DNSSEC BoF

Internet2 Member Meeting

October 15th, 2008

Noon, Napoleon A2

http://www.uoregon.edu/~joe/dnssec-bof-fall-2008/

Agenda

- **I. Introductions and**
  Signing Up For the DNSS List
- **II. DNSSEC-Related Sessions Here at the Member Meeting**
  (1) This BOF
  (2) DNSSEC at LSU, Allie Hopkins, Today, 3PM, Maurepas
- **III. Just in Case Folks Haven't Heard…**
  One More Time: The Kaminsky Vulnerability
- **IV. Some Brief Updates**
  (1) Signing the Root
  (2) ICANN Security and Stability Advisory Committee
  (3) Dot Gov and DNSSEC
  (4) Nominet/Corecom Test of Broadband Routers and Firewalls
  (5) ccTLDs and other TLDs

I. Introductions

Welcome!

- Please tell us a little about yourself (e.g., your name and institution)

- We'd also love to hear anything else you'd like to share, such as:

  -- what's spurring your interest in DNSSEC
  -- the status of DNSSEC testing or deployment at your site
  -- DNSSEC-related issues you'd like help resolving
  -- or?

Signing Up For the Internet2 DNSSEC List…

We don't want to spam you, but if you're interested, please feel free to join the Internet2 DNSSEC mailing list:

https://mail.internet2.edu/wws/subrequest/dnssec

See also the Shinkuro DNSSEC Deployment Working Group and mailing list at http://www.dnssec-deployment.org/wg/

II. DNSSEC Sessions Here at The Member Meeting

DNSSEC at Louisiana State University

- **Abstract:**
  DNSSEC has become an increasingly popular topic over the last few years amongst DNS administrators worldwide. The recent DNS cache poisoning exploit caused this interest to skyrocket. The importance of DNSSEC is much more apparent now than it has ever been before. We, at LSU, were already on the way to exploring this topic and plan to have it implemented before the close of the New Year. An even better goal is to have something implemented before October. I plan to discuss why DNSSEC is so important to the internet community, how we tackled this seemingly daunting task, and the obstacles/successes encountered along the way.

  Session will be today at 3PM, Maurepas

III. Just In Case Folks Haven't Heard…

Test, and If Necessary, Patch Your Resolvers!

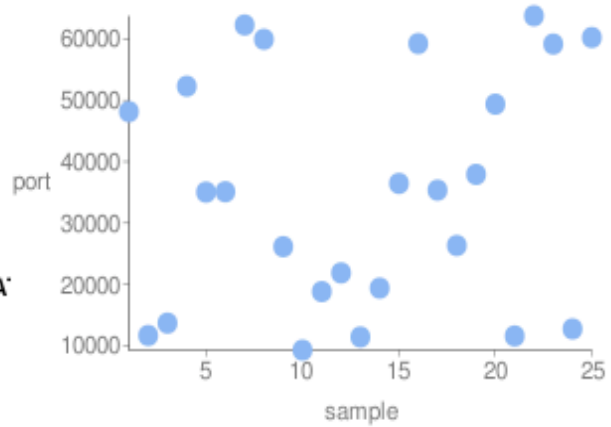
- **Problem:** Dan Kaminsky discovered a very efficient way to do DNS cache poisoning; DNSSEC would fix the issue, but until then you watch to be sure to patch your resolvers. For more information, see http://www.kb.cert.org/vuls/id/800113
- **To Test:** https://www.dns-oarc.net/oarc/services/dnsentropy (an example of what you'd like to see can be found on the following slide)
- **If Necessary, Patch:** If your resolvers don't pass, patch 'em!
- **Providers ARE Getting Hit:** For example, see "China Netcom DNS cache poisoning" (08/19/2008): http://securitylabs.websense.com/content/Alerts/3163.aspx
- **While patching is critical, and certainly better than nothing, DNSSEC is needed to definitively address this issue.**

1. 76.165.144.11 (wlan-reg-1-no.internet2.edu) appears to have GREAT source port randomness and GREAT transaction ID randomness.

Test time: 2008-10-15 14:22:34 UTC

Note that standard deviation is usually, but not always, a good indicator of randomness. Your brain is a better detector of randomness, so be su
to take a look at the scatter plots below. If you see patterns (such as straight lines), the values are probably less random than reported.

