(No.113) DNSSEC for ccTLDs: Securing National Domains

Go to Report (#report)

Status:
Accepted
Workshop Theme:
Managing Critical Internet Resources
Theme Question:

Question 5

Concise Description of Workshop:

This workshop is the result of the merger of workshop 107, "DNSSEC for ccTLDs: Securing National Domains", and workshop 113, "The Economic and Security Benefits of Securing the Internet's Unique Identifiers: DNSSEC".

Securing the critical infrastructure of the Internet, particularly ccTLDs, each country's most valuable online resource, is one of the most important Internet Governance issues being faced today. To ensure the security and privacy of the Internet's billions of users, important responsibilities must be undertaken by ccTLD operations and Internet service and network providers around the world in making DNSSEC, the cryptographic signing of domain names, available to the Internet-using constituents of each national top-level domain.

DNSSEC deployment at the root is an excellent example of how the bottom-up multi-stakeholder process has worked. DNSSEC has become a universal requirement for top-level domain operators, but today fewer than one third of ccTLDs have deployed it, making the remaining countries even more susceptible to online crime and fraud such as phishing and malware. As developed countries deploy DNSSEC more rapidly, the global burden of cybercrime falls ever more heavily on the shoulders of the remaining developing countries.

This workshop will provide an overview of the technology and practices required for successful DNSSEC deployment, including comprehensive deployments with solid, long track records; secure novel cost-effective approaches; practical examples from practitioners who have created the signing infrastructure for dozens of countries, as well as the root of the domain name system. The workshop will describe the operation and management of typical DNSSEC-signed country domains, including administrative structure, technical management, trust relationships, security practices, documentation and audit requirements, relationships with other stakeholders, business model and the role and purpose of DNSSEC in securing the domain name system and higher-level aspects of Internet networks.

The workshop will describe the current state of DNSSEC deployment and describe what developing and developed countries can do for all of us to reap the full benefits from this fundamental infrastructural Internet improvement. The workshop offers participants the opportunity to learn about DNSSEC from a practical point of view, and to realize its technical and business challenges and opportunities. At the same time, the workshop allows speakers and discussants to share their knowledge and expertise with participants who will be attending the IGF meeting. The workshop targets policy makers, business and technical advisors, particularly those of governments and businesses from the developing world.

AGENDA

- Welcome (Moderator)
- Panelist introductions (Moderator)
- DNSSEC Basics (Richard Lamb)
- PANELIST BRIEFINGS (5 min each)
  - Motivations behind deploying DNSSEC and experiences
- DISCUSSION (Panelists and Participants). Topic include but are not limited to:
  - Opportunities for security improvements and business development
  - Lessons Learned
  - What impact have you had or expect to have
- QUESTIONS AND ANSWERS SESSION (Participants and Panelists)
- Closing comments (Moderator)

Backgroung Paper:
dnsseciqf101rootb.pdf (http://wsms1.intgovforum.org/sites/default/files/dnsseciqf101rootb.pdf)
Organiser(s) Name:

- Bill Woodcock, Packet Clearing House
- Dr. Richard Lamb, ICANN

Previous Workshop(s):

http://www.intgovforum.org/cms/index.php/component/chronocontact/?chrono...

(http://www.intgovforum.org/cms/index.php/component/chronocontact/?chronoformname=Workshopsreports2009View&curr=1&wr=112)

Submitted Workshop Panelists:

- Emil Askerbeyli, Moderator, representing .AZ
- Ondrej Filip, CEO, CZ NIC, Czech Republic
- Dr. Demi Getschko, CEO, NIC BR, Brazil
- Svitlana Tkachenko/Dmitry Kohmanyuk, Hostmaster Ltd, .UA ccTLD administrator, Ukraine
- Charles Musisi, .UG ccTLD administrator, Uganda
- Roelof Meijer, CEO, SIDN, .NL ccTLD administrator, Netherlands
- Bevil Wooding, root-signing Trusted Community Representative, .TT Trinidad and Tobago
- Eduardo Santoyo, .CO ccTLD administrator, Colombia
- Bill Woodcock, Packet Clearing House
- Dr. Richard Lamb, ICANN

Name of Remote Moderator(s):
Baher Esmat, ICANN
Assigned Panellists:
Woodcock - Bill (/2012/panellist/woodcock-bill)
Lamb - Richard (/2012/panellist/lamb-richard)
Wooding - Bevil (/2012/panellist/wooding-bevil)
Filip - Ondrej (/2012/panellist/filip-ondrej)
Getschko - Demi (/2012/panellist/getschko-demi)
Tkachenko - Svitlana (/2012/panellist/tkachenko-svitlana)
Santoyo - Eduardo (/2012/panellist/santoyo-eduardo)
Kohmanyuk - Dmitry (/2012/panellist/kohmanyuk-dmitry)
Meijer - Roelof (/2012/panellist/meijer-roelof)
Transcript:
WS 113 DNSSEC for ccTLDs securing national domains.doc (http://wsms1.intgovforum.org/sites/default/files/WS 113 DNSSEC for ccTLDs securing national domains.doc)

Gender Report Card

Please estimate the overall number of women participants present at the session:
About half of the participants were women
To what extent did the session discuss gender equality and/or women's empowerment?:
It was not seen as related to the session theme and was not raised

Report

Reported by:
Bill Woodcock
A brief substantive summary and the main issues that were raised:

This panel was moderated by Richard Lamb, DNSSEC program manager at ICANN, and speakers included Demi Getschko, CEO of the Brazilian national registry; Eduardo Santoyo, administrator of the Colombian national registry; Svitlana Tkachenko and Dmitry Kohmanyuk of the Ukrainian national registry; Roelof Meijer, CEO, of the Dutch national registry; Ondrej Filip, CEO of the Czech national registry; Bill Woodcock, director of Packet Clearing House; and Bevil Wooding, root-signing Trusted Community Representative from Trinidad and Tobago. Dr. Lamb gave an overview of the state of DNSSEC technology. The national registry representatives each described the state of DNSSEC deployment within the ccTLDs they administer, and each mentioned one or two unique or unexpected challenges or accomplishments. Mr. Woodcock spoke on the topic of high-security DNSSEC practices and operation, and the future of DNSSEC as a cybersecurity building-block. Mr. Wooding described the state of DNSSEC deployment within the Caribbean region.

Conclusions and further comments:

DNSSEC has become an ever more critical cybersecurity building-block, in the wake of attacks on the DNS, problems with the Certificate Authority system and the increasing importance of authentication. DANE, which helps secure web sites, is the first major follow-on protocol, and we hope to see similar efforts to secure email and real-time text, audio, and video protocols soon.

Large payloads of DNSSEC responses have opened the door to more severe DNS reflection DDoS attacks, which in turn has required that new DNS response rate-limiting software be developed.

DNSSEC penetration has been very successful in countries with national registries that have pushed it aggressively, while countries without serious national-level buy-in generally have implementation and support lag at the registrar level.

Although not a primary barrier, implementation and maintenance costs and complexity were cited by audience members as hindering deployment.

Comprehensive awareness, education and training efforts are underway to address these and other deployment barriers by the same collaborative international multi-stakeholder community that developed DNSSEC and together manage and operate various parts of the Internet's DNS/DNSSEC infrastructure including the root.

These efforts include everything from sharing knowledge on best practices and lessons learned to providing free training to expanding free DNSSEC hosting offerings, e.g., with AFNIC joining PCH as the third operator of a FIPS 140-2 Level 4 DNSSEC signing infrastructure, and Brazil intending to be fourth. Together these organizations plan to work on a high-security DNSSEC implementation Best Current Practices document.