DNSSEC for the Enterprise: Why, When & How

Russ Mundy

Parsons

November 20, 2013

russ.mundy@parsons.com

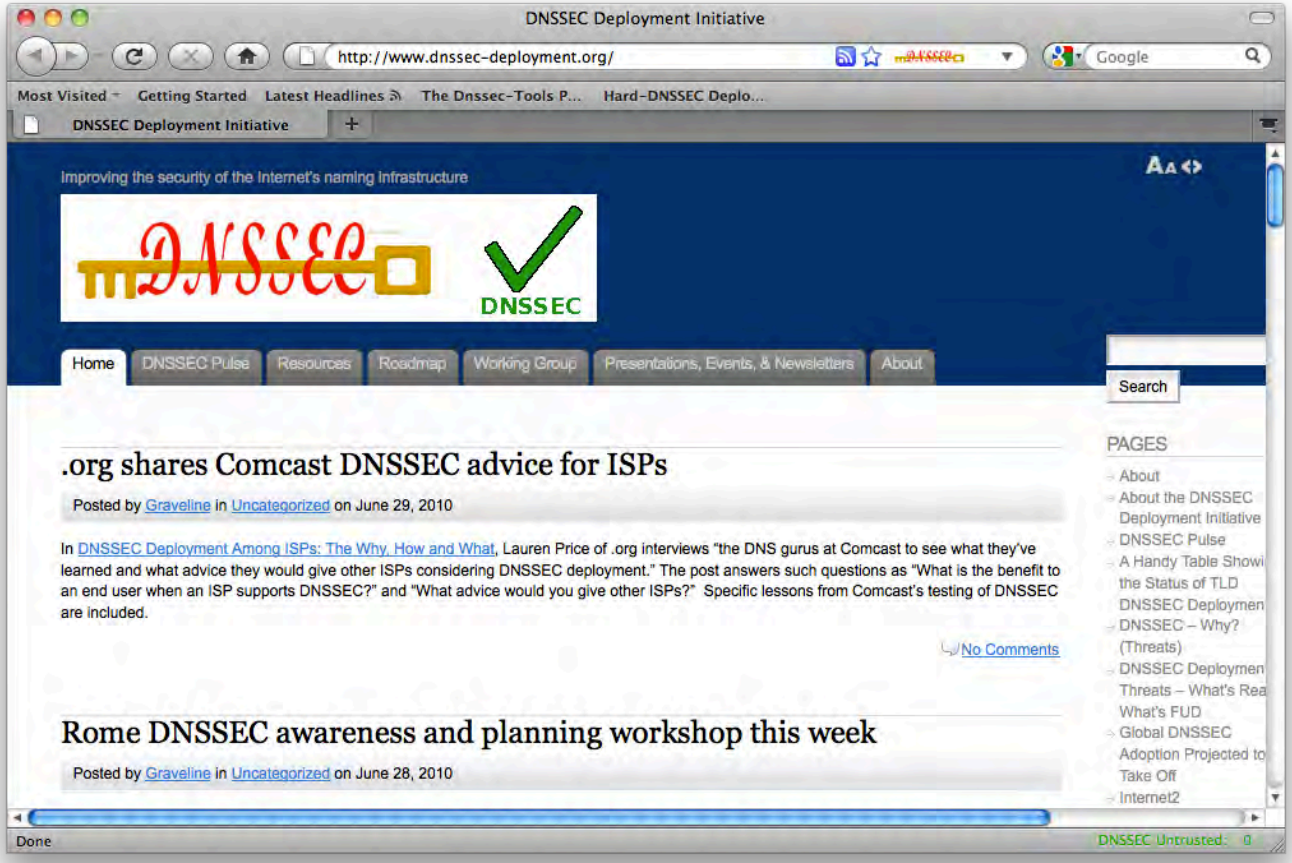
DNSSEC for Enterprise: Why Bother?

