CONTRACTOR'S QUARTERLY PROGRESS, STATUS AND MANAGEMENT REPORT

Initial Report

DOMAIN NAME SYSTEM SECURITY (DNSSEC) DEPLOYMENT COORDINATION

Contract No: FA 8750-10-C-0020

Data Item A001, CLIN 0002

Submitted by:

Shinkuro, Inc.
Bethesda, MD

Stephen D. Crocker
Principal Investigator

Jeffrey Dewhurst
Financial and Contract Administration

January 2010

Progress Against Planned Objectives (3.1.1)

- Progress was made on Path MTU an Middlebox issues, and reported on the DNSSEC blog
- Progress was made on determining useful validation policies.
- A key rollover testbed is up and running and is collecting data
- Website and newsletter were transitioned to a blog and the C&A process was brought into its final phase.

Technical Accomplishments This Period (3.1.2)

Published “DNSSEC Operations: Setting the Parameters” as a guide to registrars and others providing DNSSEC compliant name service to large numbers of small zone owners. A copy is attached and it is available online at http://wordpress.test.dnssec-deployment.org/wp-content/uploads/2009/09/Setting-the-Parameters-2009112403.pdf

Improvements to Prototypes This Period (3.1.3)

None at this time.

Deliverables This Period (3.1.5)

DNSSEC website was transitioned to a blog on January 5th. Instead of monthly updates, and a newsletter, the website has new information posted every few days and is a more interactive format allowing comments and posting on the DNSSEC wiki.
There were no deliverables scheduled for this initial period.

Publications This Period (3.1.7)

The final editions of DNSSEC This Month (attached) were published on December 1st 2009, and January 4th 2010.

Meetings and Presentations This Period (3.1.8)

Shinkuro organized and led a meeting between the DNSSEC Deployment Coordination team, including Sparta, NIST, Shinkuro, and DHS and members of the development team from Microsoft to work on planning the inclusion of DNSSEC in future Microsoft products. The emphasis was placed on future versions of Microsoft server software, and making sure that Microsoft products that are sold to the government will comply with the OMB mandate that government systems employ DNSSEC.

Issues or Concerns (3.1.9)

None at this time.

Planned Activities (3.2.1), Information Covering the Next Three Months

- The deployment initiative will be sponsoring an all day session and a group of exhibitors at the 2010 FOSE Expo and Conference, March 23 – 25. This will include a series of presentations by government representatives, deployment experts, and vendors.
- A coordination meeting is scheduled for January 26th, and will continue on a monthly basis after that.
- The next ICANN meeting will take place in Nairobi, and a DNSSEC workshop is scheduled.

Attachments (3)

DNSSEC This Month December 2009
DNSSEC This Month January 2010 (final)
DNSSEC Operations: Setting The Parameters

Welcome to the December 2009 edition of DNSSEC THIS MONTH, a monthly newsletter about advances in securing the Internet's naming infrastructure in the government, business and education sectors. The DNS Security Extensions (DNSSEC) Deployment Coordination Initiative, which produces this newsletter, is part of a global effort to deploy new security measures that will help the DNS perform as people expect it to -- in a trustworthy manner. This newsletter will offer updates on new policies, early adopters and advances in DNS security extension development. For more information on progress toward DNSSEC deployment, read the initiative roadmap at http://www.dnssec-deployment.org/technology/roadmap.htm.

The U.S. Department of Homeland Security Science and Technology Directorate provides support for coordination of the Initiative.

Deployment watch: Penn, dot-TM, VeriSign and Dyn: Help this newsletter stay up-to-date on your organization's deployment news by submitting information about your DNSSEC deployment deadlines, test beds or other progress to tldwatch@shinkuro.com. This month's updates include:

- **University of Pennsylvania first U.S. university to deploy**: The University of Pennsylvania announced it is the first U.S. university to implement DNSSEC across the entire institution. Shumon Huque, a Penn IT technical director, also is working with EDUCAUSE to secure the dot-EDU top-level domain "Higher education can take a leadership role in securing the DNS," Huque said. "If a few universities in advanced networking adopt DNSSEC and share experiences, we can make broad deployment more straightforward for the larger community." Read the announcement at http://www.upenn.edu/almanac/volumes/v56/n11/dns.html.

