DNSSEC In the Reverse Tree – An ARIN Prospective

Mark Kosters, CTO

ARIN Initiatve

- ARIN's board asked ARIN Staff to implement DNSSEC
- Turned out to be easy
- Lots of prior work to learn from and emulate
- Followed their work plus fixed tweaks to make it less operationally impactful

Past Efforts

- **Many TLD's have DNSSEC turned on – .SE, .BR, .ORG, etc**
- **Lots of prior work to learn from and emulate**
- **RIPE Turned on DNSSEC back in Q4 of 2005 via the DISI Project**
  - Great description of their keying policies
  - Useful tools
- **.SE project**
  - Again useful tools available – especially with key management

ARIN's Plan

- **Lots of prior work to learn from and emulate**
- **Follow RIPE's key procedures with some modifications on timing**
- **Survey key management tools**
  - Opendnssec
  - Secure64
  - DISI Project (RIPE)
  - DNSSEC Zone Key Tool
  - others

Principle of No Surprise

- **Documented the plan – took a lot from RIPE**
  - http://www.ripe.net/rs/reverse/dnssec/
- **Had a Consultation on arin-consult mailing list**
- **Slow rollout**
  - https://www.arin.net/about_us/dnssec/

Complications

Trust anchors

- **Parents (root/arpa/in-adr.arpa) are not signed**
- **Needs to be individually configured per recursive resolver**
- **Available at:**
  - https://www.arin.net/about_us/dnssec/trust_anchors.html (secured via https)
  - ftp://ftp.arin.net/pub/zones/trust_anchors.txt
  - ftp:/ftp.arin.net/pub/zones/trusted_keys.txt

– OR –

Aggregated Trust anchor Service (DLV)

- https://dlv.isc.org/

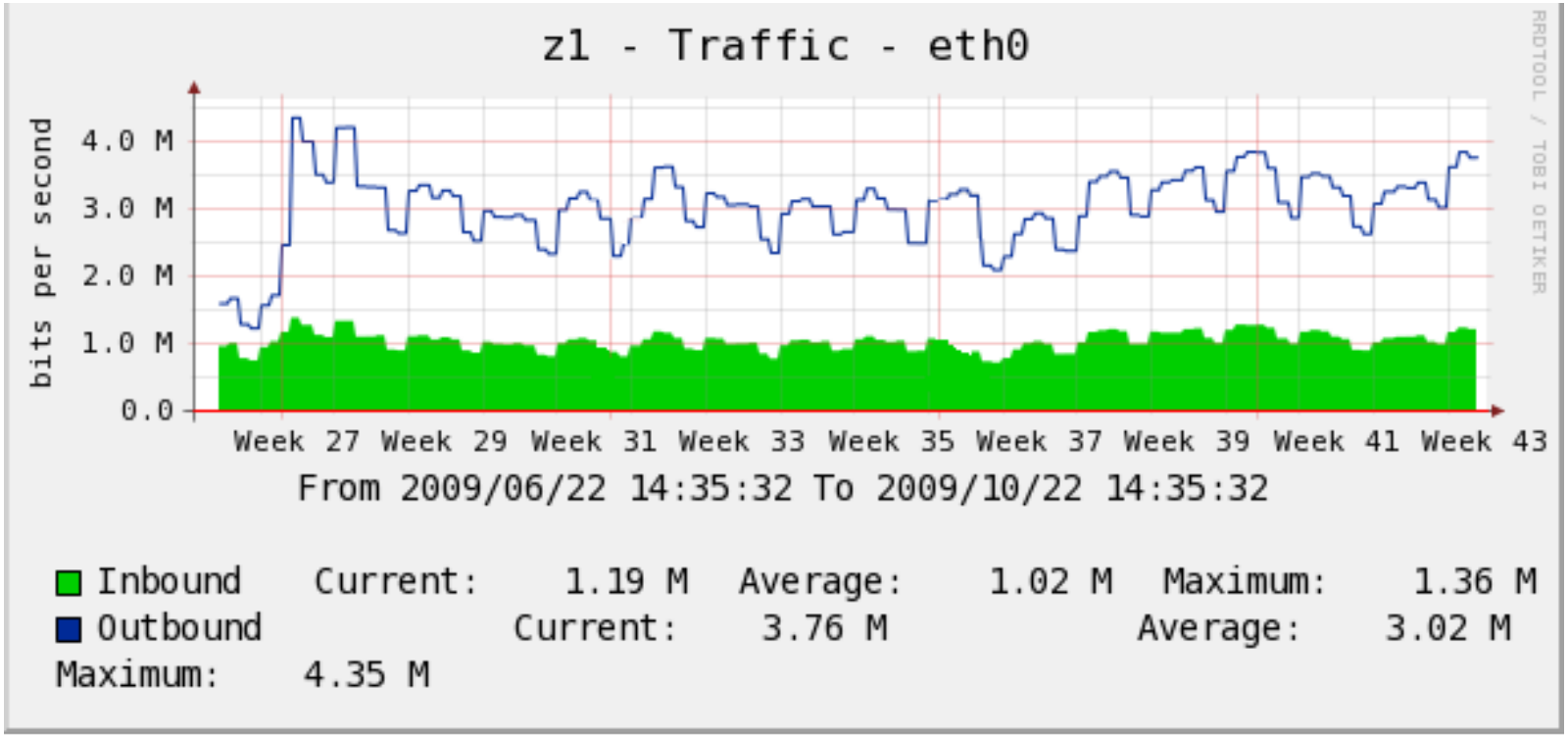
Phase 1 DNSSEC Capability

- **Validate that VeriSign and ARIN servers are conformant**
- **Got a green light for NSEC but not NSEC3**

Phase 2 – Signing the Zones

- **Turned on afternoon of July 1, 2009**
- **Both VeriSign and ARIN NOC Operations on high alert**
- **Saw increase of outbound traffic z.arin.net:**
  - Prior to DNSSEC, we were doing ~ 4.5 Mbps.
  - After DNSSEC, we jumped up to about 10.5 Mbps.
  - Currently 15–17 Mbps

Obligatory Graph



One instance in load-balanced site

Phase 3 – Serving Signed Child Zones

- **Backend Schema is currently Insufficient**
  - DNS records tied to Network Allocations – needs to be done per delegation
  - Large back-office effort 50% complete
- **Provisioning for this Service will be placed in ARIN Online**
  - Consistent and higher security then existing templates
  - Integrated into a managed dns service
- **Expected to rollout in 2010**