- 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

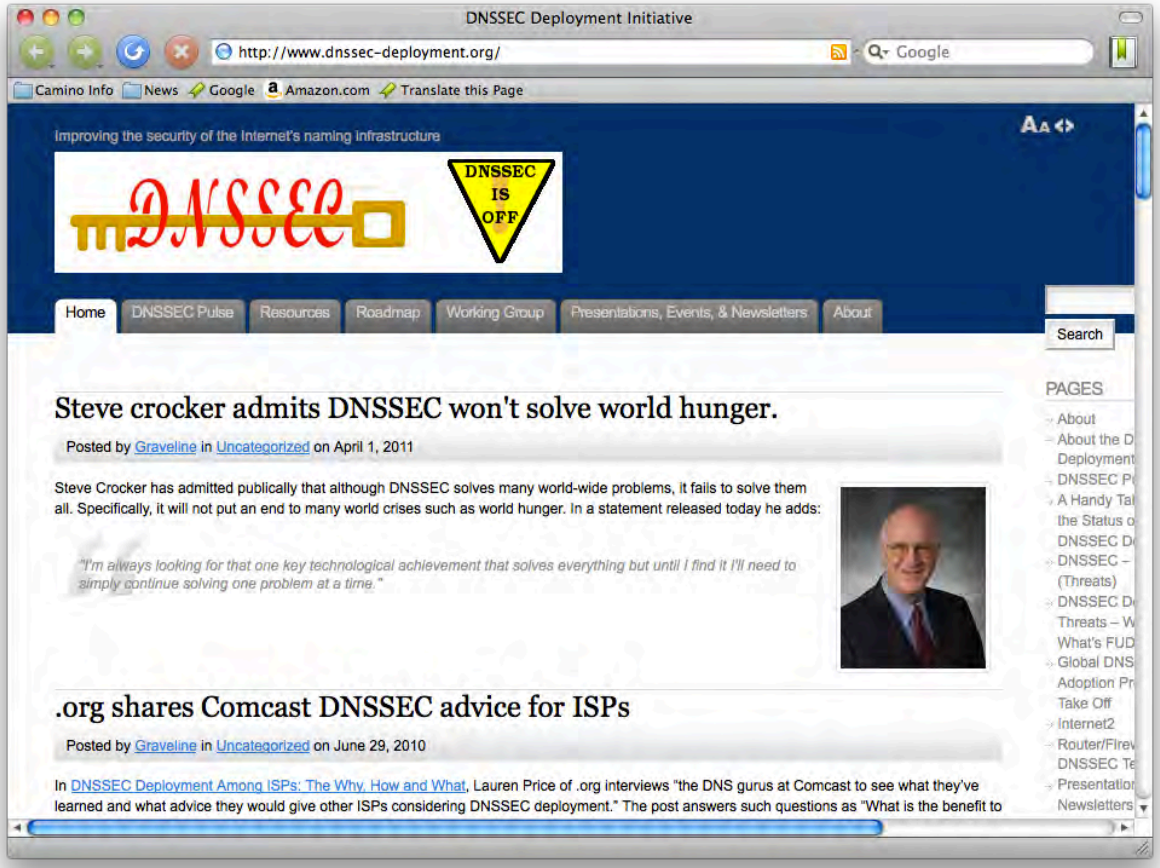
DNSSEC for Enterprise: Why Bother?