- **Turkmenistan announces DNSSEC deployment:** Turkmenistan's dot-TM domain registry has launched DNSSEC. While not a trademark registry, it encourages trademark owners to register dot-TM names. Read the announcement at http://www.reuters.com/article/pressRelease/idUS175619+29-Oct-2009+BW20091029 and more about dot-TM at http://www.zdnet.com.au/news/business/soa/-TM-domain-back-on-the-market/0,139023166,120272805,00.htm?omnRef=http://www.nic.tm/pressquotes.html.

- **VeriSign launches boot camp, tools and training to aid DNSSEC deployment**: VeriSign has created a technical "boot camp" program to train registrars, ISPs and larger registrants in DNSSEC assessment and implementation. The effort also includes an interoperability lab that will allow vendors to evaluate how their equipment works with DNSSEC. Network and computing equipment manufacturers also are being invited to VeriSign to review how DNSSEC will work with their equipment when DNSSEC is implemented in the .com and .net TLDs. VeriSign has announced it will deploy DNSSEC in the dot-COM and dot-NET domains by early 2011 and is working with EDUCAUSE on DNSSEC deployment in the dot-EDU domain. Read more at http://money.cnn.com/news/newsfeeds/articles/marketwire/0558203.htm and at the VeriSign DNSSEC resource center at http://www.verisign.com/domain-name-services/domain-information-center/dnssec-resource-center/index.html.

- **Dyn, Inc. reports on testing with dot-ORG**: Dyn, Inc. published resources and updates about its tested and other preparations for deploying DNSSEC for dot-ORG zones registered with the company. Read its updates at http://dyn.com/DynIncLeadsTheChargeForDNSSEC.

Dot-ORG documents "the DNSSEC groundswell:" A blog post from dot-ORG, the Public Interest Registry, details the "groundswell" of progress toward DNSSEC deployment, from major steps such as the U.S. federal government mandate for agencies to deploy DNSSEC to PayPal's support for the security extensions. Read the summary at http://blog.pir.org/?p=185.

Infoblox study shows tripling of DNSSEC adoption: *Government Computer News* notes that a recent Infoblox and Measurement Factory study of domain name servers on the Internet found a tripling of zones signed with DNSSEC, based on a sample of 5 percent of the Internet's IPv4 address space. From the article: "The scan showed that the number of zones signed using DNSSEC—the DNS Security

Extensions—jumped from 45 to 167 in the past year. 'The [DNSSEC] numbers in an absolute sense are small,' [Infoblox Vice President for Architecture Cricket] Liu said. 'But people do seem to be interested in it. It's catching on'." Read the full article at http://gcn.com/Articles/2009/11/10/DNS-survey-DNSSEC.aspx?Page=1.

ICANN releases DNSSEC policy and practices: A working draft of ICANN's DNSSEC Policy and Practice Statement for the root-zone key-signing key operator was issued in November, codifying practices for management and issuing of DNS keys in keeping with U.S. Department of Commerce requirements. Read the draft at http://www.ntia.doc.gov/DNS/ICANN_dnssecDraft_091112.txt.

Workshops to update your DNSSEC knowledge: Here are forthcoming conferences, workshops and sessions focused on helping you deploy and understand DNSSEC and related issues:

- **DNSSEC deployment to be featured at FOSE 2010:** A special presentation, "What's Next in DNSSEC: Securing the Domain Name System" will be presented at FOSE, the conference and exhibition for the U.S. government IT community, on **Wednesday, March 24, 2010 from 10:30 a.m. to 4:30 p.m.** Registration for the session will begin in November 2009 and is open to all FOSE and GovSec/U.S. Law attendees; pre-registration is required for the session, which is free. The day-long session will assess the U.S. federal response to securing its domains; examine challenges faced by agencies deploying DNSSEC; and share lessons learned and next steps as DNSSEC is deployed in other sectors. Software and hardware naming solutions also will be presented to update participants on available options for automating or easing deployment challenges. The session is organized by the DNSSEC Deployment Coordination Initiative and supported by the U.S. Department of Homeland Security. To exhibit in the DNSSEC Pavilion at FOSE, contact Don Berey, Show Director at 703-876-5073 or send him an email at dberey[at]1105govinfo[dot]com. For more information on the session or to register, go to http://fose.com/events/fose-2010/tracks/whats-next-in-dnssec.aspx.