76.165.144.11 Source Port Randomness: GREAT



Number of samples: 25
Unique ports: 25
Range: 9276 - 63781
Modified Standard Deviation: 19133
Bits of Randomness: 16
Values Seen: 48150 11660 13672 52293 35029 35094 62275 59943 26140 9276
18816 21864 11416 19383 36453 59251 35356 26327 37919 49370
11579 63781 59166 12735 60236

IV. Updates

Update 1: Signing The Root

NTIA Notice of Inquiry: "Enhancing the Security and Stability of the Internet's Domain Name and Addressing System," October 9th

- http://edocket.access.gpo.gov/2008/E8-23974.htm

  SUMMARY: The Department of Commerce (Department) notes the increase in interest among government, technology experts and industry representatives regarding the deployment of Domain Name and Addressing System Security Extensions (DNSSEC) at the root zone level. The Department remains committed to preserving the security and stability of the DNS and is exploring the implementation of DNSSEC in the DNS hierarchy, including at the authoritative root zone level. *Accordingly, the Department is issuing this notice to invite comments regarding DNSSEC implementation at the root zone*.

  DATES: Comments are due on November 24, 2008

- **The NTIA's questions are…**

Questions on DNSSEC Deployment Generally

- 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?
- What are the advantages and/or disadvantages of DNSSEC relative to other possible security measures that may be available?
- What factors impede widespread deployment of DNSSEC?
- 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?

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

General Questions Concerning Signing of the Root Zone (continued)

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

Operational Questions Concerning Signing of the Root Zone

- 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.
- Of the six process flow models or others not presented, which provides the greatest benefits with the fewest risks for signing the root and why? Specifically, how should key management (public and private key sets) be distributed and why? What other factors related to key management (e.g., key roll over, security, key signing) need to be considered and how best should they be approached?

Operational Questions Concerning Signing of the Root Zone (continued)

- We invite comment with respect to what technical capabilities and facilities or other attributes are necessary to be a Root Key Operator.
- What specific security considerations for key handling need to be taken into account? What are the best practices, if any, for secure key handling?
- Should a multi-signature technique, as represented in the M of N approach discussed in the appendix, be utilized in implementation of DNSSEC at the root zone level? Why or why not? If so, would additional testing of the technique be required in advance of implementation?

Appendix A: The Six Models

- The first three of the process flows described below assign the responsibilities of Root Zone Signer, Root Key Operator, and key publishing among the existing parties to the root zone file management process or to a new, as yet unspecified, third party without materially changing the other pre- existing roles and responsibilities. The fourth model represents a variation of previous models, while changing the current root zone management process flow. The fifth model is also a variation of previous models, while maintaining the current root zone management process flow. The sixth model describes a process flow in which more than one third party, as yet unspecified, are introduced as Root Key Operators, which can be applied to all the previous process flows. [continues]
- See http://www.ntia.doc.gov/DNS/dnssec.html

Update 2: ICANN Security and Stability Advisory Committee Memorandum

SSAC
ICANN Security and Stability Advisory Committee

28 January 2008

SAC 026: SSAC Statement to ICANN and Community on Deployment of DNSSEC

SSAC notes the DNSSEC deployment efforts of ICANN and the community at large and encourages continued efforts to improve the security of the domain name system. We recognize that any technology deployment on a global scale is apt to reveal issues not considered in protocol design and development and in controlled (test) environments. SSAC notes that several such issues have been exposed with respect to DNSSEC[1] and recommends the following actions.

1. As manager of the IANA function, ICANN should continue its efforts to support and

http://www.icann.org/en/committees/security/sac026.pdf

Update 3: Dot Gov and DNSSEC

OMB: dot gov <u>will</u> be signed by January 2009

New Policy

This memorandum addresses two important issues in following through with the existing policy and expanding its scope to address all USG information systems.

A. The Federal Government will deploy DNSSEC to the top level .gov domain by January 2009. The top level .gov domain includes the registrar, registry, and DNS server operations. This policy requires that the top level .gov domain will be DNSSEC signed and processes to enable secure delegated sub-domains will be developed. Signing the top level .gov domain is a critical procedure necessary for broad deployment of DNSSEC, increases the utility of DNSSEC, and simplifies lower level deployment by agencies.

B. Your agency must now develop a plan of action and milestones for the deployment of DNSSEC to all applicable information systems. Appropriate DNSSEC capabilities must

http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf
August 22nd, 2008

Update 4: Nominet/Corecom Test of Broadband Routers and Firewalls

http://download.nominet.org.uk/dnssec-cpe/DNSSEC-CPE-Report.pdf

- All 24 units could **route** DNSSEC queries addressed to upstream resolvers (referred to herein as route mode) without size limitations.

- 22 units could **proxy** DNS queries addressed directly to them (referred to herein as proxy mode), with varying degrees of success.

