DNSsec

Gerry Sneeringer
Director, IT Security
University of Maryland
sneeri@umd.edu

The Agenda Slide

Features of DNSSEC

- Data Integrity – data is received as intended by originator
- Source Authentication – data is received from the correct source
- Authenticated Denial of Existence – NXDOMAIN is confirmed and validated

DNSSEC Does Not…

- Provide for Confidentiality
- Prevent Attacks, only detects them
- Protect against Denial of Service attacks
- Stop Spam, Phishing, or Self-Centered Blogging

History of DNSSEC

- 1990 – Bellovin discovers major security flaw in DNS… doesn't publish it until 1995
- 1997 – RFC 2065, first shot at DNSSEC
- 1999 – RFC 2535, Bind9 first DNSSEC capable implementation
- 1999-2001 – Test deployments… key handling doesn't scale

History Continued

- 2001 – New Delegation Signer Resource Record, RFC 2535bis
- 2002-03 – Bind9 supports DS RR, more test deployments
- 2004 – Bind 9.3 and NSD2 support 2535bis
- 2005 – RFC 4033,4034,4035 published
- Oct 05 - .SE becomes first ccTLD to deploy DNSSEC, RIPE/NCC moving towards signing reverse zones

How Does It Work?

- Four additional RR types:
  - DNSKEY – public keys used to sign data in the zone
  - NSEC – “Next Secured” – describe the gaps in the zone file to establish what ISNT there
  - RRSIG – Signatures of the other RR’s in the zone (for every authoritative RR in the zone, there is an RRSIG)
  - DS – Designated Signer – Only in the top most zone, SHA-1 hashes of the keys of the children zones. Downward hierarchy of trust

Where does trust start?

- Trust Anchors
  - Resolvers need to have the public key for the root of each *Island of Trust.*
  - Only the anchor keys need to be published out of band
- Assigning Trust
  - Child key signed with Parent key
  - Signed key stored in parent zone, unsigned key in child zone

Using DNSSEC to validate

- Resolver queries root for RR
- Referrals until reaching zone for which resolver has an anchor key
- Query DNSKEY, compare against stored key
- Query validated server, receive delegation with DS record, query next server compare key against hash in DS record
- Rinse, lather, repeat until getting answer and it’s signature which can be verified.

DNSSEC Provisioning at the TLD

- Registrant generates a public/private key pair for a zone
- Registrant signs the zone with private key
- Registrant sends the zone's public key to the registrar
- Registrar sends the registrant's key to the registry
- Registry puts the registrants key hash into the TLD zone
- Registry signs the TLD zone
- Registry publishes the signed TLD zone

Stolen from Bill Manning

Keys

- Each key has a valid time window
- Key signing keys – maintain crypto validity longer as it only signs keys. NIST: 1-2 years
- Zone signing keys – If signed by KSK can be maintained locally and changed as needed
- Rollover issues

DS Record

- Recent addition
- If parent key become invalid, it can resign its zone without contacting children. The DS records for the children are still valid, only it’s signature needs to be updated

NSEC

- Secured zones must be sorted, Bind provides tools to process zone into secure zone
- Given a zone with a.foo, b.foo, d.foo:

  a.foo NSEC b.foo

  b.foo NSEC d.foo

  d.foo NSEC a.foo
- If c.foo is queried, the middle NSEC record confirms that it does not exist in zone.

Dynamic DNS now harder

- Private keys best stored away from DNS server
- Updated data must be signed on the fly
- NSEC processing must occur with each update
- What about NSEC records that have been cached?

Additional Overhead

- More administrative activities related to keys
- Every RR has an RRSIG, zone files increase by factor of 2-3.
- Every query response larger, bandwidth issues?
- Verisign – Signing .net/.com?
- Will your secondary server providers also provide DNSSEC services?

The root of all evils

- Signing the root zone necessary to end the islands of trust.
- Technical issues: reducing the diversity of the root servers with limited number of implementations; capacity
- Political issues:…….

Resources

- NIST SP800-81 (draft)
- NLnetlabs.NL
- Watch rollout in .SE