- **ICANN to Nairobi:** ICANN's 37th meeting will be held in Nairobi, Kenya, March 7-12, 2010. For details, go to http://nbo.icann.org/.

- **IETF to California**: IETF will convene its 77th meeting in Anaheim, Calif., March 21-26. For more on upcoming IETF meetings, go to http://www.ietf.org/meeting/upcoming.html.

Welcome to the January 2010 edition of DNSSEC THIS MONTH, a monthly newsletter about advances in securing the Internet's naming infrastructure in the government, business and education sectors. The DNS Security Extensions (DNSSEC) Deployment Coordination Initiative, which produces this newsletter, is part of a global effort to deploy new security measures that will help the DNS perform as people expect it to -- in a trustworthy manner. This newsletter will offer updates on new policies, early adopters and advances in DNS security extension development. For more information on progress toward DNSSEC deployment, read the initiative roadmap at http://www.dnssec-deployment.org/technology/roadmap.htm.

The U.S. Department of Homeland Security Science and Technology Directorate provides support for coordination of the Initiative.

Newsletter turns into new DNSSEC blog: DNSSEC THIS MONTH newsletter will re-launch as a blog beginning January 5, 2010, DNSSEC TODAY will continue to cover the progress of DNSSEC deployment, forthcoming meetings and workshops, and other resources to help you monitor news about DNSSEC deployment. The blog is part of a website redesign for the DNSSEC Deployment Coordination Initiative, and can be seen at http://www.dnssec-deployment.org. The Initiative's website redesign will include a variety of tools and resources about DNSSEC technology, policy and operations. Changes also will be occurring to the DNSSEC Deployment mailing list as part of the website revisions and will be announced on the list and on the blog.

Deployment watch: Netherlands, European Union, dot-US, root zone: Help this newsletter stay up-to-date on your organization's deployment news by submitting information about your DNSSEC deployment deadlines, test beds or other progress to tldwatch@shinkuro.com. This month's updates include:

- **SIDN to sign dot-NL in August**: SIDN, the registry for The Netherlands' dot-NL and ENUM, announced it will implement DNSSEC one month after the root zone is signed in July, setting its implementation for August 2010. SIDN CEO Roelof Meijer said, "Waiting until the root is signed means that we won't need to implement any interim solutions – which inevitably increase the risk of errors – and it will be possible to sign the whole chain at once. We believe that this is the best and safest way to implement DNSSEC for the dot-NL zone." Read the full announcement in English at http://www.sidn.nl/ace.php/c,728,6208,,,,SIDN_prepares_to_introduce_DNSSEC_for_nl_zone.html
- **European Union endorses DNSSEC and action plan:** The European Union's economic and social committee has adopted resolutions in support of priority implementation of IPv6 and DNSSEC technology throughout the EU Internet, as well as an action plan specifying DNSSEC implementation. Read the announcement at [HOLDING FOR URL HERE]
- **DNSSEC implemented in dot-US:** Neustar announced it has implemented DNSSEC in the dot-US country-code top level domain. Rodney Joffe, senior vice president and senior technologist at Neustar, said, "DNSSEC means a more secure and reliable domain name system because its extensions provide origin authentication of DNS data, data integrity and authenticated denial of existence." Read the announcement at http://www.prnewswire.com/news-releases/neustar-implements-dns-security-extensions-in-the-us-registry-79308817.html.
- **Root zone deployment schedule issued:** The root zone DNSSEC deployment team has launched a web site with updates on the effort, at http://www.root-dnssec.org.
  It includes documentation and technical status updates on DNSSEC deployment at the root, and will offer announcements as the project moves forward. You can subscribe to future status updates via RSS at http://www.root-dnssec.org/rss. For more information, contact the root deployment team at rootsign@icann.org.