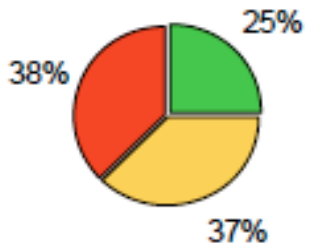
- 6 of 22 DNS proxies had difficulty with DNSSEC-related flags and/or validated responses that effectively prevented DNSSEC use in proxy mode.

- 16 of 22 DNS proxies could successfully pass DNSSEC queries and return validated responses of some size.

- 18 DNS proxies limited responses over UDP to either 512 bytes or a size constrained by the MTU. Only 4 could return responses over UDP up to 4096 bytes, while just 1 could proxy DNS over TCP (no size limit). Such limits can interfere with returning longer DNSSEC responses.

- When deployed with factory defaults, 15 units are likely to be used as DNS proxies, while 3 always route DNS queries. The rest (6) vary over time, preferring to route DNS after being connected to a WAN.

As a consequence, we conclude that just 6 units (25%) operate with full DNSSEC compatibility "out of the box." 9 units (37%) can be reconfigured to bypass DNS proxy incompatibilities. Unfortunately, the rest (38%) lack reconfigurable DHCP DNS parameters, making it harder for LAN clients to bypass their interference with DNSSEC use.



Update 5: ccTLDs (and other TLDs)

Signed ccTLDs (and Other TLDs)

- bg
- br
- cz
- museum
- pr
- se

- Sure love to see dot edu join that list :-)
  Dot org may beat us to it, however.

Dot Org


http://www.pir.org/index.php?db=content/News&tbl=Press&id=9
.ORG Advantage
Registrars
Registrants
News
News
.ORG Becomes First Generic Top Level Domain to Start DNSSEC Implementation (2008-07-21)
< Previous | Next >
Calls on ICANN for Speedy Adoption to Sign the Root
Reston, VA - July 21, 2008 - A request by .ORG, The Public Interest Registry to bolster Internet security via the implementation of Domain Name Security Extensions (DNSSEC) was unanimously approved by the board of Internet Corporation for Assigned Names and Numbers (ICANN) at the recent Paris meeting. As the first generic Top Level Domain authorized to implement DNSSEC, .ORG also is preparing an education and adoption plan within the Internet infrastructure community.

http://ws.edu.isoc.org/workshops/2008/cctld-ams/

Advanced ccTLD & DNSSEC Workshop

The ISOC-sponsored Advanced ccTLD workshop series is aimed at ccTLD operators who have either already attended the initial ccTLD Workshop series, or for ccTLD operators who are at an operational level where they would benefit from the topics presented in this workshop.

Local Host

RIPE NCC

Instructors

Jaap Akkerhuis	(NLnet Labs)	Daniel Karrenberg	(RIPE NCC)
Hervey Allen	(NSRC)	Olaf Kolkman	(NLnet Labs)
John Crain	(ICANN)	Duane Wessels	(DNS-OARC)

Organizers

Mirjam Kühne	(ISOC)	Martin Kupres	(ISOC)
Steve Huter	(NSRC)		

Agenda

Advanced ccTLD Workshop Attendee List

Attendees:

Adriatik Allamani	AL (Albania)
Barjon Rama	AL (Albania)
Luis León Cárdenas Graide	CL (Chile)
Cristián Rojas	CL (Chile)
Elena Grimany	CU (Cuba)
Ayitey Bulley	GH (Ghana)
Godfred Ofori-Som	GH (Ghana)
Nicholas Wambugu	KE (Kenya)
Dr. Paulos B. Nyirenda	MW (Malawi)
Eswari Prasad Sharma	NP (Nepal)
Rakeshman Karmacharya	NP (Nepal)
Cesar Rodas	PY (Paraguay)
Daniel Brassel	PY (Paraguay)
Medard BASSENE	SN (Sénégal)
Khalil Rakhmanov	TJ (Tajikistan)
Wafa Dahmani	TN (Tunisia)
Atef LOUKIL	TN (Tunisia)

Advanced ccTLD Workshop Instructor List

Instructors:	
Jaap Akkerhuis	NLnet Labs
Hervey Allen	Network Startup Resource Center (NSRC)
John Crain	Internet Corporation for Assigned Names and Numbers (ICANN)
Daniel Karrenberg	RIPE NCC
Olaf Kolkman	NLnet Labs
Duane Wessels	DNS-OARC / The Measurement Factory
Coordinators	
Steve Huter	Network Startup Resource Center (NSRC)
Mirjam Kühne	Internet Society (ISOC)
Martin Kupres	Internet Society (ISOC)
Observers	
Chris Evans	Delta Risk
John Schnizlein	Internet Society (ISOC)
Technical Help	
Emil Gorter	RIPE NCC