DNSSEC in the Reverse Tree

ICANN Beijing 2013
DNSSEC Workshop
Joe Abley

Reverse DNS

- Reverse DNS concerns the mapping of numbers (addresses) to names
- For IPv4, this involves delegations from the IN-ADDR.ARPA zone (RFC 1034)
- For IPv6, we use IP6.ARPA (RFC 3152)
- The IN-ADDR.ARPA and IP6.ARPA zones are managed by ICANN and served by nameservers operated by the five RIRs and ICANN (RFC 5855)

IN-ADDR.ARPA

- Originally managed and distributed by ARIN, and served by 12 of the 13 root servers
- Managed and signed by ICANN since 2011
- http://in-addr-transition.icann.org/

IP6.ARPA

- Managed and published by ICANN since delegation (RFC 3152)
- Signed since 2010

Signing Parameters

- 2048bit RSA KSK with 12-month rollover
- 1024bit RSA ZSK with 3-month rollover
- SHA256 digest
- Signatures valid for 7 days
- NSEC for authenticated denial of existence

Zone Management

- Both zones are managed through a RESTful HTTPS interface to a system hosted at ICANN
- RIRs authenticate using client-side certificates to manage delegations
- No glue to worry about in the reverse tree, NS and DS maintenance only

Secure Delegations

- 199 out of 228 IPv4 delegations are secure (DS RRSet exists in the IN-ADDR.ARPA zone)
    - some are intentionally insecure (10)
    - some are legacy /8 delegations managed by RIRs, but delegated directly to end users
- 50 out of 56 IPv6 delegations are secure (DS RRSet exists in the IP6.ARPA zone)
    - some are intentionally insecure (2.0.0.2)
    - some are delegations directly to LIRs for large allocations

Direct Delegations

- Delegations not to RIR nameservers are still managed by RIRs
    - legacy /8 holders and other end-users with direct delegations do not interact directly with the ICANN rdns management system
    - in each case such end-users manage delegations through their local RIR

Questions?

ICANN Beijing 2013
DNSSEC Workshop
Joe Abley