Incremental Deployment of a Signed Root Zone

Internetdagarna
4 November 2009

Ashley Heineman, NTIA

Joe Ableу, ICANN

Joe Waldron, VeriSign

Jakob Schlyter, Kirei

This design is the result of a cooperation between ICANN & VeriSign with support from the U.S. DoC NTIA

Goals

Goals

- Deploy a signed root zone
  - Transparent processes
  - Audited procedures
  - Trust
  - DNSSEC deployment
    - validators, registries, registrars, name server operators

Issues

DO=1

- A significant proportion of DNS clients send queries with EDNS0 and DO=1
- Some (largely unquantified, but potentially significant) population of such clients are unable to receive large responses
- Serving signed responses might break those clients

Rollback

- If we sign the root, there will be some early validator deployment
- There is the potential for some clients to break, perhaps badly enough that we need to un-sign the root (e.g., see previous slide)
- Un-signing the root will break the DNS for validators

Proposal

Deploy Incrementally

- Serve a signed zone from just L-Root, initially
- Follow up with J-Root
- Then other root servers >A
- Last, A-Root

Deploy Incrementally

- The goal is to leave the client population with some root servers not offering large responses until the impact of those large responses is better understood
- Relies upon resolvers not always choosing a single server
  - Note we propose leaving A until last

DURZ

- "Deliberately Unvalidatable Root Zone"
- Sign RRSets with keys that are not published in the zone
- Publish keys in the zone which are not used, and which additionally contain advice for operators (see next slide)
- Swap in actual signing keys (which enables validation) at the end of the deployment process

DURZ

```
.       3600    IN      DNSKEY  256  3  5 (
                        AwEAAa++++++++++++++++++++++++++++++++
                        ++THIS/KEY/AN/INVALID/KEY/AND/SHOULD
                        /NOT/BE/USED/CONTACT/ROOTSIGN/AT/ICA
                        NN/DOT/ORG/FOR/MORE/INFORMATION+++++
                        ++++++++++++++++++++++++++++++++++++
                        ++++++++++++++++++++++++++++++++++++
                        ++++++++++++++++++++++++++++++++++++
                        ++++++++++++++++++++++++++++++++++++
                        ++++++++++++++++++++++++++++++++++++
                        ++++++++++++++++++++++/=
                        ) ; Key ID = 6477
```

DURZ

- Deploy conservatively
  - It is the root zone, after all
- Prevent a community of validators from forming
  - This allows us to un-sign the root zone during the deployment phase if we have to without collateral damage

Measurement

- For those root servers that are instrumented, full packet captures and subsequent analysis around signing events
- Ongoing dialogue with operator communities to assess real-world impact of changes

Testing

- A prerequisite for this proposal is a captive test of the deployment
  - Test widely-deployed resolvers, with validation enabled and disabled, against the DURZ
  - Test with clients behind broken networks that drop large responses

Thoughts?

- Feedback on this proposal would be extremely welcome
  - Here in the room
  - E-mail Jakob, Joe or Joe