Initiative shares advice on signing zones: The DNSSEC Deployment Coordination Initiative has published advice for registrars and other DNS operators with "a reasonable set of DNSSEC configuration parameters." Titled "DNSSEC Operations: Setting the Parameters," the suggests values to choose for the configuration parameters associated with DNSSEC that provide good security without causing an undue burden on operators' name service infrastructures. The configuration parameters include key sizes and lifetimes, re-signing periods, and time-to-live for the records. Feedback on the memo is welcomed at dnssec-parameters@shinkuro.com. Read the memo at [NEED A URL FOR THE MEMO – Jeffrey, can you insert it here?].

RIPE issues new app to gauge DNSSEC readiness: RIPE NCC has release an application to help network administrators determine the maximum size of DNS responses that a resolver can receive so they can prepare their networks and resolvers for a signed root zone. Download the app and see instructions athttp://labs.ripe.net/content/testing-your-resolver-dns-reply-size-issues.

Report on DNSSEC administrative tools released: dot-SE (The Internet Infrastructure Foundation) has released a report it commissioned from independent IT security firm Certezza focused on the functionality of signing and key management tools. The report notes, "the product standard is good and the tested products work as expected." Read the report at http://www.iis.se/docs/DNSSEC-Admin-tools-review-1.01.pdf

Google launches Public DNS: Google launched a free, global Domain Name System (DNS) resolution service, offering it as "an alternative to your current DNS provider." The new service supports EDNS0 extensions, accepting and forwarding DNSSEC-formatted messages, but does "not yet" validate responses. Read the Public DNS FAQ at http://code.google.com/speed/public-dns/faq.html#whatis.

California CISOs hear about DNSSEC: Initiative sponsor Douglas Maughan, Ph.D., of the U.S. Department of Homeland Security, spoke on DNSSEC deployment at the California Chief Information Security Officer lecture series on December 15 in Sacramento, to an audience of the state's **information security officers, disaster recovery coordinators, and chief information officers.**

Workshops to update your DNSSEC knowledge: Here are forthcoming conferences, workshops and sessions focused on helping you deploy and understand DNSSEC and related issues:

- ***Reminder!*** **DNSSEC deployment to be featured at FOSE 2010:** A special presentation, **"What's Next in DNSSEC: Securing the Domain Name System"** will be presented at FOSE, the conference and exhibition for the U.S. government IT community, on **Wednesday, March 24, 2010 from 10:30 a.m. to 4:30 p.m.** Registration for the session will begin in November 2009 and is open to all FOSE and GovSec/U.S. Law attendees; pre-registration is required for the session, which is free. The day-long session will assess the U.S. federal response to securing its domains; examine challenges faced by agencies deploying DNSSEC; and share lessons learned and next steps as DNSSEC is deployed in other sectors. Software and hardware naming solutions also will be presented to update participants on available options for automating or easing deployment challenges. The session is organized by the DNSSEC Deployment Coordination Initiative and supported by the U.S. Department of Homeland Security. **To exhibit in the DNSSEC Pavilion at FOSE**, contact Don Berey, Show Director at 703-876-5073 or send him an email at dberey[at]1105govinfo[dot]com. For more information on the session or to register, go to http://fose.com/events/fose-2010/tracks/whats-next-in-dnssec.aspx.

ADD SECSPIDER DATA and: You can subscribe to the SECSpider blog at http://blog.secspider.cs.ucla.edu/

SPARTA
Pride in Performance

shinkuro
シンクロ

DNSSEC Operations: Setting the Parameters

SPARTA, Inc.[1]
Shinkuro, Inc.[2]

November 2009

[1] SPARTA, Inc., dba Cobham Analytic Solutions, is supporting the creation of this document under the DNSSEC Deployment Initiative with funding from the Department of Homeland Security Science and Technology (S&T) Directorate under contract FA8750-04-C-0229.

