From: "David A. Wheeler" <dwheeler@dwheeler.com>
To: <DNSSEC@ntia.doc.gov>
Date: Fri, Oct 10, 2008 2:14 PM
Subject: Enhancing DNS Security: Use multiple signatures for the DNS root, one per nation

Dear National Telecommunications and Information Administration (NTIA):

Thank you for requesting public comments about DNS security in the Federal Register (October 9, 2008 (Volume 73, Number 197), Page 59608-59612, docket Number: 0810021307-81308-01), "Enhancing the Security and Stability of the Internet's Domain Name and Addressing System", as posted at:
 http://edocket.access.gpo.gov/2008/E8-23974.htm
 http://www.ntia.doc.gov/DNS/DNSSEC.html
Many have noted your request, including:
 http://blog.wired.com/27bstroke6/2008/10/feds-take-step.html

I believe this request for public comment fails to address the fundamental problems for signing the DNS root, which IS desirable. Instead, I believe a process is needed where EVERY country signs the DNS root data, if they choose. Countries may work in blocs, if they choose, but that should be the choice of each country. Here is my explanation of why I believe this is needed.

=====================================

This request for public comment fails to address the true problem: There is NO single party that EVERYONE trusts worldwide. In particular, different countries - rightly or wrongly - are keenly unhappy with another country "controlling" their citizens' DNS root keys. Whether or not this is sensible is really not relevant; many nations clearly feel this way. Approaches such as "M of N" key-signing approaches (option 6 of appendix A) fail to address this fundamental issue.

I recommend that NTIA develop processes that have MANY MULTIPLE signatures, one for each country. DNS clients would decide which signatures they will accept (often using their user's nationality to select an acceptable key) and reject the rest. Some countries might decide to band together (e.g., EU members might have the EU sign for all of them), but that would be the decision of each nation. Should a change be proposed to the DNS root data, the process should provide the proposed revision to the organizations which hold the private keys for their authority, and then they can decide whether or not to sign the revision. In practice, I would expect them to eventually agree to sign most revisions... but having the ABILITY to reject signing something would give each country the confidence to sign the set. By _allowing_ countries to "opt out" at any time (including setting up their own root servers and DNS root signing), they will be far more willing to opt in... and may be delighted in doing so. Allow each country to decide who gets the job; thus, the current estrangement between Canada and ICANN would be irrelevant, since it would be

Canada (not ICANN) who makes the decisions for Canada.

There may need to be technical modifications or testing
to DNSSEC to make this practical at the DNS root (e.g., having clients
include a signature they would accept). In that case, it may be acceptable
to temporarily sign with 1 or 2 signatures, to help test and transition the
Internet to DNSSEC. But such temporary measures must be clearly
identified as temporary, with a workable plan and firm dates to transition
to multiple signatures (say, in a 4-year time period).

ICANN makes an inaccurate claim in:
"http://www.icann.org/en/announcements/dnssec-qaa-09oct08-en.htm".
I quote: "8) Why is it important for DNSSEC security that the vetting,
the editing and the signing by one organization?
For DNSSEC the strength of each link in the chain of trust is based on the
trust the user has in the organization vetting key and other DNS information
for that link. In order to guarantee the integrity of this information and
preserve this trust once the data has been authenticatediv it must be
immediately protected from errors, whether malicious or accidental, which can
be introduced any time key data is exchanged across organizational boundaries.
Having a single organization and system directly incorporate the authenticated
material into the signed zone maintains that trust through to publication. It
is simply more secure."
This is, at a fundamental level, false. The problem is that having
a single organization and system maintain something is only "more secure"
to some person X if person X _trusts_ that organization. There is no
organization on
that has the complete trust of all members of the human race; certainly ICANN
does not.
We routinely solve this problem in treaties by requiring that all
parties sign something before it's agreed to; those who choose to not sign
are not bound to the promises, nor do they (necessarily) receive the benefits.

Others have noted the value of having multiple signers, e.g.:
http://blog.internetgovernance.org/blog/_archives/2007/5/17/2957108.html
This proposal simply takes it to its logical conclusion: Since countries
do not extend 100% trust to each other, allow each one to make its
own decisions.

Having said that, let me attempt to answer your questions:

* In terms of addressing cache poisoning and similar attacks on
the DNS, are there alternatives to DNSSEC
that should be considered prior to or in conjunction with consideration
of signing the root?

Sure. Security is best implemented by having a range of
measures, especially since it will probably take many years
to get widespread DNSSEC implementation. Other countermeasures,
such as DNS port randomization, should still be implemented.
But they should be used in _conjunction_ with DNSSEC deployment.

* What are the advantages and/or disadvantages of DNSSEC
relative to other possible security measures that may be available?

