FCC CSRIC III

Working Group 5

DNSSEC Implementation Practices for ISPs

Steve Crocker

CEO, Shinkuro, Inc.

steve@shinkuro.com

- U.S. Federal Communication Commssion (FCC)
- Communications Security, Reliability and Interoperability Council (CSRIC)
  - This is the third Council
- Working Group 5 – DNSSEC Implementation Practices for ISPs
- Working Group includes ISP DNS experts and DNSSEC experts

http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii

Formal Structure

- ✓DNSSEC Implementation Practices for ISPs
- DNS Security Performance Metrics
- Status of DNS Security Performance Metrics

Task Structure

- Protection against cache poisoning
- Security increasingly resonates with customers
- DNSSEC can be a market differentiator for early adopters
- DNSSEC may help ISPs avoid some costs if a cache poisoning attack occurs
- ISP DNSSEC awareness in DNS recursive name servers is necessary for end-user validation (e.g., DANE)

- Recommend best practices for deploying and managing the Domain Name System Security Extensions (DNSSEC) by Internet service providers (ISPs).
- Recommend metrics and measurements for evaluation of the effectiveness of DNSSEC deployment by ISPs.

WG5 Objective

- Unclear U.S. government policy regarding use of DNS redirection to block botnets and advanced persistent threats (APTs) as well as other malicious or illicit activity
- DNSSEC efforts may create an inaccurate impression of DNS infrastructure security
- Loss of nonexistent domain (NXDOMAIN) revenues

The Challenges - 1

- Perceived impact to Internet service reliability
- Poor WHOIS contact information complicates troubleshooting
- DNSSEC may exacerbate DNS amplification attacks
- Possible unanticipated abuses of DNSSEC-enabled services for attacks

The Challenges - 2

- Lack of direct financial benefit from DNSSEC adoption
- More signed domains needed
- End-system validation obviates the need for ISP validation
- DNSSEC may increase operating costs for ISPs and other DNS service providers

The Challenges - 3

- Content distribution network service providers, e.g. Akamai, may face additional challenges in implementing and managing DNSSEC
- Alternate DNS providers may compete with services provided by ISPs, and those providers may not implement DNSSEC

The Challenges - 4

- Categorization of the ISP DNS service

vs

- End system requests

Tells us

- ISP service level necessary to serve users who do their own validation and users who depend ISP validation

ISP and End System Interaction

A. Always DNSSEC Validating

B. DNSSEC Aware **(Resolver sets DO bit in its queries in order to keep cache consistent.)**

C. EDNS0 Enabled

D. RFC 1034 (very old)

1. RD bit off; end system goes around ISP to authoritative servers
2. RD, EDNS0, DO and CD
3. RD, EDNS0 and DO
4. RD and EDNS0
5. RFC 1034

	A	B	C	D
1	NA	NA	NA	NA
2	V or D	D	P	C
3	V	D	P	C
4	V	P	P	C
5	P	P	P	P

Interaction Results

- V = Validated
- D = DNSSEC chain returned

- P = Plain DNS, no valid'n or DNSSEC records
- C= Compatibility mode (RFC 1034)
- NA = Not Applicable

Interaction Key

- ISPs implement their DNS recursive nameservers so that they are at a minimum DNSSEC-aware, as soon as possible.
- Key industry segments, such as banking, credit cards, healthcare and others, sign their respective domain names with DNSSEC.

The Recommendations - 1

- Software developers study how and when to incorporate DNSSEC validation functions into their software.
  - operating-system, web-browser, and other Internet-focused applications

The Recommendations - 2

ISP support for DNSSEC is necessary even if end systems eventually perform all validation. ISPs must be able to, at least, recognize DNSSEC-related traffic and allow it to pass for the smooth functioning of an end-to-end, DNSSEC-secured system.

Thank You

Steve Crocker
steve@shinkuro.com