DNSSEC Status Report

Steve Crocker

ICANN SSAC

SAC026, *Statement on Deployment of DNSSEC*

1. Protocol completeness
2. Key rollover process
3. Trust anchor repositories
4. Implementation and deployment testing
5. Performance and error analysis, establishing metrics for success
6. End User Application development
7. Availability of DNSSEC on commonly used DNS server platforms

1. Protocol Completeness

- Multiple, interoperable implementations of DNSSEC standards exist
  - RFC 4033, DNS Security Introduction and Requirements
  - RFC 4034, DNS Security Extensions Resource Records
  - RFC 4035, DNS Security Extensions Protocol Modifications
  - RFC 5011, DNS Key Rollover
  - RFC 5155, DNSSEC Hashed Authenticated Denial of Existence
- In use in test and production environments
  - Bulgaria, Czech Republic, Sweden, Brazil, Puerto Rico, dot Museum, dot Org, dot Gov

1. Ongoing standards activities

- Expanded set of return values for error responses from validating resolvers
- Formal DNSSEC Validator API
- Framework for Trust Anchor Repositories
- Conventions for transferring secured domains from one registrar to another
- Migration methods
  - to larger keys sizes for existing digital signature algorithms
  - to a newly specified digital signature algorithm

2. Key Rollover & 3.Trust Anchor Repositories

- Treated together (related)
- Four ways to deal with trust anchor rollover
  - Manually
  - via a TAR (e.g., IANA ITAR)
  - Via DNS Look aside Validation (DLV)
  - automatically via the RFC 5011 process
- Report examines issues in some detail
- Initial work complete, further work and consensus within the community is needed

4. Implementation and Deployment testing

- SAC035, Test Report: DNSSEC Impact on Broadband Routers and Firewalls
  - Laboratory testing of most popular 24 devices
  - Summary of results:
    - All 24 units could route DNSSEC queries addressed to upstream resolvers without size limitations.
    - Units that proxy DNS queries addressed directly to them exhibit varying degrees of success, especially when processing UDP encapsulated DNSSEC responses larger than 512 bytes
- SSAC report stimulated additional industry testing
- Further testing on enterprise and carrier grade “middle boxes” is appropriate

5. Performance and error analysis

- Authoritative name servers
  - 5x to 10x increase in memory footprint
  - 2x to 5x increase in answer size
  - Negligible increase in computation time

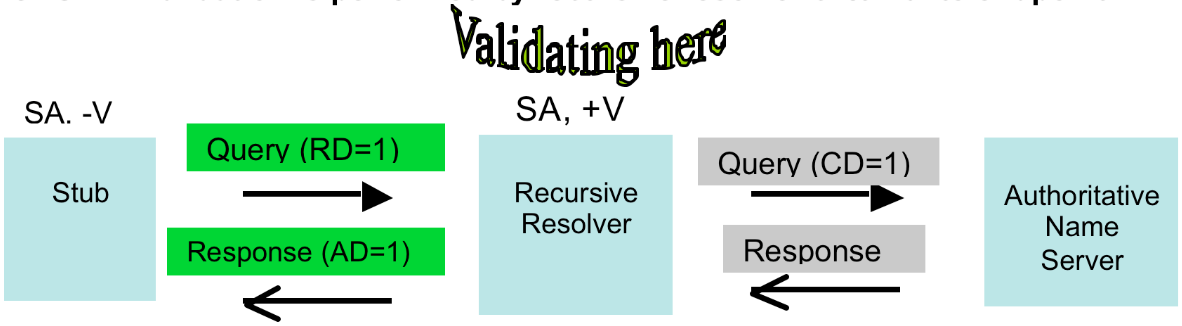
- Validating resolvers
  - Less complete data
  - Initial experience from Comcast, among others, shows no problems

6. End User Application Support

- No formal survey performed as yet
- Open source DNSSEC validation libraries and patches available for Linux, BSD, etc. for
  - Web browsers
  - Email clients and servers
  - FTP
  - IP security (IPSec clients)
  - Secure Shell
- Windows 7 and 2008 R2 DNS client will support a non-validating security-aware stub resolver
  - Lack of availability of stub resolver for current Windows Operating Systems inhibiting adoption by 3rd party application developers

