Fiona Alexander
Associate Administrator,
Office of International Affairs,
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W., Room 4701
Washington, D.C. 20230

To Whom It May Concern:

My comment on NTIA docket number 0810021307–81308–01 (Enhancing the Security and Stability of the Internet's Domain Name and Addressing System) follows. I would appreciate an acknowledgment of receipt.

Executive Summary: I advise against deployment of the DNSSEC protocol on Root DNS servers because

1. DNSSEC does not secure DNS services to any reasonable expectation of security,
2. Deployment of DNSSEC on Root servers enables new DNS Amplification Attacks which cannot be easily mitigated
3. Trust and confidence in DNSSEC is misplaced because critics have been silenced and many problems have not been addressed.

Specific Technical Failures

Reasonable Expectations of Security

One can't easily sign certain kinds of dynamically generated zones, such as those used by DNS Blacklists. Florian Wiemer has noted this fact on the IETF Discussion List[1]. There is an argument that such uses are outside the scope of DNSSEC—that is to say that DNSSEC anticipates that unsecured delegations may be required. One may also argue that DNSBL records don't comply with the DNS protocol anyway, but many expect that DNSSEC provides trustworthy DNS. Many of the comments received by the NTIA make that very assertion. But that is not the case. There are a variety of "holes" in DNSSEC, where security expectations aren't met. These "holes" and gaps in security are not easy for non-experts to foresee and avoid.

[1] http://www.ietf.org/mail-archive/web/ietf/current/msg53993.html

Contradiction in NSEC3 Specification (RFC5155)

Recently, (November 17th, 2008) it was reported on the DNSEXT Working Group List that there is a contradiction in the NSEC3 specification[2]. That contradiction represents a design failure, a design review failure, and a lack of implementation before standardization. There is far too much specification without adequate implementation, testing and review. DNSSEC has been under development since 1993, yet so much either doesn't work, or hasn't been critically reviewed. Critics have been silenced.

Replay Attacks

DNSSEC Resource Records Sets are signed so that the record set will be cryptographically valid for a recommended 30-day period. While the period can be set to any value, an attacker can copy and replay cryptographically valid records for the duration of the valid period even if the DNS administrator (that is, the root operator, IANA in this case) decides to alter the records. The old records can be just as damaging as any other spoofed record, resulting in a potential hijacking with the old DNS data by causing data to be sent to the wrong IP address or mail server, etc. One can also effect a Denial of Service attack using the old data if the old IP address is no longer in service. The precaution necessary to avoid replay attacks has been well understood for a long time, and implemented by protocols such as Kerberos, yet this knowledge, wisdom and experience was ignored.

Adaptive Chosen Plaintext Attack

DNSSEC depends on public key signatures for its security. In TLD zones such as .com which has an estimated 70,000,000 records, a large number messages and signatures can enable an adversary to deduce a pattern and then forge a signature of its choice. Cryptographic authorities recommend that a random nonce be added to the document to be signed to avoid certain cryptographic attacks using public key signatures[3] There is no point to signing the root if the TLD and lower zones can't be signed or if signing them might not be secure.

"DNSSEC Suicide"

As pointed out by Dr. Bernstein, the administrator has to update the database and the zone every month or the zone drops off the Internet. Dr. Bernstein names this "DNSSEC Suicide". The DNSSEC records will not be accepted by validating DNS resolvers if the administrator doesn't resign the zone at just the right time each month. Inaction by the administrator for only a short time can result in an unexpected outage. This is not a desirable feature of any critical service. It is also possible that DNS caches might not expire records at just the right time. Alternately, the surge in DNS requests at the expiration date might result in more failures as servers are overloaded. Consequently, the cryptographic expiration date also sets a date known in advance for a most effective time of attack on the Root DNS servers.

[2] http://ops.ietf.org/lists/namedroppers/namedroppers.2008/msg02194.html

[3] CRC Handbook of Applied Cryptography, Menezes (1997), Note 11.15, pg 433

Cache poisoning

DNSSEC caches are still vulnerable to cache poisoning. By setting the CD bit, the caching server will not validate the Resource Record Set (RRSET). If the server implements the BAD cache, (Section 4.7 of RFC4035) then from Section 3.2.2 of RFC4035:

```
   If the CD bit is set,
   the name server side SHOULD return the data from the BAD cache; if
   the CD bit is not set, the name server side MUST return RCODE 2
   (server failure).
```

The BAD cache, caches results that don’t validate. Of course, replay’ed record sets do validate, so this is only relevant to poisoning with record sets that don’t validate. The target stub resolver either uses the CD bit or it doesn’t. If it uses the CD bit, it gets the bad data, which it will discard (resulting in a Denial of Service) or it gets an RCODE 2, which also results in a Denial of Service. But if the record validates, because it is replayed, then it gets to wrong record in spite of its replacement by administrators. The effect in this case is either spoofing or Denial of Service.

