DNSSEC Trust Anchor Repositories (TAR) Update

Russ Mundy
Co-Chair DNSSEC Deployment Initiative
Russ.Mundy@cobham.com / mundy@sparta.com
www.dnssec-deployment.org
DNSSEC Trust Anchors

- Starting point for DNSSEC validation
- Choice of trust anchors is a local decision
  - Bad choice of trust anchors can completely undermine value of DNSSEC
- In the absence of a valid secure delegation from the parent zone to the child zone, a validator MUST have trust anchors for the child zone in order to be able to validate names from (and below) it.
Number of Trust Anchors

**Ideal:** Entire DNS Tree is signed

**Reality:** DNS Name Space is fragmented into a (potentially large) number of “islands of trust”
(very quick) Background

DNSSEC Trust Anchor Repositories (TARs)

• What are they?

• Why would TARs be used?
(very quick) Background (Cont.)

DNSSEC Trust Anchor Repositories (TARs)

• What are they?
  – Way to get trust anchors to validators
  – Validator gets multiple trust anchors by using a single TAR
(very quick) Background (Cont.)

DNSSEC Trust Anchor Repositories (TARs)

• Why would TARs be used?
  – Facilitate DNSSEC Deployment by “filling holes in the hierarchy”
  – Used by ‘community of interest’ to provide their community needs

(Not discussed further in this presentation)
Trust Anchor Repository (cont.)

Trust Anchors from Islands of Trust
Pros & Cons: Very High-level Summary

• Pros:
  – “holes in the hierarchy” will persist for a long time
  – Provides method for any signed zone to be used by any validator
  – ...

• Cons:
  – Diverts/detracts effort from dnssec deployment
  – Lowers motivation for getting parent zones signed
  – ...

TAR Discussion Venues

- DNSSEC Deployment plenary telecons
- DNSSEC Deployment mail list
- ICANN meeting discussions
- RIPE meetings
- IETF meetings (note: NOT in conjunction with any working group)
TARs: Current Status

• Limited consensus on TARs
  – What should & should not be considered a DNSSEC TAR
  – Whether or not one or more DNSSEC TAR(s) are needed
TARs: Current Status (Cont.)

• By some definition for DNSSEC TAR, several exist today:
  – ICANN ITAR
    https://itar.iana.org/
  – ISC DLV
    https://www.isc.org/solutions/dlv
  – SecSpider
    http://secspider.cs.ucla.edu/
  – IKS Jena Survey
    http://www.iks-jena.de/leistungen/dnssec.php
TARs: Current Status (Cont.)

• Some developing consensus on need for DNSSEC TARs of some sort
  – lack of consensus on what should - or should not - be considered a DNSSEC TAR

• DNSSEC Deployment WG
  – Plan to develop Best Current Practice type of description for one or two ‘levels’ of DNSSEC TAR
  – Document the details
Some pointers to TAR material

• TAR SONIC - Paper
  http://www.dnssec-deployment.org/tar/tarpaper.pdf
  presentation at ICANN 32
  http://par.icann.org/files/paris/Mundy-tar-sonic.pdf

• Challenges to DNSSEC Deployment (dnssec-deployment mail list archive)
More pointers to TAR material

• SecSpider Presentation (dnssec-deployment mail list archive)

• TAR meeting notes from 25 Mar 09 (dnssec-deployment mail list archive)
  http://mail.shinkuro.com:8100/Lists/dnssec-deployment/Message/2039.html?Language=
Closing Thoughts

• Folks who have thought about DNSSEC TARs often think they know exactly what a TAR is (or is not) and are surprised when other people don't view TARs the same way!

• Details of a TAR are important
  – many people have different views of what the details of a DNSSEC TAR should be
Contributions Welcome

• Questions & Comments Today
  (Time permitting)

• Participate in the DNSSEC Deployment mail list and plenary meetings
  http://www.dnssec-deployment.org/