[2] Shinkuro, Inc. produced this document as part of the DNSSEC Deployment Initiative with funding from the Department of Homeland Security Science and Technology (S&T) Directorate under contracts FA8750-04-C-0269 and FA8750-10-C-0020. The information presented does not necessarily represent the views of the U.S. Government. For more information on the initiative, see http://dnssec-deployment.org

Overview

Domain Name System Security Extension (DNSSEC) adds digital signatures to the Domain Name System to secure it against a variety of attacks. With the signing of .ORG and other Top Level Domains (TLDs), registrars that provide name service for their customers and other DNS operators are looking for a reasonable set of DNSSEC configuration parameters. This memo provides advice on the values to choose for the configuration parameters associated with DNSSEC that provide good security without causing an undue burden on operators' name service infrastructures. The configuration parameters include key sizes and lifetimes, re-signing periods, and time-to-live (TTL) for the records. Some of these parameters are visible in the zone; others are internal to the operation.

This is a work in progress. Please provide feedback to dnssec-parameters@shinkuro.com.

Assumptions

We assume that the zones in question are relatively small and neither need nor would benefit from protection against zone walking. This assumption is the basis for some of the parameter values, so it's likely that zones with other attributes (e.g., larger, including non-obvious names) will require different parameters to maintain sufficient security.

All of the configuration parameters are from current experience and are applicable for the near future. Many of the choices are driven by the need to support DNSSEC during the initial phase of adoption. Therefore there will likely be changes as the population (recursive resolvers, clients) supporting DNSSEC grows and as we gain experience dealing with the increased resource requirements (CPU, bandwidth) of longer keys and other variables. In some cases, these choices are at variance with guidance from the U.S. National Institutes and Standards and Technology (NIST). These differences are noted and explained in the text.

DNS settings upon which DNSSEC settings are predicated					
RR Type	TTL				
SOA	1 day				
NS	1 day				
A/AAAA	≤1 day				
DNSKEY	1 day				
Max UDP Packet Size	1492[3]				
SOA Expire Value	1 week				
SOA Negative Cache Time	1 hour				

[3] 4096 is the default max UDP size for many authoritative server implementations. However, PMTU between the authoritative server and the recursive resolver may be less. If there are Ethernet-based links that do not support fragmentation (often due to firewall or similar device), a max UDP size of 1500 or less will be necessary. 1492 includes room for PPoE encapsulation and will suffice for the length of responses likely to be returned based on the DNSSEC parameters suggested above. If the maximum UDP size is exceeded, TCP fallback will be used. Additional measurement using tools like dnsfunnel (http://www.vantage-points.org/) may be needed should TCP fallback be greater than expected.

DNSSEC Settings					
DNSSEC Key Type	RSA(w/SHA1) Key Length[4]	Key Lifetime	Signature Lifetime	Re-Signing	Jitter[5]
KSK	1280	4 years	4 weeks	2 weeks	1 hour
ZSK	1024	1 year	2 weeks	1 week	1 hour
Negative Response	Support				
NSEC	Default				
		Iterations	Salt Size	Salt Lifetime	
NSEC3	Optional[6]	1[7]	64 bits	Signature lifetime	
Rollover	Prepublication/ Signing Policy	Introduction Time[8] for New Key	Retirement Time[9] for Old Key		
KSK	2K,1S[10]	1 week[11]	4 weeks		
ZSK	2K,1S	4 days	2 weeks		

[4] Key lengths are shorter and key lifetimes are longer than current NIST recommendations found in NIST Special Publication 800-81. These values should provide less of a burden in terms of signature size and re-signing in the near term. Since key lifetime is a matter of policy, not protocol, longer keys and shorter lifetimes can be issued in one rollover cycle if it is later determined they are needed.

[5] Jitter represents random variation in the signature timers that prevents certain pre-computation attacks.

[6] See the description NSEC and NSEC3 in the text for more information.

[7] Parameters such as this should be used explicitly in the signing command. BIND 9.6.1, for example, defaults to 100 iterations with NSEC3.

