DNSSEC for the Enterprise: Why, When & How

Russ Mundy
Parsons
November 20, 2013
russ.mundy@parsons.com
DNSSEC for Enterprise: Why Bother?

• Protect your valuable DNS name
  – Your DNS name REPRESENTS YOU on the Internet
  – DNS based attacks can cause financial, reputation and real physical damage

• Proper DNS security and DNS management protects your organization
  – Use of DNSSEC essential but not enough
  – All DNS activities require proper security attention

• ‘Bad guys’ most likely to attack weakest spot

11/20/13

https://www.dnssec-tools.org/
Sponsored by: DHS S&T
DNSSEC for Enterprise: Why Bother?

• Permit use of current capabilities:
  – Web sites, e.g., www.icann.org, www.ietf.org
  – Web browsers
    • Bloodhound: full DNSSEC validation plus DANE support
    • Plug-ins available to validate URL bar DNS

• Use emerging DNSSEC-based emerging capabilities:
  – Enhanced security for Email
  – New secure capabilities not previously available

11/20/13

https://www.dnssec-tools.org/
Sponsored by: DHS S&T
Valid Web Site Content

http://www.dnssec-tools.org/

Sponsored by: DHS S&T
INVALID Web Site Content
From DNS Based Attack

Steve crocker admits DNSSEC won't solve world hunger.
Steve Crocker has admitted publicly that although DNSSEC solves many world-wide problems, it fails to solve them all. Specifically, it will not put an end to many world crises such as world hunger. In a statement released today he adds:

"I'm always looking for that one key technological achievement that solves everything but until I find it I'll need to simply continue solving one problem at a time."

.org shares Comcast DNSSEC advice for ISPs
In DNSSEC Deployment Among ISPs: The Why, How and What, Lauren Price of .org interviews the DNS guru at Comcast to see what they've learned and what advice they would give other ISPs considering DNSSEC deployment. The post answers such questions as 'What is the benefit to
1 address = multiple DNS lookups

www.weather.com

www.foxnews.com
DNSSEC for Enterprise: When?

https://www.dnssec-tools.org/
Sponsored by: DHS S&T
DNSSEC for Enterprise: When?

NOW!!
DNSSEC for Enterprise: How?

• Ensure DNS roles and responsibilities defined
  – E.g., Who has policy responsibility for DNS such as what names are used, how and what content goes into DNS zones?
  – Where does an enterprise get their DNS names (probably from one or more registrar(s))? 
  – What activity/entity has responsibility for name server operation for the enterprise?
  – Is there a defined authority for DNS changes?
DNS Zone Content Flow
(for example, www.icann.org or www.cnn.com)

Provisioning Area

- Content Input

Content Starts Here

- Registrars

- DNS ‘Content Picture’

- DNS Resolvers

- User Applications

Publication Area

- Content Output

- Content Used Here

- Registrants

- Zone Name Servers

- Registrars

- Provisions

- Public Area

- Content Here

- Output

- DNS

- Content Picture

- Input
DNSSEC for Enterprise: How?

• Once roles and responsibilities are defined, all roles should be examined to determine if sufficient security is being used:
  – E.g., Is there sufficient security between the enterprise and the registrar(s)?

• Each technical element, e.g., registrar, name servers, must be able to do their DNSSEC functions – correct if needed.

• Consider independent monitoring of DNS
DNSSEC for Enterprise: How?

• Initiate DNSSEC signing process with a non-mission critical zone
  – Make sure registrar & name server functions properly handle DNSSEC related actions properly
  – Test properly functionality & flow with available open source tools

• Once all is solid, use same steps for mission critical zones

• Ensure proper checks and measures in place

11/20/13

https://www.dnssec-tools.org/
Sponsored by: DHS S&T
DNSSEC for Enterprise: What next?

Make use of new and additional security capabilities for a more secure enterprise