Deployment Scenarios

CASE 1: Validation is performed by recursive resolver *external* to endpoint



Validating here

SA. -V

Stub

Query (RD=1)

Response (AD=1)

SA, +V

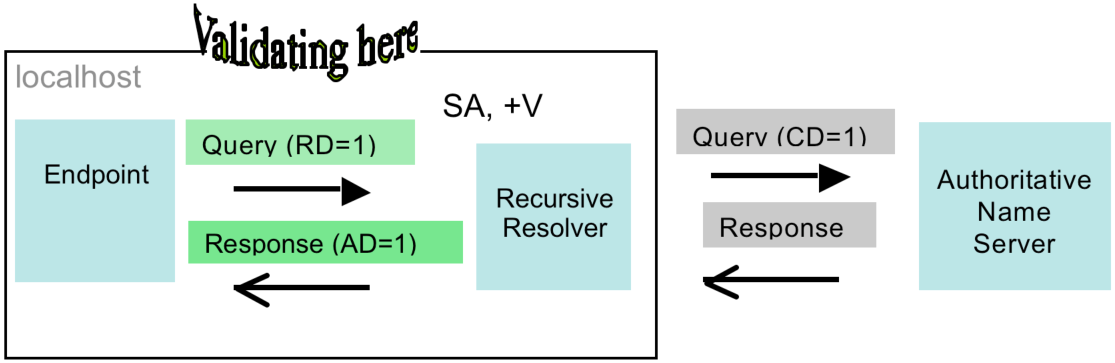
Recursive Resolver

Query (CD=1)

Response

Authoritative Name Server

Case 2: Validation is performed by endpoint running a validating recursive resolver



Validating here

localhost

Endpoint

Query (RD=1)

Response (AD=1)

SA, +V

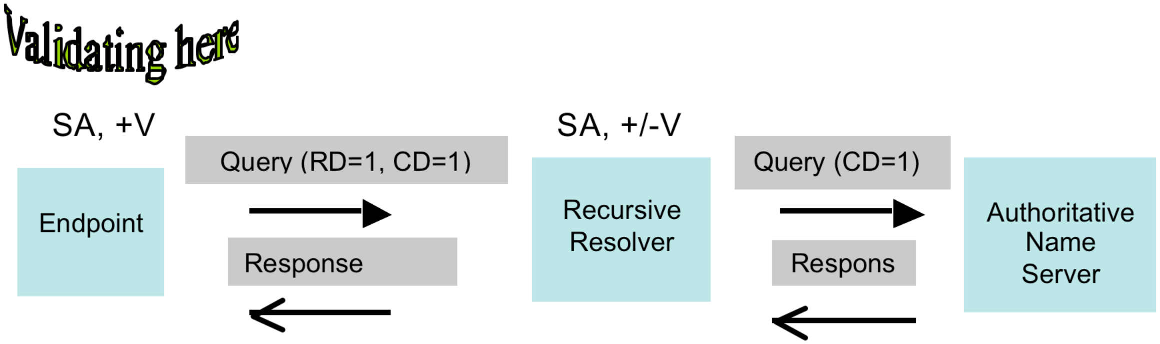
Recursive Resolver

Query (CD=1)

Response

Authoritative Name Server

Case 3: Validation is performed by validating endpoint via recursive resolver



Validating here

SA, +V

Endpoint

Query (RD=1, CD=1)

Response

SA, +/-V

Recursive Resolver

Query (CD=1)

Respons

Authoritative Name Server

7. Availability of DNSSEC name server platforms

- SAC 030, Survey of DNSSEC Capable DNS Implementations
- Responses from commercial developers (represents preponderance of installed base)
  - 11 of 17 products now support DNSSEC.
    - 8 products can host a signed zone and return DNSSEC metadata
    - Key management tools are available for 10 of the 11 products
    - DNSSEC-aware utilities are available for 8 products.
    - All 11 products support RSA/SHA1 and DSA signatures
    - 8 products support more than this minimum set
    - Five products supported NSEC3
  - 3 commercial manufacturers indicated they would support DNSSEC by 1st quarter 2009
    - (in process of confirming)

Conclusions

- Main open areas are…
  - Trust anchor distribution and use
  - SOHO broadband firewalls and routers
  - Integrating DNSSEC with recursive resolvers

- Deployment experience is accumulating
- Registrars and recursive resolvers are the current areas