[8] *Introduction Time* is the time a new key of its type (KSK/ZSK) is added before it is the only key being used to sign.

[9] *Retirement Time* is the time an existing key of a type (KSK/ZSK) must continue to be used for signatures after a new key has been introduced.

[10] *2K,1S* means two keys and one active signature. Old keys must be removed to prevent DNSKEY answers from growing in size with each rollover.

[11] Assumes signed parent (TLD). Otherwise, use 45 days per RFC5011.

DS Records

DS records are stored at the parent and tie trust from the parent to the keys that may sign the DNSKEY set in the child. DS records are derived from the subject DNSKEY records per RFC 4034. If a zone is being signed and served by a registrant or a third party, the registrar must accept DS records and pass them to the registry accordingly.

NSEC and NSEC3 Explained

In addition to providing signed responses for resource records that exist, DNSSEC provides signed responses for negative replies (*provable non-existence*). DNSSEC provides a choice of two ways to do this, NSEC and NSEC3. NSEC is simpler to implement and results in smaller packets when a negative answer is required, but it provides an easy way for someone to find out all the names in the zone. NSEC3 provides protection against *zone walking*. Also, for very large zones, NSEC3 reduces the cost of initial operation because NSEC3 records can efficiently facilitate unsigned delegations.

If the zone is not very large and contains names that are easy to guess, e.g. “www,” “mail,” etc. then NSEC3 provides no advantage. For registrars and others who provide name service for customers with small zones that would not benefit from having their names hidden, we recommend the use of NSEC. For registrars and others who provide name service to customers with large zones or who require the protection of having their names hidden, NSEC3 is necessary.

Underneath the Covers of NSEC and NSEC3

NSEC[12] was the first solution to the problem of providing negative answers and continues to be viable in many cases. At a very high-level, NSEC records identify the gaps in zones. With some level of detail about the types of RRsets available, an NSEC record says little more than there’s no name between *A* and *B*. For example, there are no records between mail.example.org and www.example.org. Such an NSEC record can be generated and signed when the rest of the zone is signed and can represent the infinite number of non-existent name/RRset combinations between mail.example.org and www.example.org.

There are two issues with NSEC that caused some to search for an alternative. First, there’s *zone walking*. Since NSEC records identify spans of non-existent name/RRsets by identifying the names and RRsets that do exist at the end of the span, it’s fairly trivial to fetch one NSEC record after another and *walk* the entire zone, learning every name and RRset it contains. Before the application of DNSSEC, one could prevent the wholesale learning of the contents of a zone merely by disallowing zone transfers. The second issue is that NSEC must specify the status of every delegation (zones below the zone in question) as signed or not. As DNSSEC is rolled out, TLDs like .ORG will be signed before most of the

[12] Defined in RFCs 4034 & 4035

zones below it are signed. Without a more efficient mechanism to identify intent, large zones (e.g., .ORG) will grow larger because even unsigned delegations – the vast majority to start – must have an NSEC record.

Neither of these issues with NSEC will affect a zone with easily guessable names or ones that either do not have child zones or have child zones that are all using DNSSEC.

NSEC3[13] adds a cryptographically hashed name space and a new set of rules to prove non-existence and includes an option that permits unsigned delegations to be omitted from the chain of names protected by NSEC3 records. The former adds privacy when the names in a zone are not otherwise easily guessable and the latter makes a phased rollout of DNSSEC possible. For both of these reasons, some existing TLDs will sign using NSEC3.

NSEC3 requires additional computation when signatures are generated, when negative responses are generated and validated, and on unsigned referrals. NSEC3 negative responses are also larger. These are the reasons we suggest that NSEC be used for the small, simple, guessable, childless zones that many registrars will server for their customers.

Tools Used to Implement DNSSEC

The use of DNSSEC is still relatively new. For those using others' tools, it should be noted that default parameters differ not only between tools, but also between versions of the same tool. Our suggested parameters are not necessarily the default for these tools. Explicit setting of parameters is needed to prevent surprise when changing tools or upgrading existing tools.

[13] Defined in RFC 5155