Spoofing NSEC Untrusted Delegations

The NSEC (Next Secured) record is used to indicate that no signed records exist in an enumeration between two signed records. A flag in this record allows unsigned delegations to be made between two signed records. This allows one to delegate an unsigned zone from a signed zone. Suppose that bankofamerica.com has an NSEC record between specialoffer.bankofamerica.com and www.bankofamerica.com for the unsigned delegation test.bankofamerica.com. Later, it decides to create specialtwo.bankofamerica.com which is between the two signed records, and covered by the NSEC record created for test.bankofamerica.com. The attacker can replay the NSEC record and spoof the delegation to specialtwo.bankofamerica.com, enabling the theft of data from customers who want to get to the legitimate specialtwo.bankofamerica.com. Those customers, *placing misplaced trust in DNSSEC*, fail to check the TLS certificates or fail to use TLS to encrypt and validate the identity of the remote server.

Specific New Harms Created by DNSSEC

DNS Amplification Attack using Root, TLD, or Authority Servers
Because DNSSEC record sets are large, one may see 8KB records in response to DNSSEC queries. By spoofing the source address of the query, one can turn a 64byte query into a 8KB response. This is 126X amplification factor, making it by far the most largest and most effective amplification in the history of the Internet to date. Amplification attacks are used to flood internet links and take sites down by sheer volume of traffic. Mitigation of such attacks involves Access Control Lists (ACL) on the target customer that block the servers being used in the attack, and ACLs on the exploited servers blocking the target source address. Usually, the customer and the exploited servers have no close relationship, and a mutual block harms neither. However, this

strategy can't be used on Root DNS servers. If the customer blocks root DNS servers, their DNS will fail for the entire Internet. If the root servers block the customer, again, DNS for the entire internet will be denied to that customer. So in this case, the cure is just as bad as if not worse than the original attack.

The new DNS Amplification attack, at 126X, is enough to take down the DNS servers themselves, should their outbound connections be so saturated that legitimate requests are lost. The significance of this fact cannot be overstated.

Network Security Recommendation

Anyone interested in avoiding cache poisoning should use port randomization or TCP, or a combination of both. I have suggested that a common deployment scenario consists of a group of site-wide recursors serving stub resolvers. If the stub resolvers are handled with UDP port randomization, and the recursors are made to use TCP, then cache poisoning is limited to Man In the Middel(MITM) attacks. Only the site recursors need to be altered, and this alteration is completely within the current DNS specifications. The stub resolvers (which often do not cache responses) are speedily serviced by UDP as before. The recursors (which usually do cache responses) get a lot of benefit from the overhead of TCP.

The key point is that there is only two categories of attacks on DNS: One category of attack that can come from anywhere, and the other category of attack can only come from the middle. TCP eliminates the first category, so no further effort is needed to eliminate that category. TLS, properly verified, completely eliminates the second category, so no further effort is needed to eliminate that category. All done. No more changes to DNS are needed. It does mean that there will be more TCP access to DNS Root Servers, and that some further optimization of TCP on Root Servers may be necessary. Anycast of DNS Root Servers will probably need to be curtailed or eliminated.

Kaminsky-Vixie "Media Hack"

Much attention has been given to DNSSEC after the "Kaminsky Attack" was described. The December 2008 issue of MIT's *Technology Review* reports the "Media Hack" aspect of the event. The truth of the matter as, reported by *Technology Review* on pg. 64 is that "Kaminsky had not really discovered a new attack". Dr. Bernstein discovered this attack many years ago, and fixed the DNSCache server software in 1999. The PowerDNS caching server was fixed in 2006. In 2006, NLnet (Kolkman et al) noted the spoofing of NS Records. A design report for the Unbound DNS Server software, developed by Nominet, Verisign, NLnet Labs (Kolkman et al), EP.NET (Bill Manning))
in which the authors describe that "spoofed NS additionals confuse iterator"[4]. This paper was discussed at IETF 67, in November 2006.

