement/revised-root-transition-agreement-clean-29jan06.pdf

[26] ICANN Annual Operating Objectives for Fiscal Year 2006-07, Draft dated 22 Jun 2006 http://www.icann.org/announcements/operating-plan-22jun06.htm

[27] U.S. Principles on the Internet's Domain Name and Addressing System, http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.pdf