- 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

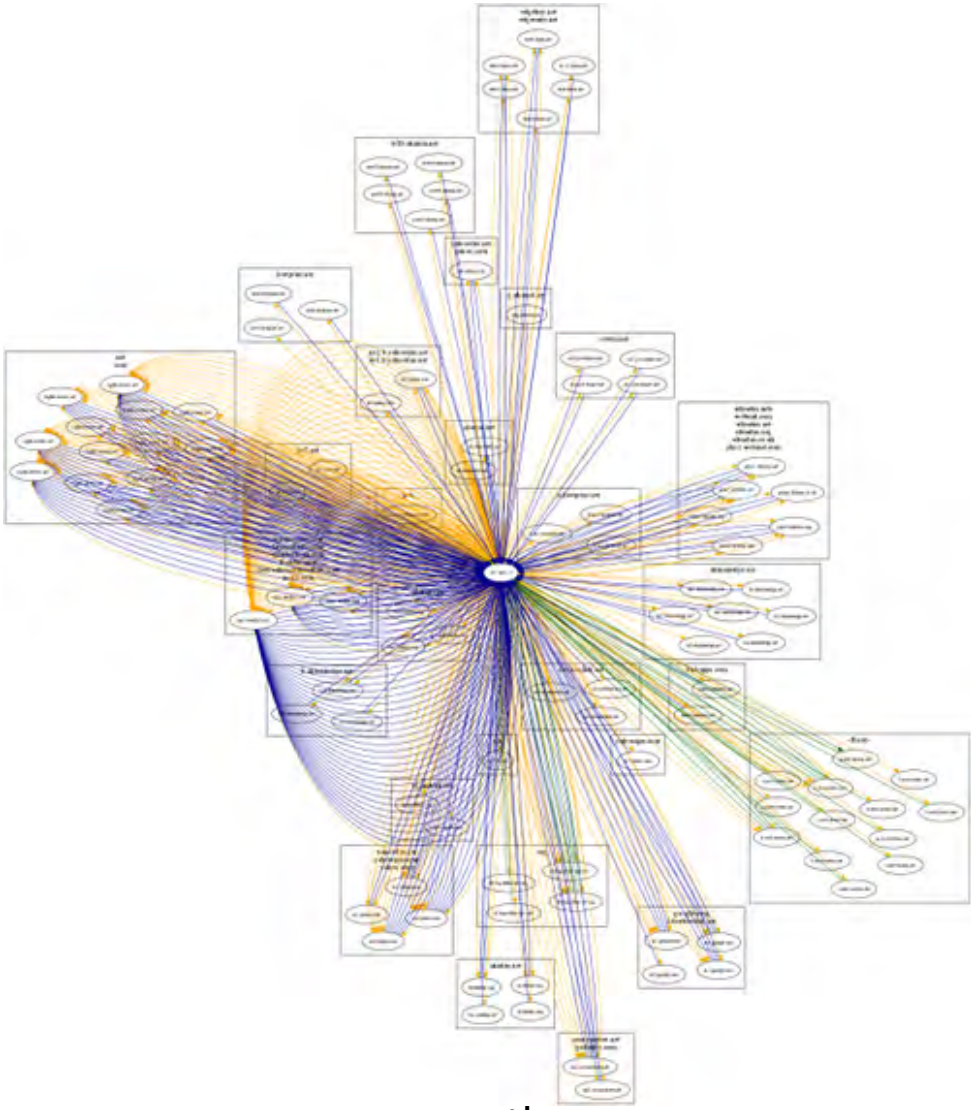
Valid Web Site Content



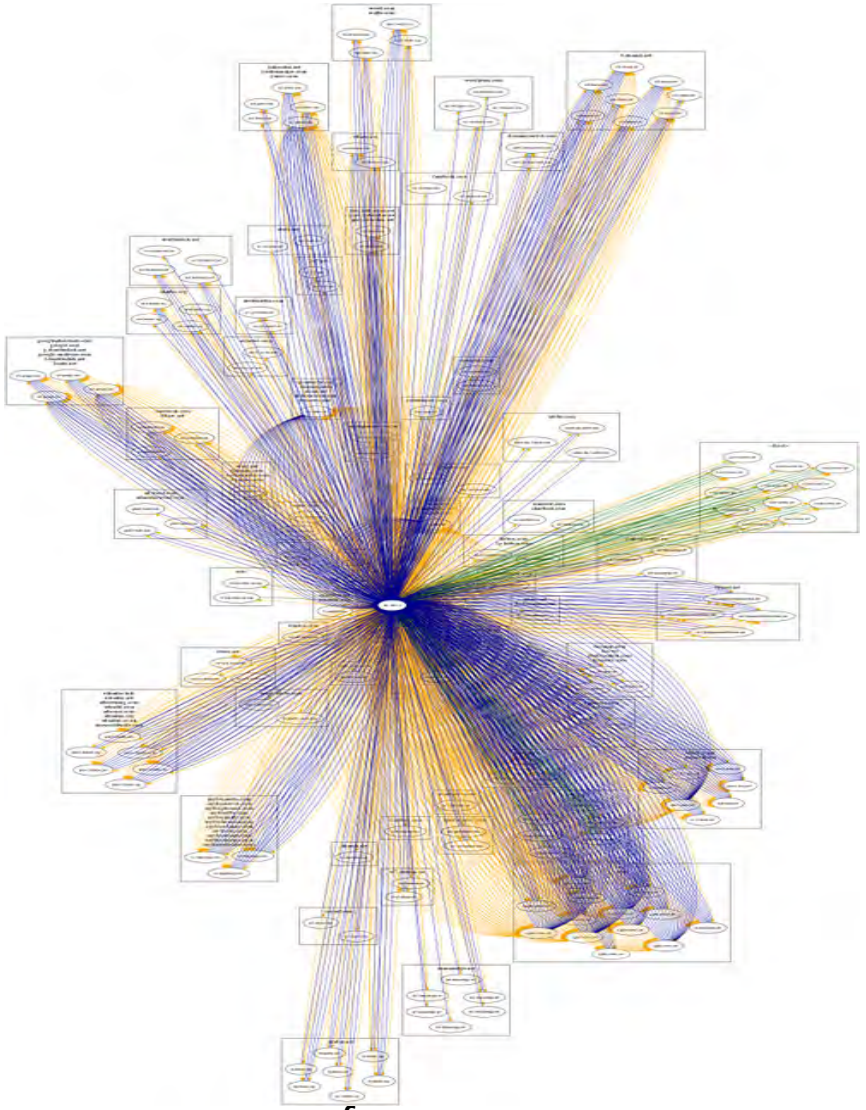
INVALID Web Site Content From DNS Based Attack



1 address = multiple DNS lookups



www.weather.com



www.foxnews.com

DNSSEC for Enterprise: When?