DNSSEC provides real authentication of DNS data, and by extension, data related to systems. If we wish for a secure Internet, we need (in the long term) DNSSEC. DNSSEC's primary disadvantage is that it will take a long time to fully deploy, but that just means we need to start NOW.

* What factors impede widespread deployment of DNSSEC?

The biggest problem is the traditional chicken-and-egg problem; it must be widely deployed on clients and servers to do much good.

Historically, another problem has been DNSSEC's failure to provide confidentiality; older versions failed to provide protection against zone enumeration. This made many potential users unwilling to support it. But I believe NSEC3, while imperfect, is sufficient to resolve this problem.

* What additional steps are required to facilitate broader DNSSEC deployment and use? What end user education may be required to ensure that end users possess the ability to utilize and benefit from DNSSEC?

1. Ensure that the root and key top-level domains are signed (including ".com", ".org", ".edu", ".gov", and most countries').
2. Ensure that popular second-level domains are signed (including "google.com", "yahoo.com", "ebay.com", and so on).
3. Ensure that key client and server tools implement DNSSEC. In particular, make sure that there are open source software implementations of both, sufficiently so that developers can use them at no cost (increasing likelihood of use)
4. Ensure that key clients (such as Firefox) embed support of DNSSEC. It needs to require NO extra work, not even an extra plug-in... it must "work by default".

If end users require education, then that is a major defect to fix. We have conclusively demonstrated that most users do not really understand these issues. Nor should they need to. DNSSEC use should be automatic, requiring no end-user configuration or understanding in normal circumstances. Once people can get an acceptably signed key for a given DNS system, their system should never accept one that is not acceptably signed, and thus they need know little. Root keys should be built into major clients (e.g., browsers), with the selection based on "where they are from" on first sign-in.

(General Questions Concerning Signing of the Root Zone)

* Should DNSSEC be implemented at the root zone level? Why or why not? What is a viable time frame for implementation at the root zone level?

Yes, within 6 months. There is no reason the DNS root cannot be signed today. The problem is the insistence that there be a single signer; this is not technically necessary, nor (in the long term) politically acceptable.

*What are the risks and/or benefits of implementing DNSSEC at the root zone level?

The obvious. This would make it easy to authenticate DNS data, presuming that the sub-tiers implement DNSSEC as well. The latter is much more likely if the root zone is signed. DNS security is note as a specific need in the "U.S. National Strategy to Secure Cyberspace" (2003). Many plea for signing the DNS root; there's even a website specifically devoted to it (http://stfr.org/).

* Is additional testing necessary to assure that deployment of DNSSEC at the root will not adversely impact the security and stability of the DNS? If so, what type of operational testing should be required, and under what conditions and parameters should such testing occur? What entities (e.g., root server operators, registrars, registries, TLD operators, ISPs, end users) should be involved in such testing?

Sweden and others have demonstrated that DNSSEC, as now defined, can handle many DNS users.

Testing may be necessary to see the impact of a large number of signers. If DNSSEC implementations cannot handle a large number of signers well (as I suspect is true), then temporary implementations with few signers may be a useful intermediate step, with many signers once those problems have been addressed. It is quite likely that there will need to be small extensions or conventions to DNSSEC to handle this efficiently, but these should be relatively small. In any case, handling a "root DNS" key specially is hardly surprising from a security point of view.

* How would implementation of DNSSEC at the root zone impact DNSSEC deployment throughout the DNS hierarchy?

It would be greatly simplified.

* How would the different entities (e.g., root operators, registrars, registries, registrants, ISPs, software vendors, end users) be affected by deployment of DNSSEC at the root level? Are these different entities prepared for DNSSEC at the root zone level and /or are each considering deployment in their respective zones?

Again, greatly simplified.

* What are the estimated costs that various entities may incur to implement DNSSEC? In particular, what are the estimated costs for those entities that would be involved in deployment of DNSSEC at the root zone level?

They would be lower. Each country would determine how they would choose to sign (or not sign) a proposed change, but this would be at most a cost incurred once per nation, and probably not even that. For everyone else, they can simply start at the DNS root and work down, a simpler approach.

* The Department recognizes that the six process flow models discussed in the appendix may not represent all of the possibilities available. The Department invites comment on these process flow models as well as whether other process flow model(s) may exist that would implement deployment of DNSSEC at the root zone more efficiently or effectively.

I believe the proposal I have outlined, where each country signs separately (possibly in blocs) and each client decides which root signatures to accept, will be more acceptable long-term than any of the approaches outlined in appendix A.

Thank you for your time.

Speaking for myself,

--- David A. Wheeler

CC: <aheineman@ntia.doc.gov>