[4] http://www.unbound.net/documentation/ietf67-design-02.pdf

Kaminsky is also connected to other questionable activity. In January 2006, Kaminsky announced he had found 580,000 open recursors at a hacker conference called Schmoocon. Its unclear how all this scanning was done without notice or complaint. Coincidentally, the first DNS reflection attack is reported to have taken place in October 2005 in a paper by Professor Vaughn of Baylor University and Gadi Evron[5] These events are the subject of a document called “draft-ietf-dnsop-reflectors-are-evil”, which seeks to close all open recursive DNS Servers.

After news of the “Kaminsky Attack” leaked out, Kaminsky wrote on Twitter:

> “DNS bug is public. You need to patch, or switch to OpenDNS, RIGHT NOW.”

OpenDNS is a company that offers Open Recursor service, using open recursors to provided DNS services that deny DNS to phishing sites, and enable the collection of data on user browsing preferences, which is presumably mined for marketing research and other statistics. There are connections between Vixie et al (the BIND Cartel) and OpenDNS founder David Ulevitch and OpenDNS employee Bill Fumerola.

Every part of Kaminsky’s “attack” was well-known to most DNS experts for a long time, including Paul Vixie. Vixie describes his conversation with Kaminsky very dramatically as ‘taking 20 seconds to explain the problem’. Vixie, having debated the issue with Bernstein, should have realized in that 20 seconds that the problem Kaminsky described was well-known. Instead, with great drama Vixie says:

> “Dan, I am speaking to you over an over an unsecure cell phone. Please do not ever say to anyone what you just said to me over an unsecure cell phone again”

But the well-known bug just doesn’t warrant that sort of drama.

Dan Kaminsky and Kevin Day subsequently asserted that there was a problem in DNSCache software. Their proposed fixes, discussed offlist with Dean Anderson, would have introduced a combination of two Birthday attacks into DNSCache, leaving it even MORE vulnerable to spoofing attacks.[6] Nothing more has been reported by either Kevin Day or Dan Kaminsky regarding bugs in DNSCache. No vulnerability was ever identified in DNSCache. The code patching BIND has not been analyzed for the presence of the combined Birthday attacks.

The *Technology Review* discusses how a great deal of “urgency” was artfully created. A reasonable review of the facts shows that the alarm is completely without justification. As a result of the “urgency”, many people deployed software changes that weren’t properly reviewed. This massive software update, performed on blind trust, is unprecedented in the history of the Internet. The urgency was unjustified, and one must

[5] http://www.isotf.org/news/DNS-Amplification-Attacks.pdf

[6] http://ops.ietf.org/lists/namedroppers/namedroppers.2008/msg02017.html

question whether deployment of DNSSEC as a knee-jerk reaction to a artfully created but unjustified perception could ever be wise. Instead, I think the connections between Kaminsky and the BIND Cartel DNSSEC promoters ought to be investigated to see if there was an effort to trick the government IANA function into adopting DNSSEC under artfully created, but false "urgency".

Trust in the DNS System, Confidence in DNSSEC

Comments by Olaf Kolkman, (Nlnet, IAB Chair, former DNSEXT WG Chair) note that "DNSSEC is the only standards-track mechanism to prevent corruption and replacement of the DNS data on its path through the Internet". While literally true that this is the only mechanism the IETF has considered, it is not the case that DNS is the ONLY mechanism proposed for secure DNS. Dr. Dan Bernstein, currently Research Professor, Department of Computer Science, University of Illinois, Chicago, has proposed a system called DNSCurve for the security of DNS data[7]. This proposal was made in the face of DNSSEC failures to secure DNS data. Dr. Bernstein is an implementer of the popular DNScache and TinyDNS domain name server software, yet has frequently been harassed, abused and censored by IETF decision-makers between 1998 and 2002[8]. Dr. Bernstein isn't the only one improperly abused. IAB Chair Kolkman states in his comments to the NTIA advocates a "multi-stakeholder process". However, his past acts have not demonstrated genuine respect for a truly open multi-stakeholder process.