DNSSEC for Enterprise: When?

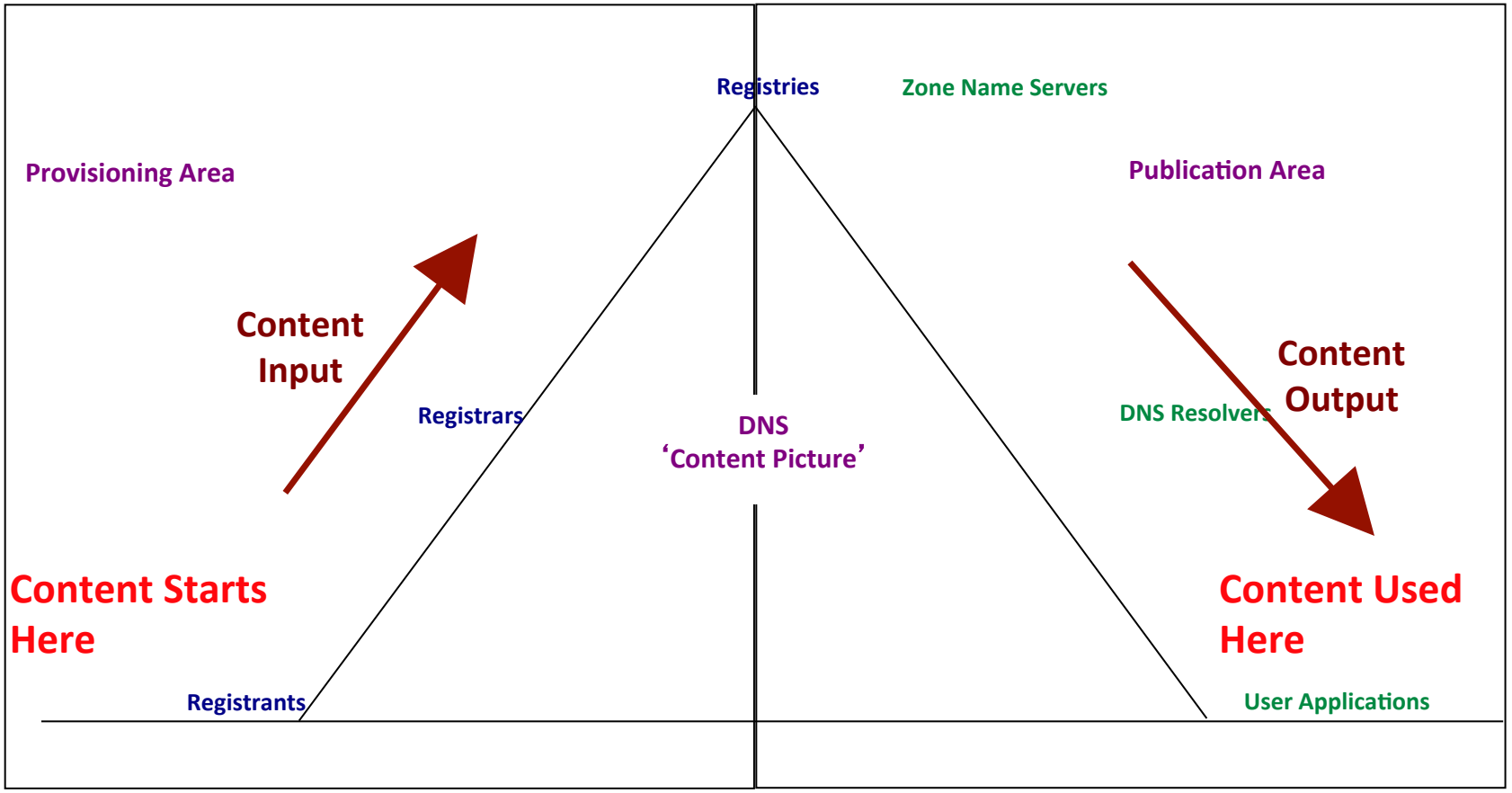
NOW!!

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)



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

DNSSEC for Enterprise: What next?

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