Promoters of DNSSEC include Paul Vixie et al with ISC's BIND product, Dave Conrad et al with Nomimum's CNS, Olaf Kolkman et al with NLnet's NSD server, and Ed Lewis through employment at Neustar/UltraDNS and ARIN. Vixie and Conrad were founders of Nominum. NLnet was an underwriters of the ISC BIND9 product. These people, along with about 30 or so other persons involved in the control of ICANN, ARIN, ISOC/IETF and NANOG, are connected through common business ownership and control, or just "I got mine, he should get his". The business and financial connections often involve connections at more than one company. However, this group of people does not represent the entire industry, but just one very closely connected segment, I have labeled the "BIND Cartel" and Dr. Bernstein labeled the "BIND Company". DNSSEC was just one case where stakeholders and contributors were quite literally chased away from the DNSEXT Working Group that standardized DNSSEC in spite of fairly obvious problems. IAB Chair Kolkman participated in this misconduct by silent consent, when as IAB Chair and former DNSEXT Chair, he had an obligation to intervene to protect the rights of other stakeholders. Instead, Kolkman followed his parochial business interest in conflict of his duties as IAB Chair.

For example, a dispute raised by myself on the DNSEXT Working Group list was silenced in January 2008. This dispute cited conflicts of interest between Ed Lewis, David Conrad, and Paul Vixie regarding a draft known as AXFR-Clarify. This draft was submitted in 2001 as a "clarification" that would not alter the DNS wire protocol. Dr.

[7] http://cr.yp.to/talks/2008.08.22/slides.pdf
[8] http://cr.yp.to/djbdns/namedroppers.html

Bernstein discovered that the draft did alter the DNS wire protocol, and as a result, was abused and censored repeatedly. Changes were discovered in the BIND program that implemented the altered the protocol. As Dr. Bernstein writes quoting Sam Trenholme, implementer of MaraDNS DNS software:

> Trenholme blasted Gudmundsson on another mailing list:
>
> > The process for making DNS-related RFCs is open only in name. In reality, the people in the process of making DNS-releated RFCs are not listening to a number of important objections. For example, there was a recently proposed RFC which adds a bunch of arbitrary and, quite frankly, useless, rules to the AXFR (zone transfer) process.
> >
> > Dan, rightly so, brought up a number of objections with this internet draft.
> >
> > These objections were completely ignored.

In early 2003, there was additional controversy about fraudulent consensus on the document[9]. The AXFR-clarify draft then languished for 5 years, until January 2008, when Ed Lewis of Neustar/UltraDNS again took up the cause. In January 2008, Anderson objected to assigning the draft to Lewis because he is connected to the earlier abuse of Bernstein and to the deception of the Working Group. Anderson did this by detailing the connection between Lewis and those known to be associated with the BIND Cartel and the prior abuse. While this is a relevant objection concerning facts that affect the integrity of the IETF process, Anderson was silenced on the false claim:

> It has come to my attention that Dean Anderson <dean at av8 dot com> has posted some messages to this mailing list that are not technical butpersonal attacks and conspiracy theories.

There were no personal attacks: the information about past wrongdoing (deception of the working group) was relevant to the business of the working group.

Trust and Confidence in the ISOC; the IAB and IETF

The ISOC by its corporate charter and bylaws defines itself to be a non-profit membership organization. The ISOC in statements to the public and to the Internal Revenue Service claims to be a membership organization with objectives consistent with public policy objectives for non-profit organizations. The ISOC IETF Activity, controlled and constrained by the ISOC bylaws, charter, and the laws of the United States, describes itself in documents such as its web pages and “The TAO of the IETF”. In those documents it describes itself as a member organization having no membership standards. Well, having no membership standards and keeping no membership rolls does not mean that it isn’t subject to its bylaws and the law regarding the rights of members. Indeed, the question of member rights and the expulsion or suspension of members in such cases is long resolved in law regarding Associations and Clubs as well as Corporations. Yet the IESG has stated that it can silence many stakeholders in Internet technology and Policy. Among the stakeholders it has silenced or censored:

[9] http://ops.ietf.org/lists/namedroppers/namedroppers.2003/msg00269.html

- Dean Anderson, CEO of AV8 Internet, Inc, President of the League for Programming Freedom
- Dr. Dan Bernstein, University of Illinois, Chicago
- Todd Glassey, Chief Scientist and CTO at Certichron Corporation
- JFC Morfin, Executive Director, INTLNET

In several cases, fabrications of wrongdoing have been made to justify censorship. In at least one case, fabrication of "consensus" was reported[10] by the IESG and IAB. For example, Mr. Anderson was suspended for merely opposing Root DNS Anycast and exposing false claims that TCP Anycast of DNS would be stable. Mr. Anderson also objected to failures to comply with requirements of patent disclosures required by RFC 3979. The IPR Working Group Chair, Steven Bellovin falsely stated that RFC3979 was not the policy of the IETF. IETF Activity Attorney Jorge Contreras repudiated Bellovin's statement in January 2007, implicitly vindicating Anderson's claims that it was false. If one single example is to stand in dispute of the ISOC IETF reputation for honesty and integrity, the following page must be read: http://www.av8.net/IETF-watch/IESG/IESG-PR-discussion.html That page details the fabricated reports of consensus by the IESG and IAB to silence Dean Anderson.

As a result of these and other examples of activities too numerous to detail here which are at least contrary to public policy and contrary the stated objectives of the ISOC, it is impossible to place confidence in the assurances of the ISOC IETF Activity on the suitability of DNSSEC, and particularly in those persons described as the BIND Cartel who have involvement in conflicts of interest, false claims and censorship in order to promote their parochial business interests as decision makers for the ISOC IETF Activity. It should be noted that the improper activities are not limited to the ISOC IETF Activity; the same BIND Cartel group has, for example, infiltrated ARIN, ICANN, and NANOG. For example, Paul Vixie and Bill Manning were "elected" to the Board of Trustees of ARIN in 2007. However, that election did not have a quorum necessary to elect Board Members, according to the voting tally and the membership rolls reported at ARIN's own web site. Bill Manning refused to accept certified mail notifying him of this fact. ARIN CEO Ray Plzak recently resigned suddenly from ARIN, one day after complaints were made public that Plzak was involved in fabricated statements on which ARIN based decisions to suspend and interfere with the membership rights of Dean Anderson and AV8 Internet to contact other ARIN members. AV8's lawyer had previously written a letter to ARIN informing it of the fabrication. Plzak also had an obligation as CEO and as Board Member to ensure that other elected Directors were properly elected, and that un-elected Board Members did not act as Board Members. This is but a short sample of improper activity by the BIND Cartel.

At a recent talk at Harvard University, Al Gore, quoting Theodore Adorno said

[10] http://www.av8.net/IETF-watch/IESG/IESG-PR-discussion.html

> “science is often met with opposition from leaders who want to turn “questions of fact” into “questions of power,”.
>
> “Questions of fact should be questions to be explored,” he said. “They should not be waylaid on their way to the public forum.”

A significant part of the disputes involves questions of fact, and instead of exploring the questions of fact, they attempted to silence the people who raised the questions, often by subverting the public policy and charter of the organizations to investigate questions of fact, and subverting, by fabrication and false statement, the rules of the organization. The ISOC and consequently the ISOC IETF Activity, is chartered to be a scientific organization. As such, its principle interest is in exploring questions of fact. Instead, questions of fact have become questions of power, and have been improperly waylaid on their way to the public forum. This alone is reason to doubt whether one should place great trust and confidence in the ISOC IETF Activity.

Of course, it must be recognized that these problems are the result of acts by identifiable persons in decision-making positions, rather than some obscurely intangible corporation. A corporation by itself has no intent: good, bad, or indifferent. It is the people who make decisions for the corporation that exercise bad decision-making, that exercise conflict of interest, that exercise dishonesty. Recovery from these problems requires a focus on the people involved in the decision-making. This quote comes to mind:

> This group of gangsters, aided and abetted by their relatives and sycophants, engaged in a multifaceted orgy of criminal activity. For those that enthusiastically followed these arrogant mobsters in their morally debased activity there were material rewards. For those who accepted the side benefits of this perverted interpretation of business unionism, see J. Hutchinson, The Imperfect Union p. 371, (1970), there was presumably the rationalization of "I've got mine, why shouldn't he get his." For those who attempted to fight, the message was clear. Murder and other forms of intimidation would be utilized to insure silence. To get along, one had to go along, or else. —U.S. v. Local 560? 581 F.Supp. 279

Similarly, there has been a perverted interpretation of “open standards”. DNSSEC is just one object of that perverted interpretation. But for those who attempted to fight, the message was just as clear and the result was the same: Intimidation would be used to insure silence, and to get along, one must go along, **or else**.

As a result of these and other activities that perverted the open process of standardization, the serious technical flaws described above, and the very serious new D.D.O.S. attacks made possible by DNSSEC, I oppose the deployment of DNSSEC on the root DNS servers and the TLD servers, and I ask the NTIA to look into the matter of open process failures and conflicts of interest contrary to public policy objectives by the BIND Cartel at the ISOC, ARIN, ICANN, and NANOG.

Sincerely,

Dean Anderson
CEO
AV8 Internet, Inc